Groupe de travail Réseau
Request for Comments : 4261
RFC mise à jour : 2748
Catégorie : Sur la voie de la normalisation

J. Walker
A. Kulkarni, éd., Intel Corp.
décembre 2005
Traduction Claude Brière de L'Isle

Service commun de politique ouverte (COPS) sur sécurité de la couche Transport (TLS)

Résumé
Le présent document décrit comment utiliser la sécurité de la couche Transport (TLS, *Transport Layer Security*) pour sécuriser les connexions du service commun de politique ouverte (COPS, *Common Open Policy Service*) sur l'Internet.

Le présent document met aussi à jour la RFC 2748 en modifiant le contenu du message Client-Accept.

Table des matières

1. Introduction

COPS [RFC2748] a été conçu pour distribuer des informations de politique en clair à partir d'un point de décision de politique (PDP, *Policy Decision Point*) centralisé à un ensemble de points d'application de politique (PEP, *Policy Enforcement Point*) dans l'Internet. COPS fournit ses propres mécanismes de sécurité pour protéger l'intégrité bond par bond de la politique déployée. Cependant, l'utilisation de COPS pour des applications sensibles (par exemple, certains types de distribution de politique de sécurité) exige des mesures de sécurité supplémentaires comme la confidentialité des

données. C'est parce que certaines organisations estiment nécessaire de cacher certaines de leurs politiques de sécurité, ou toutes, par exemple, parce que la distribution de la politique aux appareils comme les plate-formes mobiles peut traverser des limites de domaines.

TLS [RFC2246] a été conçu pour fournir une sécurité centrée sur le canal. TLS normalise SSL et peut être utilisé avec tout service en mode connexion. TLS fournit des mécanismes pour l'authentification aussi bien unidirectionnelle que bidirectionnelle, le chiffrement dynamique de session, et la protection de la confidentialité et de l'intégrité du flux de données.

Le présent document décrit comment utiliser COPS sur TLS. "COPS sur TLS" est abrégé en COPS/TLS.

Glossaire

COPS *(Common Open Policy Service)* : service commun de politique ouverte (voir la [RFC2748]).

COPS/TCP : mise en œuvre de base de COPS.

COPS/TLS : mise en œuvre sécurisée de COPS utilisant TLS.

PDP *(Policy Decision Point)* : point de décision de politique, aussi appelé serveur de politique (voir la [RFC2753]).

PEP *(Policy Enforcement Point)* : point d'application de politique, aussi appelé client de politique (voir la [RFC2753]).

Conventions utilisées dans le document

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. COPS sur TLS

COPS/TLS est très simple : utiliser COPS sur TLS comme on utiliserait COPS sur TCP (COPS/TCP). À part une procédure spécifique utilisée pour initialiser la connexion, il n'y a pas de différence entre COPS/TLS et COPS/TCP.

3. Accès sépares contre négociation vers l'amont

Il y a deux façons dont les versions sûres et non sûres du même protocole peuvent fonctionner simultanément.

Dans la première méthode, la version sûre du protocole est aussi allouée à un accès bien connu. Cette tactique d'avoir des numéros d'accès bien connus pour les deux versions, sûre et non sûre, est aussi appelée "accès séparés". Les clients qui exigent la sécurité peuvent simplement se connecter à l'accès sûr bien connu. Cette méthode est aisée à mettre en œuvre, sans avoir besoin de modification aux mises en œuvre non sûres existantes. L'inconvénient est cependant que cela ne s'adapte pas bien parce que un nouvel accès est nécessaire pour chaque mise en œuvre sûre. Plus de problèmes de cette approche ont été mentionnés dans la [RFC2595].

La seconde méthode est appelée "négociation vers l'amont". Dans cette méthode, les versions, sûre et non sûre, du protocole, fonctionnent sur le même accès. Le client se connecte au serveur, et ils découvrent tous deux leurs capacités réciproques, et commencent les négociations de sécurité si ils le désirent. Cette méthode exige généralement quelques changements au protocole à sécuriser.

