Groupe de travail Réseau
Request for Comments : 3893
Catégorie : En cours de normalisation

J. Peterson, NeuStar
septembre 2004
Traduction Claude Brière de L'Isle

Format de corps d'identité authentifiée (AIB) du protocole d'initialisation de session (SIP)

Résumé
La RFC3261 introduit le concept d'ajout d'un corps S/MIME à une demande ou réponse du protocole d'initialisation de session (SIP) afin de fournir l'intégrité de référence sur ses en-têtes. Le présent document fournit un mécanisme plus spécifique pour déduire les propriétés d'intégrité et d'authentification à partir d'un "corps d'identité authentifié", un message SIP signé numériquement, ou un fragment de message. Un format standard pour de tels corps (connus sous le nom de corps d'identité authentifiés, AIB, *Authenticated Identity Bodies*) est fourni par le présent document. On donne aussi certaines considérations sur le traitement des AIB par les receveurs de messages SIP qui comportent de tels corps.

Table des Matières

1. Introduction

Le paragraphe 23.4 de la [RFC3261] décrit un mécanisme de protection de l'intégrité qui s'appuie sur la signature de corps MIME 'message/sip' tunnelés au sein des demandes SIP. L'objet de ce mécanisme est de dupliquer les en-têtes d'une demande SIP au sein d'un corps porté dans cette demande afin de fournir une signature numérique sur ces en-têtes. La signature sur ce corps fournit aussi l'authentification.

L'exigence centrale qui motive le mécanisme de 'message/sip' tunnelé est le problème de la fourniture d'une identité cryptographiquement vérifiable au sein d'une demande SIP. Le protocole SIP de base permet à un agent d'utilisateur d'exprimer l'identité de son utilisateur dans n'importe quel nombre d'en-têtes. La principale place pour les informations d'identité affirmées par l'envoyeur d'une demande est l'en-tête From. L'en-tête From contient un URI (comme 'sip:alice@example.com') et un nom d'affichage facultatif (comme "Alice") qui identifie l'origine de la demande. Un

utilisateur peut avoir plusieurs identités qui seront utilisées dans des contextes différents.

Normalement, cet URI est une adresse d'enregistrement qui peut être déréférencée afin de contacter l'origine de la demande ; précisément, c'est généralement la même adresse d'enregistrement sous laquelle un usager enregistre ses appareils afin de recevoir les demandes entrantes. Cette adresse d'enregistrement est allouée et entretenue par l'administrateur du service SIP dans le domaine identifié par la portion hôte de l'adresse d'enregistrement. Cependant, le champ From d'une demande est généralement réglé à une valeur arbitraire par l'utilisateur d'un agent d'utilisateur SIP ; l'en-tête From d'un message ne fournit aucune assurance interne que l'utilisateur d'origine peut légitimement revendiquer l'identité affichée. Néanmoins, de nombreux agents d'utilisateur SIP vont obligeamment afficher le contenu du champ From comme identité de l'origine d'une demande reçue (comme une sorte de fonction d'identification de l'appelant) un peu comme les mises en œuvre de messagerie électronique affichent le champ From comme identité de l'envoyeur.

Pour fournir au receveur d'un message SIP une plus grande assurance de l'identité de l'envoyeur, on peut fournir une signature cryptographique sur les en-têtes de la demande SIP, qui permet au signataire d'affirmer une identité vérifiable. Malheureusement, une signature sur l'en-tête From seul est insuffisante parce que elle pourrait être copiée collée dans une attaque en répétition ou de transmission, et plus d'en-têtes sont donc nécessaires pour corréler une signature avec une demande. La RFC3261 recommande donc de copier tous les en-têtes de la demande dans un corps MIME signé ; cependant, les messages SIP peuvent être grand, et beaucoup des en-têtes d'un message SIP ne seront pas pertinents pour déterminer l'identité de l'envoyeur ou assurer l'intégrité de référence avec la demande, et de plus certains en-têtes peuvent changer dans le transit pour des raisons parfaitement valides. Donc, ce grand corps 'message/sip' tunnelé va presque nécessairement comporter des variations des en-têtes d'une demande lorsque il sera reçu par l'UAS, et c'est l'UAS qui aura la charge de déterminer quels changements d'en-tête étaient légitimes, et quels sont des violations de la sécurité. Il est donc souhaitable de trouver un moyen heureux pour signer juste assez d'en-têtes pour que l'identité de l'envoyeur puisse être confirmée et corrélée avec la demande. Le 'message/sipfrag' [RFC3420] donne le moyen pour qu'un sous ensemble d'en-têtes SIP soient inclus dans un corps MIME ; le format de corps d'identité authentifiée (AIB, *Authenticated Identity Body*) décrit à la Section 2 se fonde sur 'message/sipfrag'.

