Groupe de travail Réseau
Request for Comments : 2750
RFC mise à jour : 2205
Catégorie : En cours de normalisation

S. Herzog, IPHighway
janvier 2000

Traduction Claude Brière de L'Isle

Extensions à RSVP pour le contrôle de politique

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

Résumé
Le présent mémoire présente un ensemble d'extensions pour la prise en charge de contrôles d'admission fondés sur une politique générique dans RSVP. Il devrait être perçu comme une extension aux spécifications fonctionnelles de RSVP [RFC2205]

Ces extensions incluent le format standard des objets POLICY_DATA et une description du traitement des événements de politique par RSVP.

Le présent document ne plaide pas en faveur d'un mécanisme de contrôle de politique particulier ; cependant, on trouvera dans les [RFC2748], [RFC2749] et [RFC2753] la description du protocole de routeur/serveur de politique pour ces extensions.

Table des matières

1. Introduction

RSVP fait, par définition, une discrimination entre les utilisateurs, en fournissant à certains un meilleur service aux dépends des autres. Il est donc raisonnable de s'attendre à ce que RSVP soit accompagné de mécanismes de contrôle et de mise en application des politiques d'accès et d'usage. La version 1 de la spécification fonctionnelle de RSVP [RFC2205] utilise comme bouche-trou l'objet POLICY_DATA pour la prise en charge de la politique.

La spécification fonctionnelle de RSVP actuelle décrit l'interface du contrôle d'admission (du trafic) qui ne se fonde "que" sur la disponibilité des ressources. Dans le présent document, on décrit un ensemble d'extensions à RSVP pour la prise en

charge aussi bien de contrôles d'admission fondés sur la politique. La portée du présent document se limite à ces extensions et ne prône aucune architecture spécifique pour les contrôles fondés sur la politique.

Pour les besoins de ce document, on ne fait pas de différence entre point de décision de politique (PDP, *Policy Decision Point*) et point de décision local (LDP, *Local Decision Point*) tels que décrits dans la [RFC2753]. Le terme de PDP devrait être supposé inclure aussi bien le LDP.

2. Scénario simple

On suppose généralement que la mise en application d'une politique (au moins dans ses stades initiaux) va vraisemblablement se concentrer sur les nœuds bordures entre des systèmes autonomes.

La Figure 1 illustre un domaine autonome simple avec deux nœuds frontières (A, C) qui représentent les PEP contrôlés par les PDP. Un nœud central (B) représente un nœud à capacité RSVP ignorant de la politique (PIN, *policy ignorant node*) avec des capacités limitées au traitement de politique par défaut (paragraphe 4.2).

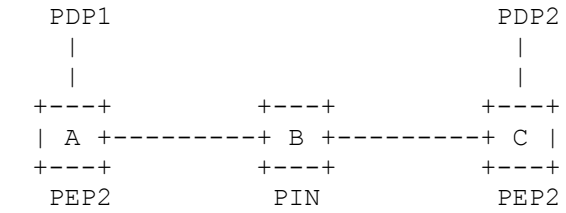


Figure 1 : Scénario de domaine autonome

Ici, les objets de politique transmis à travers le domaine traversent un nœud PIN intermédiaire (B) qui est autorisé à traiter le message RSVP mais considéré comme n'étant pas de confiance pour traiter les informations de politique.

Le présent document décrit les règles de traitement pour les nœuds PEP aussi bien que PIN.

3. Objets Données de politique

Les objets POLICY_DATA sont portés par les messages RSVP et contiennent les informations de politique. Tous les nœuds à capacité de politique (à n'importe quel endroit du réseau) peuvent générer, modifier, ou retirer des objets de politique, même lorsque envoyeurs ou receveurs ne fournissent pas, et peuvent même tout ignorer, des objets de données de politique.