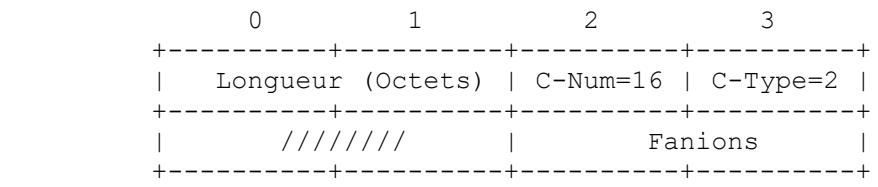
Vus les nombreux problèmes de l'approche des accès séparés, les auteurs ont décidé d'utiliser la méthode de la négociation vers l'amont pour COPS/TLS.

4. Objets et codes d'erreur COPS/TLS

Cette section décrit les objets COPS et les codes d'erreur nécessaires pour prendre en charge COPS/TLS

4.1 Objet Intégrité de message TLS (Integrity-TLS)

L'objet TLS Integrity est utilisé par le PDP et le PEP pour commencer la négociation TLS. Cet objet devrait être inclus seulement dans les messages Client-Open ou Client-Accept. Il NE DOIT PAS être inclus dans tout autre message COPS.



Note : //// implique que le champ est réservé, réglé à 0, et devrait être ignoré à réception.

Fanions : 16 bits : 0x01 = commencer TLS
Ce fanion indique que l'envoyeur du message souhaite initier une prise de contact TLS.

Le type de client de tout message contenant cet objet DOIT être 0. Le type de client 0 est utilisé pour négocier la sécurité de niveau connexion COPS et ne doit être utilisé que durant la phase d'établissement de connexion. Voir plus de détails au paragraphe 4.1 de la [RFC2748].

4.2 Codes d'erreur

Ce paragraphe utilise les codes d'erreur décrits au paragraphe 2.2.8 (Objet Erreur) de la [RFC2748].

Code d'erreur : 13 = Objet COPS inconnu

Le sous code (octet 2) contient le C-Num de l'objet inconnu, et l'octet 3 contient le C-Type de l'objet inconnu. Si le PEP ou le PDP ne prend pas en charge TLS, le C-Num spécifié DOIT être 16 et le C-Type DOIT être 2. Cela démontre que la version TLS de l'objet Integrity n'est pas connu.

Ce code d'erreur DOIT être utilisé par le PEP ou le PDP pour indiquer une clôture de connexion en rapport avec la sécurité si il ne peut pas prendre en charge une connexion TLS pour le protocole COPS.

Si le PDP souhaite négocier un mécanisme de sécurité différent de celui demandé par le PEP dans le Client-Open, il DOIT envoyer le code d'erreur suivant :

Code d'erreur : 15= Authentification exigée

Lorsque le sous code (octet 2) contient la valeur de C-Num=16 pour l'objet Integrity et l'octet 3 DOIT spécifier le C-Type d'objet Integrity exigé/préféré du PDP. Si le serveur ne prend en charge aucune forme de sécurité COPS, il DOIT alors régler le sous code (octet 2) à 16 et l'octet 3 à zéro, signifiant qu'aucun type d'objet Integrity n'est pris en charge.

5. Initialisation de connexion COPS/TLS sécurisée

La négociation de la sécurité peut être initiée par le PDP ou le PEP. Le PEP peut initier une négociation via un message Client-Open, tandis qu'un PDP peut initier une négociation via un message Client-Accept.

Une fois que la connexion TLS est établie, toutes les données COPS DOIVENT être envoyées comme "données d'application" TLS.

5.1 Négociation de sécurité initiée par le PEP

Un PEP PEUT initier une négociation de sécurité TLS avec un PDP en utilisant le message Client-Open. Pour ce faire, le message Client-Open DOIT avoir un type de client de 0 et DOIT inclure l'objet Integrity-TLS.

À réception du message Client-Open, le PDP DEVRAIT répondre par un message Client-Accept contenant l'objet Integrity-TLS.

Noter qu'afin de porter l'objet Integrity-TLS, le contenu du message Client-Accept défini au paragraphe 3.7 de la [RFC2748] n'a pas besoin de changer, sauf que le C-Type de l'objet Integrity qui y est contenu devrait maintenant être C-Type=2. Par exemple :

<Client-Accept> ::= <En-tête commun>
<Temporisateur KA>
[<Temporisateur ACCT>]
[<Integrity (C-Num=16, C-Type=2)>]

Noter aussi que ce nouveau format du message Client-Accept ne remplace ni ne rend obsolète le format existant de message Client-Accept, qui peut continuer d'être utilisé pour les négociations COPS non sécurisées.