Pour des raisons de confidentialité de bout en bout, il peut aussi être souhaitable de chiffrer les AIB ; les procédures pour ce chiffrement sont données à la Section 8.

Le présent document propose que le format AIB soit utilisé à la place du mécanisme existant de 'message/sip' tunnelé décrit au paragraphe 23.4 de la [RFC3261], afin de fournir l'identité de l'appelant ; si la vérification de l'intégrité sur d'autres en-têtes sans relation est requise, le mécanisme 'message/sip' devrait alors être utilisé.

1.1 Notation des exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans la [RFC2119].

2. Format d'AIB

Comme moyen pour partager une identité authentifiée entre des parties dans le réseau, un type spécial de format de corps MIME, le format de corps d'identité authentifiée (AIB, *Authenticated Identity Body*) est défini dans cette section. Les AIB permettent à une partie à une transaction SIP de signer cryptographiquement les en-têtes qui affirment l'identité de l'origine d'un message, et fournissent d'autres en-têtes nécessaires pour l'intégrité de la référence.

Un AIB est un corps MIME de type 'message/sipfrag' (pour plus d'informations sur la construction des sipfrag, incluant des exemples, voir la [RFC3420]). Ce corps MIME DOIT avoir un type de disposition de disposition de contenu [RFC2183] de 'aib', nouvelle valeur définie dans le présent document spécifiquement pour les corps d'identité authentifiée. L'en-tête Content-Disposition DEVRAIT aussi contenir un paramètre "traitement" indiquant que ce corps MIME est facultatif (c'est-à-dire, si ce mécanisme n'est pas pris en charge par le serveur d'agent d'utilisateur, il peut quand même tenter de traiter la demande).

Les AIB qui utilisent le type MIME 'message/sipfrag' DOIVENT contenir les en-têtes suivants lorsque ils fournissent l'identité pour une demande INVITE : From, Date, Call-ID, et Contact ; ils DEVRAIENT aussi contenir les en-têtes To et CSeq. Les propriétés de sécurité de ces en-têtes, et les circonstances dans lesquelles ils devraient être utilisés, sont décrites à la Section 10. Les AIB PEUVENT contenir tout autre en-tête qui aide à identifier de façon univoque la transaction ou confirme l'intégrité de la référence qui s'y rapporte. Un exemple de format AIB pour un INVITE est :

Content-Type: message/sipfrag

Content-Disposition: aib; handling=optional

From: Alice <sip:alice@example.com>
To: Bob <sip:bob@example.net>
Contact: <sip:alice@pc33.example.com>
Date: Thu, 21 Feb 2002 13:02:03 GMT
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE

Les AIB non signés DOIVENT être traités par tous receveurs selon les règles établies dans la Section 7 pour les AIB qui ne valident pas. Après la signature de l'AIB, il DEVRAIT être ajouté aux corps MIME existants dans la demande (comme une SDP) si nécessaire en transformant les corps MIME les plus externes en un format 'multipart/mixed'.

3. Exemple de demande avec AIB

Voici une demande INVITE SIP complète avec un AIB :

INVITE sip:bob@example.net SIP/2.0
Via: SIP/2.0/UDP pc33.example.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@example.net>
From: Alice <sip:alice@example.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:03 GMT
Contact: <sip:alice@pc33.example.com>
Content-Type: multipart/mixed; boundary=unique-boundary-1

--unique-boundary-1

Content-Type: application/sdp
Content-Length: 147

v=0
o=UserA 2890844526 2890844526 IN IP4 example.com
s=Session SDP
c=IN IP4 pc33.example.com
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=boundary42
Content-Length: 608

--boundary42
Content-Type: message/sipfrag
Content-Disposition: aib; handling=optional
From: Alice <sip:alice@example.com>
To: Bob <sip:bob@example.net>
Contact: <sip:alice@pc33.example.com>
Date: Thu, 21 Feb 2002 13:02:03 GMT
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE

--boundary42
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64

Content-Disposition: attachment; filename=smime.p7s;
handling=required

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT64VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUu
jhJh756tbB9HGTrfvbnjn8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF47GhIGfHfYT64VQbnj756

--boundary42--

--unique-boundary-1--

4. AIB pour identifier les tiers

Il y a des cas particuliers d'utilisation de la méthode INVITE dans lesquels certains messages SIP sont échangés avec un tiers avant qu'un INVITE soit envoyé, et dans lesquels l'identité du tiers doit être portée dans l'INVITE suivant. Les détails de l'identité d'adressage dans de tels contextes sortent du domaine d'application du présent document. À haut niveau, il est possible que les informations d'identité pour un tiers soient portées dans un AIB supplémentaire. La présence d'un AIB supplémentaire dans un message n'empêcherait pas l'apparition d'un AIB 'régulier' comme spécifié dans ce document.