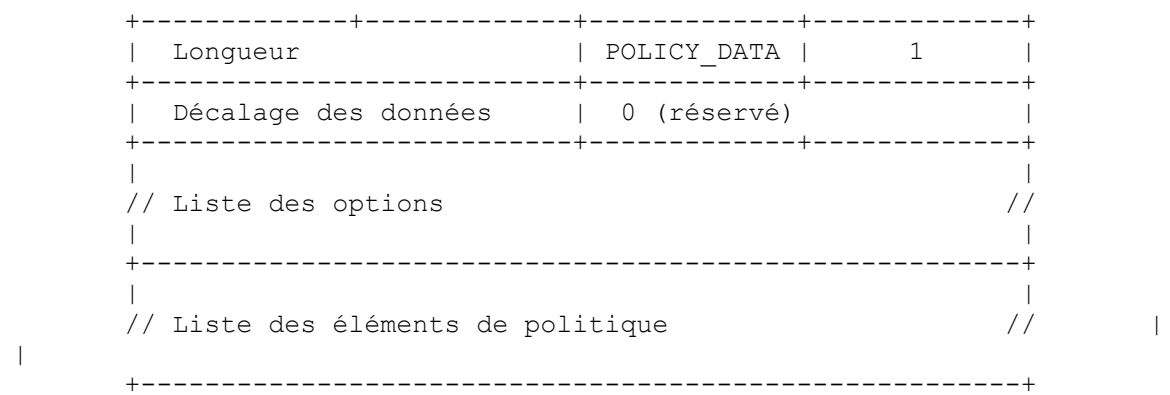
L'échange des objets POLICY_DATA entre les nœuds capables de politique le long du chemin des données, accepte la génération de politiques cohérentes de bout en bout. De plus, de telles politiques peuvent être déployées avec succès à travers plusieurs domaines administratifs lorsque les nœuds frontières manipulent et traduisent les objets POLICY_DATA conformément à des ensembles établis d'accords bilatéraux.

Ce qui suit constitue une extension au paragraphe A.13 de la [RFC2205].

3.1 Format de base

Classe de POLICY_DATA = 14

o Objet POLICY_DATA de type 1 : classe = 14, C-Type = 1



Décalage des données : 16 bits
Le décalage en octets de la portion de données (à partir du premier octet de l'en-tête de l'objet).

Réservé : 16 bits
Toujours à 0.

Liste des options : Longueur variable.
La liste des options et leur usage est définie au paragraphe 3.2.

Liste des éléments de politique : Longueur variable.
Le contenu des éléments de politique est opaque pour RSVP. Voir les détails au paragraphe 3.3.

3.2 Options

Ce paragraphe décrit un ensemble d'options qui peuvent apparaître dans les objets POLICY_DATA. Toutes les options de politique apparaissent dans les objets RSVP mais leur sémantique est modifiée lorsque elles sont utilisées comme options de données de politique.

Objet FILTER_SPEC (liste) ou objet SCOPE
Ces objets décrivent l'ensemble des envoyeurs associés à l'objet POLICY_DATA. Si aucun n'est fourni, les informations de politique sont supposées être associées avec tous les flux de la session. Ces deux types d'objets sont mutuellement exclusifs, et ne peuvent pas être mélangés.

Dans les messages Resv FF empaquetés, cette option FILTER_SPEC fournit une association entre un flux réservé et ses objets POLICY_DATA.

Dans les styles WF ou SE, cette option préserve l'association originale flux/POLICY_DATA telle que formée par les PDP, même à travers des PIN à capacité RSVP. Une telle préservation est exigée car les nœuds PIN peuvent changer la liste des flux réservés à chaque bond, sans considération des aspects légitimes de politique de PDP de bord à bord.

Enfin, l'objet SCOPE devrait être utilisé pour empêcher des "boucles de politique" de façon similaire à celle décrite au paragraphe 3.4 de la [RFC2205]. Lorsque des nœuds PIN font partie d'un chemin de réservation WF, l'objet RSVP SCOPE n'est pas capable d'empêcher des boucles de politique et l'objet de politique SCOPE séparé est nécessaire.

Note : L'utilisation de l'option SCOPE peut avoir un impact significatif sur l'adaptabilité et la taille des objets POLICY_DATA.

Origine du RSVP_HOP
L'objet RSVP_HOP identifie le nœud à capacité de politique voisin/homologue qui a construit l'objet de politique. Lorsque la politique est mise en application à des nœuds frontières, les nœuds de politique homologues peuvent se trouver éloignés de plusieurs bonds RSVP les uns des autres, et l'origine du RSVP_HOP est la base du mécanisme qui leur permet de se reconnaître les uns les autres et de communiquer directement et en toute sécurité.

Si aucun objet RSVP_HOP n'est présent, les données de politique sont implicitement supposées avoir été construites par le RSVP_HOP indiqué dans le message RSVP lui-même (c'est-à-dire que le nœud RSVP voisin est à capacité de politique).