À réception du message Client-Accept approprié, le PEP DEVRAIT initier la prise de contact TLS.

L'échange de messages est le suivant :

C : Client-Open (Client-Type = 0, Integrity-TLS)
S : Client-Accept (Client-Type = 0, Integrity-TLS)
<prise de contact TLS>
C/S : <...autres messages...>

Dans le cas où le PDP ne souhaite pas ouvrir une connexion sûre avec le PEP, il DOIT répondre par un message Client-Close et clore la connexion. Le message Client-Close DOIT inclure le code d'erreur 15 = Authentification exigée, avec le sous code (octet 2) réglé à 16 pour le C-Num de l'objet Integrity, et l'octet 3 réglé au C-Type correspondant au type Integrity préféré du serveur, ou zéro pour "pas de sécurité".

Un PEP exigeant l'objet Integrity-TLS dans un message Client-Accept DOIT clore la connexion si l'objet Integrity-TLS manque. Le message Client-Close qui s'ensuit DOIT inclure le code d'erreur 15 = Authentification exigée, avec le sous code (octet 2) contenant le C-Num=16 de l'objet Integrity exigé, et l'octet 3 contenant le C-Type=2 de l'objet Integrity exigé.

5.2 Négociation de sécurité initiée par le PDP

Le PEP ouvre initialement une connexion TCP avec le PDP sur l'accès COPS standard et envoie un message Client-Open. Ce message Client-Open DOIT avoir un type de client de 0.

Le PDP DEVRAIT alors répondre avec un message Client-Accept. Afin de signaler au PEP de commencer la prise de contact TLS, le PDP DOIT inclure l'objet Integrity-TLS dans le message Client-Accept.

À réception du message Client-Accept avec l'objet Integrity-TLS, le PEP DEVRAIT initier la prise de contact TLS. Si pour une raison quelconque le PEP ne peut pas initier la prise de contact, il DOIT clore la connexion.

L'échange de message est le suivant :

C : Client-Open (Client-Type = 0)
S : Client-Accept (Client-Type = 0, Integrity-TLS)
<prise de contact TLS>
C/S : <...autres messages...>

Après la réception du Client-Accept, le PEP NE DOIT PAS envoyer de message jusqu'à l'achèvement de la prise de contact TLS. À réception de tout message provenant du PEP avant le début de la prise de contact TLS, le PDP DOIT produire un message Client-Close avec un code d'erreur de 15 = Authentification exigée.

Un PDP qui souhaite négocier la sécurité avec un PEP qui a une connexion existante non sûre DOIT envoyer un Client-Close avec le code d'erreur 15 = Authentification exigée, avec le sous code (octet 2) contenant le C-Num =16 de l'objet Integrity exigé, et l'octet 3 contenant le C-Type =2 de l'objet Integrity exigé, et ensuite attendre que le PEP se reconnecte. À réception du message Client-Open, il DEVRAIT utiliser le message Client-Accept pour initier la négociation de la sécurité.

6. Clôture de connexion

TLS fournit des facilités pour clore ses connectons en toute sécurité. La réception d'une alerte de clôture valide assure à une mise en œuvre qu'aucune donnée supplémentaire ne va arriver sur cette connexion. La spécification TLS exige des mises en œuvre TLS qu'elles initient un échange d'alerte de clôture avant de clore une connexion. Elle permet aussi aux mises en œuvre TLS de clore les connexions sans attendre de recevoir les alertes de clôture de l'homologue, pourvu qu'elles envoient d'abord la leur. Une connexion close de cette façon est appelée une "clôture incomplète". TLS permet aux mises en œuvre de réutiliser la session dans ce cas, mais COPS/TLS n'utilise pas cette capacité.