Des exemples de cas où des AIB supplémentaires pourraient apparaître incluent :
- l'utilisation de la méthode REFER [RFC3892], par exemple, a une exigence que le receveur d'un INVITE s'assure de l'identité du référant qui a causé l'envoi de l'INVITE ;
- le contrôle d'appel de tiers (3PCC, *Third-party call control*) [RFC3725] a un problème d'identité encore plus compliqué. Un contrôleur central envoie des INVITE à une partie, rassemble des informations d'identité (et de contexte de session) sur cette partie, puis utilise ces informations pour envoyer un INVITE à une autre partie. Idéalement, le contrôleur va aussi avoir un moyen pour partager une signature cryptographique d'identité donnée par la première partie qui a reçu l'INVITE du contrôleur avec la seconde partie invitée par le contrôleur.

Dans ces deux cas, le Call-ID et le CSeq de la demande originale (INVITE 3PCC ou REFER) ne vont pas correspondre avec ceux de la demande dans le INVITE suivant, ni les champs To ou From. Dans les deux cas du REFER et du 3PCC, le Call-ID et le CSeq ne peuvent être utilisés pour garantir l'intégrité de la référence, et il est donc beaucoup plus difficile de corréler un AIB à une demande INVITE.

Donc, dans ces cas, d'autres en-têtes pourraient être utilisés pour fournir l'intégrité de référence entre les en-têtes dans un AIB supplémentaire avec les en-têtes d'un INVITE généré par un 3PCC ou un REFER, mais cet usage sort du domaine d'application du présent document. Afin que les AIB soient utilisés dans ces contextes de tiers, un travail de spécification complémentaire est nécessaire pour déterminer quels en-têtes supplémentaires, s'il en est, doivent être inclus dans un AIB dans le cas spécifique d'un tiers, et comment différencier l'AIB principal dans un message provenant d'un AIB de tiers.

5. Identité dans les demandes non INVITE

Les exigences pour remplir un AIB dans les demandes au sein d'un dialogue sont généralement parallèles à celles de l'INVITE : les champs d'en-tête From, Call-ID, Date, et Contact sont EXIGÉS.

Certaines demandes non INVITE, peuvent cependant avoir des exigences d'identité différentes. Les nouvelles méthodes ou extensions SIP qui démultiplieront la sécurité des AIB DEVRONT identifier toutes les exigences d'identité particulières dans la section Considérations sur la sécurité de leur spécification.

6. Identité dans les réponses

Beaucoup des pratiques décrites dans les paragraphes précédents peuvent s'appliquer aux réponses aussi bien qu'aux demandes. Noter qu'un nouvel ensemble d'en-têtes doit être généré pour remplir l'AIB dans une réponse. Le champ d'en-tête From de l'AIB dans la réponse à un INVITE DOIT correspondre à l'adresse d'enregistrement de celui qui répond, et NON au champ d'en-tête From reçu dans la demande. Le champ d'en-tête To de la demande NE DOIT PAS être inclus. Un nouveau champ d'en-tête Date et un champ d'en-tête Contact devraient être générés pour l'AIB dans une réponse. Le Call-ID et le CSeq devraient cependant être copiés de la demande.

Généralement, le champ d'en-tête To de la demande va correspondre à l'adresse d'enregistrement de celui qui répond. Dans certaines architectures où un reciblage est utilisé, cela n'a cependant pas besoin d'être le cas. Certains receveurs d'AIB de

réponse peuvent le considérer comme une cause de problèmes de sécurité si le champ d'en-tête To de la demande n'est pas le même que celui de l'adresse d'enregistrement du champ d'en-tête From de l'AIB dans une réponse.

7. Réception d'un AIB

Lorsque un agent d'utilisateur reçoit une demande qui contient un AIB, il DOIT vérifier la signature, incluant de valider le certificat du signataire, et comparer l'identité du signataire (le subjectAltName) avec, dans le cas d'un INVITE, la portion domaine de l'URI dans le champ d'en-tête From de la demande (pour les demandes non INVITE, d'autres en-têtes PEUVENT être soumis à cette comparaison). Les deux devraient correspondre exactement ; si ils ne le font pas, l'agent d'utilisateur DOIT rapporter cette condition à son utilisateur avant de continuer. Les agents d'utilisateur PEUVENT distinguer des variations mineures plausibles (la différence entre 'example.com' et 'sip.example.com') et des variations majeures ('example.com' contre 'example.org') lorsque ils rapportent ces discordances afin de donner à l'utilisateur une idée de la façon de traiter cette situation. L'analyse et la comparaison des champs d'en-tête Date, Call-ID, et Contact comme décrites à la Section 10 DOIVENT aussi être effectuées. Toutes les discordances ou violations DOIVENT être rapportées à l'utilisateur.