Destination RSVP_HOP
Un second objet RSVP_HOP peut suivre l'objet RSVP_HOP d'origine. Ce second RSVP_HOP identifie le nœud de politique de destination. C'est utilisé pour s'assurer que l'objet POLICY_DATA est livré aux nœuds de politique ciblés. Il peut être utilisé pour émuler une livraison en envoi individuel dans des messages Path en diffusion groupée. Il peut aussi aider à empêcher d'utiliser un objet de politique dans d'autres parties du réseau (attaques en répétition).

Du côté receveur, un nœud de politique devrait ignorer tout POLICY_DATA qui comporte un RSVP_HOP de destination qui ne correspond pas à sa propre adresse IP.

Objet INTÉGRITÉ
La Figure 1 (de la Section 2) donne un exemple où les objets POLICY_DATA sont transmis entre des nœuds frontières tout en traversant des nœuds PIN non sécurisés. Dans ce scénario, le mécanisme RSVP d'intégrité devient inefficace car il place la politique de confiance dans les nœuds PIN intermédiaires (qui sont de confiance pour effectuer la signalisation RSVP mais pas pour effectuer les décisions ou manipulations de politique).

L'option d'objet INTÉGRITÉ au sein de l'objet POLICY_DATA crée des communications directes sûres entre des PEP non

voisins (et leurs PDP de contrôle) sans impliquer les nœuds PIN.

Cette option peut être utilisée à la discrétion des PDP, et elle est calculée d'une manière qui est décrite à l'Appendice B.

Valeurs de rythme de rafraîchissement de politique (PRT, *Policy Refresh TIME_VALUES*)
L'option PRT *(Policy Refresh TIME_VALUES)* est utilisée pour ralentir la fréquence des rafraîchissements de politique pour les politiques qui ont des contraintes de rythme plus lâches par rapport à RSVP. Si l'option PRT est présente, les rafraîchissements de politique peuvent être retenus aussi longtemps qu'au moins un rafraîchissement est envoyé avant l'arrivée à expiration du temporisateur de rafraîchissement de politique. Une valeur minimale pour le PRT est R ; les valeurs les plus faibles sont supposées être R (aucune erreur ni avertissement ne devrait être déclanché).

Pour simplifier le traitement de RSVP, les valeurs de rythme ne sont pas directement fondées sur la valeur du PRT, mais sur un multiplicateur N de rafraîchissement de politique calculé par N = plancher(PRT/R). Les règles de rafraîchissement et de purge sont déduites du paragraphe 3.7 de la [RFC2205] en supposant que la période de rafraîchissement pour le PRT de données de politique est R' calculé par R' = N*R. En pratique, le rafraîchissement et la purge d'état sont ralentis par un facteur de N).

Le multiplicateur de rafraîchissement s'applique seulement aux rafraîchissements périodiques sans changement (plutôt que des mises à jour). Par exemple, une politique qui est rafraîchie aux instants T, T+N, T+2N,... peut rencontrer un changement de chemin détecté à T+X. Dans ce cas, l'événement va forcer une mise à jour immédiate de politique et devrait remettre le rythme de rafraîchissement à T+X+N, T+X+2N,...

Lorsque les nœuds de réseau redémarrent, les messages RSVP entre les PRT de rafraîchissement de politique peuvent être rejetés car ils arrivent sans le nécessaire objet POLICY_DATA. Cette situation d'erreur serait éclaircie par le prochain rafraîchissement de politique périodique ou avec une mise à jour de politique déclanchée par des messages ResvErr ou PathErr.

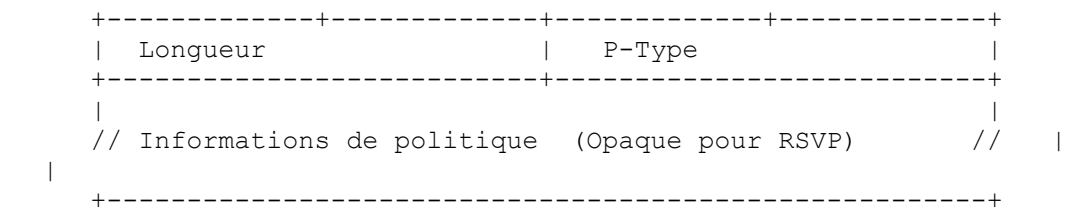
Cette option est particulièrement utile pour combiner des certificats d'authentification forts (redondance élevée) et faibles (faible redondance) comme données de politique. Dans de tels schémas le certificat faible peut prendre en charge l'admission d'une réservation pour seulement une durée limitée, après quoi le certificat fort est exigé.