Une connexion close sans l'envoi préalable d'une alerte de clôture est appelée une "clôture prématurée". Noter qu'une clôture prématurée ne remet pas en question la sécurité des données déjà reçues, mais indique simplement que les données suivantes peuvent avoir été tronquées. Parce que TLS ignore les limites de message COPS, il est nécessaire d'examiner les données COPS elles-mêmes (précisément l'en-tête de message) pour déterminer si une troncature s'est produite.

6.1 Comportement du système PEP

Les mises en œuvre de PEP DOIVENT traiter les clôtures prématurées comme des erreurs et toutes les données reçues comme potentiellement tronquées. Le protocole COPS permet au système de PEP de trouver si la troncature a eu lieu. Un système de PEP qui détecte une clôture incomplète DEVRAIT récupérer en douceur.

Les systèmes de PEP DEVRAIENT envoyer une alerte de clôture avant de clore la connexion. Les systèmes de PEP qui ne sont pas prêts à recevoir plus de données PEUVENT choisir de ne pas attendre l'alerte de clôture du système de PDP et clore simplement la connexion, générant donc une clôture incomplète du côté du PDP.

6.2 Comportement du système PDP

COPS permets à PEP de clore la connexion à tout moment, et exige des PDP qu'ils récupèrent en douceur. En particulier, les PDP DEVRAIENT être prêts à recevoir une clôture incomplète de la part du PEP, car un PEP ferme souvent pour des raisons de fonctionnement sans relation avec le transfert d'informations de politique entre le PEP et le PDP.

Note de mise en œuvre : le PDP s’attend normalement à être capable de signaler la fin des données en fermant la connexion. Cependant, le PEP peut avoir déjà envoyé l'alerte de clôture et abandonné la connexion.

Les systèmes de PDP DOIVENT tenter d'initier un échange d’alertes de clôture avec le système de PEP avant de clore la connexion. Les systèmes de PDP PEUVENT clore la connexion après l'envoi de l'alerte de clôture, générant donc une clôture incomplète du côté PEP.

7. Identification et contrôle d'accès de point d'extrémité

Toutes les mises en œuvre de PEP de COPS/TLS DOIVENT prendre en charge un mécanisme de contrôle d'accès pour identifier les PDP autorisés. Cette exigence fournit un niveau d'assurance que la politique qui arrive au PEP est bien valide. Les déploiements de PEP DEVRAIENT exiger l'utilisation de ce mécanisme de contrôle d'accès pour le fonctionnement de COPS sur TLS. Quand le contrôle d'accès est activé, la mise en œuvre de PEP NE DOIT PAS initier de connexions COPS/TLS aux systèmes non autorisés comme PDP par le mécanisme de contrôle d'accès.

De façon similaire, les mises en œuvre de PDP COPS/TLS DOIVENT prendre en charge un mécanisme de contrôle d'accès leur permettant de restreindre leur service aux seuls systèmes de PEP autorisés. Cependant, des déploiements PEUVENT choisir de ne pas utiliser un mécanisme de contrôle d'accès au PDP, car des organisations peuvent ne pas considérer les types de politique déployées comme sensibles, et n'ont donc pas besoin de supporter les coûts de gestion des accréditifs pour les systèmes de PEP. Si le contrôle d'accès est utilisé, la mise en œuvre de PDP DOIT cependant terminer les connexions COPS/TLS provenant de systèmes de PEP non autorisés à enregistrer une erreur si un mécanisme de journal d'enregistrement d'incidents est présent.

Les mises en œuvre de COPS/TLS DOIVENT utiliser les certificats X.509 v3 conformes à la [RFC3280] pour identifier les systèmes de PDP et de PEP. Les systèmes COPS/TLS DOIVENT effectuer le traitement de vérification de certificat conformément à la [RFC3280].

Si une extension subjectAltName de type dNSName ou iPAddress est présente dans le certificat du PDP, elle DOIT être utilisée comme identité du PDP. Si les deux types sont présents, dNSName DEVRAIT être utilisé comme l'identité du PDP. Si aucun des deux types n'est présent, le champ de nom commun le plus spécifique dans le champ Subject du certificat DEVRAIT être utilisé.