Lorsque l'agent d'utilisateur d'origine d'une demande reçoit une réponse contenant un AIB, il DEVRAIT comparer l'identité dans le champ d'en-tête From de l'AIB de la réponse avec la valeur d'origine du champ d'en-tête To de la demande. Si elles représentent des identités différentes, l'agent d'utilisateur DEVRAIT rapporter l'identité qui est dans l'AIB de la réponse à son utilisateur. Noter qu'une discordance entre ces champs d'identité n'est pas nécessairement l'indication d'une violation de la sécurité ; un reciblage normal peut simplement avoir dirigé la demande sur une destination finale différente. Les mises en œuvre peuvent donc considérer que dans ce cas, il n'est pas nécessaire d'alerter l'usager d'une violation de sécurité.

8. Chiffrement d'identité

De nombreuses entités SIP qui prennent en charge l'utilisation de S/MIME pour les signatures prennent aussi en charge le chiffrement de S/MIME, comme décrit au paragraphe 23.4.3 de la [RFC3261].

Bien que le chiffrement des AIB ait pour conséquence que seul le détenteur d'une clé spécifique puisse déchiffrer le corps, cette seule clé pourrait être distribuée dans tout un réseau d'hôtes qui existent sous une politique commune. La sécurité de l'AIB est donc liée à la sécurité de la distribution de la clé. Cependant, pour certains réseaux (dans lesquels il y a des fédérations d'hôtes de confiance sous une politique commune) la large distribution d'une clé de déchiffrement pourrait être appropriée. Certains réseaux téléphoniques, par exemple, pourraient requérir ce modèle.

Lorsque un AIB est chiffré, il DEVRAIT être chiffré avant d'être signé. Les mises en œuvre DOIVENT quand même accepter les AIB qui ont été signés puis chiffrés.

9. Exemple de chiffrement

Voici un exemple d'AIB chiffré et signé (sans aucun des en-têtes SIP qui le précèdent). Dans une restitution de ce corps envoyé sur le réseau, le texte entouré d'astérisques serait chiffré.

```
Content-Type: multipart/signed;
  protocol="application/pkcs7-signature";
  micalg=sha1; boundary=boundary42
Content-Length: 568
Content-Disposition: aib; handling=optional

--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: 231

**********************************************************
* Content-Type: message/sipfrag                          *
```

```
* Content-Disposition: aib; handling=optional                *
*                                                            *
* From: sip:alice@example.com                                *
* Call-ID: a84b4c76e66710                                    *
* Contact: sip:alice@device21.example.com                    *
* Date: Thu, 21 Feb 2002 13:02:03 GMT                        *
************************************************************

--boundary42

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

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT64VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUu
jhJh756tbB9HGTrfvbnj n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF47GhIGfHfYT64VQbnj756

--boundary42--
```

10. Considérations sur la sécurité

L'objet d'un AIB est de fournir une identité pour l'envoyeur d'un message SIP. Cette identité est détenue dans le champ d'en-tête From d'un AIB. Bien que d'autres en-têtes soient aussi inclus, il ne sont fournis que pour aider à la détection des attaques en répétition et en copié collé lancées pour se faire passer pour l'appelant. Le contenu du champ d'en-tête From d'un AIB valide peut être affiché comme un "identifiant d'appelant" pour l'envoyeur du message SIP.

Le présent document rend obligatoire l'inclusion des champs d'en-tête Contact, Date, Call-ID, et From au sein d'un AIB, et recommande l'inclusion des champs d'en-tête CSeq et To, lorsque 'message/sipfrag' est utilisé pour représenter l'identité de l'envoyeur d'une demande. Si ces en-têtes sont omis, des propriétés de sécurité importantes de l'AIB sont perdues. En général, les considérations relatives à l'inclusion de divers en-têtes dans un AIB sont les mêmes que celles données dans la [RFC3261] pour l'inclusion des en-têtes dans les corps 'message/sip' MIME tunnelés (voir la Section 23 en particulier).