Cette approche peut réduire la redondance du traitement de POLICY_DATA. Des certificats forts pourraient être transmis moins fréquemment, alors que les certificats faibles sont inclus dans chaque rafraîchissement RSVP.

3.3 Éléments de politique

Le contenu des éléments de politique est opaque pour RSVP ; leur format interne est compris par les homologues de politique, par exemple un point de décision local RSVP (LDP) ou un point de décision de politique (PDP) [RFC2753]. Un registre des codets d'éléments de politique et leur signification est conservé par la [RFC2434] (voir aussi à la Section 5).

Les éléments de politique ont le e format suivant :



3.4 Purge de l'état de politique

L'état de politique arrive à expiration avec la granularité des éléments de politique (les objets POLICY_DATA sont de simples conteneurs et ne se périment pas en tant que tels).

Les éléments de politique arrivent à expiration exactement de la même manière que l'état RSVP reçu dans le même message (voir au paragraphe 3.7 de la [RFC2205]). L'état contrôlé par le PRT arrive à expiration N fois plus lentement (voir au paragraphe 3.2).

Seuls les éléments de politique d'un certain P-Type peuvent être actifs à un moment donné. Les éléments de politique sont donc remplacés instantanément lorsque un autre élément de politique du même P-Type est reçu du même PDP (du RSVP_HOP de politique précédent ou prochain). Un élément de politique vide d'un certain P-Type est utilisé pour supprimer (plutôt que remplacer) tous les états de politique du même P-Type.

4. Règles de traitement

Ces paragraphes décrivent les règles minimales de traitement de politique exigées pour RSVP.

4.1 Signalisation de base

Le présent mémoire rend obligatoire la mise en application du contrôle de politique pour les seuls messages Path, Resv, PathErr, et ResvErr. PathTear et ResvTear sont supposés ne pas exiger de contrôle de politique sur la base de deux hypothèses principales. D'abord, que la vérification de l'intégrité de la [RFC2747] garantit que le message Tear est reçu du même nœud qui a envoyé la réservation installée, et ensuite, qu'il est fonctionnellement équivalent que ce nœud s'abstienne de faire des rafraîchissements pour cette réservation.

4.2 Traitement par défaut pour les nœuds PIN

La Figure 1 illustre un exemple d'objets Données de politique qui traversent des nœuds PIN en transit d'un PEP à un autre.

Un nœud PIN est obligé au minimum de transmettre les objets POLICY_DATA reçus dans les messages sortants appropriés conformément aux règles suivantes :

- Les objets POLICY_DATA sont à transmettre comme ils sont, sans aucune modification.

- Les nœuds de fusion (partage) en diffusion groupée :
  Dans la direction vers l'amont :
  Lorsque plusieurs objets POLICY_DATA arrivent de l'aval, le nœud RSVP devrait tous les enchaîner (comme une liste des objets POLICY_DATA originaux) et les transmettre avec les message sortant (vers l'amont).
  Dans la direction vers l'aval :
  Lorsque un seul objet POLICY_DATA entrant arrive de l'amont, il devrait être transmis (copié) à toutes les branches aval de l'arbre de diffusion groupée.

Les mêmes règles s'appliquent aux (sous-objets) de politique non reconnus au sein de l'objet POLICY_DATA. Cependant, comme cela ne peut se produire que dans un nœud à capacité de politique, elles sont de la responsabilité du PDP et non de RSVP.

4.3 Signalisation des erreurs

Les erreurs de politique font l'objet d'un rapport par les messages ResvErr ou PathErr avec un code d'erreur Défaillance de politique dans l'objet ERROR_SPEC. Le message Erreur de politique doit comporter un objet POLICY_DATA ; l'objet contient les détails du type d'erreur et la cause dans un format spécifique du P-Type (voir au paragraphe 3.3).

Si une réservation de diffusion groupée échoue pour des raisons de politique, RSVP ne devrait pas tenter de découvrir quelle réservation a causé la défaillance (comme il le ferait pour l'état Blocage). Au lieu de cela, il devrait tenter de livrer la ResvErr de politique à TOUS les bonds vers l'aval, et laisser le PDP (ou LDP) décider où les messages devraient être envoyés. Ce mécanisme permet au PDP de limiter la distribution de l'erreur en décidant quel prochain bond "coupable" devrait être informé. Cela permet aussi au PDP d'empêcher une plus large distribution des messages ResvErr ou PathErr en effectuant une réparation locale (par exemple, en substituant à l'objet POLICY_DATA défaillant un objet différent).