La confrontation est effectuée en utilisant les règles de correspondance spécifiées dans la [RFC3280]. Si plus d'une identité d'un certain type est présente dans le certificat (par exemple, plus d'un dNSName dans l'extension de certificat subjectAltName) une correspondance dans une des identités fournies est acceptable. Généralement, le système COPS utilise le premier nom pour la correspondance, excepté comme noté ci-dessous dans les exigences de vérification d'adresse IP.

7.1 Identité de PEP

Lorsque les systèmes de PEP ne sont pas en contrôle d'accès, le PDP n'a pas besoin d'une connaissance externe de ce que devrait être l'identité du PEP', et donc les vérifications ne sont ni possibles ni nécessaires. Dans ce cas, il n'est pas exigé que les systèmes de PEP s'enregistrent auprès d'une autorité de certification, et COPS sur TLS utilise l'authentification unidirectionnelle du PDP au PEP.

Quand les systèmes de PEP sont en contrôle d'accès, les PEP DOIVENT être les sujets des certificats d'entité d'extrémité. Dans ce cas, COPS sur TLS utilise l'authentification bidirectionnelle, et le PDP DOIT effectuer les mêmes vérifications d'identité pour les PEP que décrites ci-dessus pour le PDP.

Quand le contrôle d'accès est activé au PDP, les mises en œuvre de PEP DOIVENT avoir un mécanisme pour acquérir en toute sécurité l'ancre de confiance pour chaque autorité de certification autorisée qui produit les certificats pour les PEP pris en charge.

7.2 Identité de PDP

Généralement, les demandes COPS/TLS sont générées par le PEP qui consulte les informations de politique d'amorçage qui identifient les PDP auxquels le PEP est autorisé à se connecter. Cette politique donne au PEP le nom de l'hôte ou l'adresse IP du PDP. Comment ces informations de politique d'amorçage arrivent au PEP sort du domaine d'application du présent document. Cependant, toutes les mises en œuvre de PEP DOIVENT fournir un mécanisme pour livrer ou configurer en toute sécurité la politique d'amorçage.

Toutes les mises en œuvre de PEP DOIVENT être capables d'acquérir en toute sécurité l'ancre de confiance pour chaque autorité de certification (CA, *Certification Authority*) autorisée qui produit les certificats de PDP. Aussi, les PEP DOIVENT prendre en charge un mécanisme pour acquérir en toute sécurité une liste de contrôle d'accès (ACL, *Access Control List*) ou un filtre identifiant l'ensemble des PDP autorisés associés à chaque CA. Les mises en œuvre doivent veiller à éviter les dépendances circulaires dans l'accès aux ancres de confiance et aux ACL. Au minimum, les ancres de confiance et les ACL peuvent être installées manuellement.

Les développements de PEP qui participent à plusieurs domaines, comme ceux sur des mises en œuvre de plates-formes de PEP mobile, PEUVENT utiliser différentes CA et listes de contrôle d'accès dans chaque domaine.

Si le nom d'hôte PDP ou l'adresse IP est disponible via la politique d'amorçage, le PEP DOIT la vérifier par rapport à l'identité du PDP telle que présentée dans le message Certificat TLS du PDP.

Dans certains cas, la politique d'amorçage va identifier le PDP autorisé seulement par une adresse IP du système de PDP. Dans ce cas, le subjectAltName DOIT être présent dans le certificat, et il DOIT inclure un format iPAddress correspondant au nom attendu par le serveur de politique.

Si le nom d'hôte du PDP ne correspond pas à l'identité dans le certificat, un PEP sur un système en mode utilisateur DOIT soit le notifier à l'utilisateur (les systèmes de PEP PEUVENT donner à l'utilisateur l'opportunité de continuer la connexion dans tous les cas) soit terminer la connexion avec une erreur de "mauvais certificat". Les PEP sur les systèmes non participatifs DOIVENT enregistrer l'erreur dans un journal d'audit approprié (si il en est de disponible) et DOIVENT terminer la connexion avec une erreur de "mauvais certificat". Les systèmes de PEP non participatifs PEUVENT fournir un réglage de configuration qui désactive cette vérification, mais ils DOIVENT alors fournir un réglage qui la permette.

8. Exigences pour les suites de chiffrement

Les mises en œuvre DOIVENT prendre en charge la suite de chiffrement TLS_RSA_WITH_3DES_EDE_CBC_SHA. Toutes les autres suites de chiffrement sont facultatives.