Le champ d'en-tête From indique l'identité de l'envoyeur du message ; si cet en-tête était exclu, le créateur de l'AIB n'affirmerait plus d'identité du tout. Les en-têtes Date et Contact fournissent une protection de l'intégrité de la référence et contre la répétition, comme décrit au paragraphe 23.4.2 de la [RFC3261]. Les mises en œuvre de la présente spécification DOIVENT suivre les règles pour l'acceptation du champ d'en-tête Date dans les demandes 'message/sip' tunnelées décrites au paragraphe 23.4.2 de la [RFC3261] ; cela assure que les AIB périmés ne seront pas répétés (l'intervalle suggéré est que l'en-tête Date doit indiquer une heure dans les 3600 secondes de la réception d'un message). Les mises en œuvre DOIVENT aussi enregistrer les Call-ID reçus dans les AIB, et DOIVENT se rappeler ces Call-ID pendant au moins la durée d'un seul intervalle de Date (c'est-à-dire, 3600 secondes). En conséquence, si un AIB est répété dans l'intervalle de Date, les receveurs vont reconnaître qu'il est invalide parce que le Call-ID est dupliqué ; si un AIB est répété après l'intervalle de Date, les receveurs vont reconnaître qu'il est invalide parce que la Date est périmée. Le champ d'en-tête Contact est inclus pour lier l'AIB à une instance particulière d'appareil qui a généré la demande. Si un attaquant actif avait intercepté une demande contenant un AIB, et avait copié collé l'AIB dans sa propre demande (réutilisant les champs From, Contact, Date, et Call-ID qui apparaissaient dans l'AIB) elle ne serait pas éligible à recevoir des demandes SIP de la part de l'agent d'utilisateur de l'appelé, car ces demandes sont acheminées à l'URI identifié dans le champ d'en-tête Contact.

Les champs d'en-tête To et CSeq fournissent des propriétés qui sont généralement utiles, mais pas pour toutes les applications possibles des AIB. Si un nouvel AIB est produit chaque fois qu'est initiée un nouvelle transaction SIP dans un dialogue, le champ d'en-tête CSeq fournit une propriété précieuse (la protection contre la répétition pour cette transaction particulière). Si cependant un AIB est utilisé pour un dialogue entier, les transactions suivantes dans le dialogue vont utiliser le même AIB qui apparaissait dans la transaction INVITE. Utiliser un seul AIB pour un dialogue entier réduit la charge qui pèse sur le générateur de l'AIB. Le champ d'en-tête To désigne généralement l'URI d'origine que l'appelant avait l'intention d'atteindre, et donc, il peut différer de celui mentionné dans l'URI de demande si un reciblage se produit en un point du réseau. En conséquence, inclure le champ d'en-tête To dans l'AIB aide à identifier les attaques de copié collé dans lesquelles un AIB envoyé à une destination particulière est réutilisé pour se faire passer pour l'envoyeur à une destination différente. Cependant, l'inclusion du champ d'en-tête To n'aura probablement pas beaucoup de sens dans de nombreux cas d'AIB de tiers (comme décrit à la Section 4) et son inclusion ne sera pas non plus nécessaire pour les réponses.

11. Considérations relatives à l'IANA

Le présent document définit une nouvelle valeur de type de disposition de disposition de contenu MIME de 'aib'. Cette valeur est réservée aux corps MIME qui contiennent une identité authentifiée, comme décrit à la Section 2.

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.

[RFC2183] R. Troost, S. Dorner, K. Moore, éd., "Communication des informations de présentation dans les messages Internet : le champ d'en-tête Contenu-disposition", août 1997. (*MàJ par* RFC2184, RFC2231) *(P.S.)*

[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.

12.2 Références pour information

[RFC3892] R. Sparks, "Mécanisme Referred-by du protocole d'initialisation de session (SIP)", septembre 2004.

[RFC3725] J. Rosenberg et autres, "Bonne pratiques actuelles pour la commande d'appel de tiers (3pcc) dans le protocole d'initialisation de session (SIP)", avril 2004. (BCP0085)

13. Remerciements

L'auteur tient à remercier Robert Sparks, Jonathan Rosenberg, Mary Watson, et Eric Rescorla de leurs commentaires. Rohan Mahy a aussi fourni des indications précieuses.

14. Adresse de l'auteur

Jon Peterson
NeuStar, Inc.
1800 Sutter St
Suite 570
Concord, CA 94520
USA

téléphone : +1 925/363-8720
mél : jon.peterson@neustar.biz
URI : http://www.neustar.biz/

15. Déclaration complète de droits de reproduction

d'autres langues que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Internet Society ou ses successeurs ou ayant 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 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 pourrait 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.