9. Rétro compatibilité

Le PEP et le PDP DEVRAIENT être rétro compatibles avec leurs homologues qui n'ont pas été modifiés pour prendre en charge COPS/TLS. Ils DEVRAIENT traiter les erreurs générées en réponse à l'objet Integrity-TLS.

10. Considérations relatives à l'IANA

L'IANA a ajouté la combinaison suivante de C-Num, C-Type pour l'objet Integrity-TLS au registre http://www.iana.org/assignments/cops-parameters :

0x10 0x02 Message Integrity, Integrity-TLS [RFC4261]

Pour le Client-Type 0, l'IANA a ajouté la valeur de fanion suivante pour l'objet Integrity-TLS :

0x01 = StartTLS

De plus, pour le Client-Type 0, l'IANA a ajouté le texte suivant pour les sous codes d'erreur :

Code d'erreur : 15
Sous code d'erreur :
Octet 2 : C-Num de l'objet Integrity
Octet 3 : C-Type de l'objet Integrity pris en charge/préféré ou zéro.

Code d'erreur	Sous code d'erreur		Description
	Octet 2	Octet 3	
15	16	0	pas de sécurité
15	16	2	Integrity-TLS pris en charge/préféré

D'autres valeurs pour le champ Fanions et le champ réservé ne peuvent être alloués que par la règle de consensus de l'IETF, comme défini dans la [RFC2434].

11. Considérations sur la sécurité

Un PDP et un PEP COPS DOIVENT vérifier le résultat de la négociation TLS pour voir si un degré acceptable d'authentification et de confidentialité a été réalisé. Si la négociation a résulté en un algorithme ou une longueur de clé inacceptables, l'un ou l'autre côté PEUT choisir de terminer la connexion.

Une attaque par interposition peut être lancée en supprimant l'objet Integrity-TLS ou en altérant les messages Client-Open ou Client-Accept. Si la sécurité est requise, la politique d'amorçage de PEP et de PDP doit le spécifier, et les mises en œuvre de PEP et de PDP devraient rejeter les messages Client-Open ou Client-Accept qui manquent à inclure un objet Integrity-TLS.

12. Remerciements

Le présent document reproduit librement et adapte le document similaire d'Eric Rescorla [RFC2818] qui spécifie comment HTTP fonctionne sur TLS.

Des discussions avec David Durham, Scott Hahn, et Ylian Sainte-Hillaire ont aussi conduit à des améliorations de ce document.

Les auteurs tiennent à remercier Uri Blumenthal pour sa très sérieuse relecture du présent document quant à la sécurité.

13. Références

13.1 Références normatives

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

[RFC2246] T. Dierks et C. Allen, "Protocole TLS version 1.0", janvier 1999. *(P.S. ; MàJ par* RFC7919)

[RFC2748] D. Durham et autres, "Protocole COPS (Service commun de politique ouverte)", janvier 2000. (*MàJ par* RFC4261) *(P.S.)*

[RFC2753] R. Yavatkar, D. Pendarakis, R. Guerin, "Cadre pour le contrôle d'admission fondé sur la politique", janvier 2000. *(Info.)*

[RFC3280] R. Housley, W. Polk, W. Ford et D. Solo, "Profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", avril 2002. *(Obsolète, voir* RFC5280)

13.2 Références pour information

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre 1998. *(Rendue obsolète par la* RFC5226)

[RFC2595] C. Newman, "Utilisation de TLS avec IMAP, POP3 et ACAP", juin 1999. (*MàJ par* RFC4616, 7817, 8314) *(P.S.)*

[RFC2818] E. Rescorla, "HTTP sur TLS", mai 2000. *(Information)*

Adresse des auteurs

Amol Kulkarni
Intel Corporation
2111 N.E. 25th Avenue
Hillsboro, OR 97214
US
mél : amol.kulkarni@intel.com

Jesse R. Walker
Intel Corporation
2111 N.E. 25th Avenue
Hillsboro, OR 97214
US
mél : jesse.walker@intel.com

Déclaration complète de droits de reproduction

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 la Internet Society.