Les codes d'erreur sont décrits à l'Appendice A.

5. Considérations relatives à l'IANA

Éléments de politique RSVP (P-Types)

Suivant les politiques exposées dans la [RFC2434], les numéros 0 à 49 151 sont alloués comme éléments de politique standard par action de consensus de l'IETF, les numéros dans la gamme 49 152 à 53 247 sont alloués comme spécifiques des fabricants (un par fabricant) au premier arrivant, et les numéros de 53 248 à 65 535 sont réservés pour utilisation privée et ne sont pas alloués par l'IANA.

6. Considérations pour la sécurité

Le présent mémoire décrit l'utilisation des objets POLICY_DATA pour transporter des informations en rapport avec la politique entre les nœuds RSVP. Deux mécanismes de sécurité peuvent facultativement être utilisés pour assurer l'intégrité des informations transportées. Le premier mécanisme s'appuie sur l'intégrité RSVP [RFC2747] pour fournir une chaîne de confiance lorsque tous les nœuds RSVP sont à capacité de politique. Le second mécanisme s'appuie sur l'objet INTÉGRITÉ au sein de l'objet POLICY_DATA pour garantir l'intégrité entre des PEP RSVP non voisins (voir aux paragraphes 2 et 3.2).

7. Références

[RFC2205] R. Braden, éd., L. Zhang, S. Berson, S. Herzog, S. Jamin, "Protocole de réservation de ressource (RSVP) -- version 1, spécification fonctionnelle", septembre 1997. (*MàJ par* RFC2750, RFC3936, RFC4495) *(P.S.)*

[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)*

[RFC2747] F. Baker, B. Lindell, M. Talwar, "Authentification cryptographique RSVP", janvier 2000. (*MàJ par* RFC3097) *(P.S.)*

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

[RFC2749] S. Herzog, et autres, "Utilisation de COPS avec RSVP", janvier 2000. *(P.S.)*

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

8. Remerciements

Le présent document incorpore des apports de Lou Berger, Bob Braden, Deborah Estrin, Roch Guerin, Timothy O'Malley, Dimitrios Pendarakis, Raju Rajan, Scott Shenker, Andrew Smith, Raj Yavatkar, et de nombreux autres.

9. Informations sur l'auteur

Shai Herzog
IPHighway, Inc.
55 New York Avenue
Framingham, MA 01701
USA
téléphone : (508) 620-1141
mél : herzog@iphighway.com

Appendice A : Codes d'erreur de politique

Le présent appendice étend la liste des codes d'erreur décrite à l'Appendice B de la [RFC2205].

Noter que les erreurs spécifiques des éléments de politique sont présentés comme décrit au paragraphe 4.3 et ne peuvent pas être rapportés par RSVP (en utilisant ce mécanisme). Cependant, ce mécanisme donne un moyen simple, moins sûr pour faire rapport des erreurs génériques de politique. Il est très vraisemblable que les deux seront utilisés de concert de telle sorte qu'un code d'erreur générique soit fourni par RSVP, alors que les erreurs spécifiques d'un élément de politique sont encapsulés dans un objet POLICY_DATA en retour (comme au paragraphe 4.3).

Classe de ERROR_SPEC = 6

Code d'erreur = 02 : Défaillance du contrôle de politique

Valeur d'erreur : 16 bits

0 = ERR_INFO : Rapport d'informations

1 = ERR_WARN :	Avertissement
2 = ERR_UNKNOWN :	Raison inconnue
3 = ERR_REJECT :	Rejet générique de politique
4 = ERR_EXCEED :	Violation de quota ou comptable
5 = ERR_PREEMPT :	Flux préempté
6 = ERR_EXPIRED :	La politique installée précédemment a expiré (non rafraîchie)
7 = ERR_REPLACED :	Les données de politique précédentes ont été remplacées et ont causé le rejet
8 = ERR_MERGE :	Les politiques n'ont pas pu être fusionnées (diffusion groupée)
9 = ERR_PDP :	PDP mort ou non fonctionnel
10 = ERR_SERVER :	Serveur tiers (par exemple, Kerberos) indisponible
11 = ERR_PD_SYNTX :	L'objet POLICY_DATA a une mauvaise syntaxe
12 = ERR_PD_INTGR :	L'objet POLICY_DATA n'a pas passé les essais d'intégrité
13 = ERR_PE_BAD :	L'objet POLICY_ELEMENT a une mauvaise syntaxe
14 = ERR_PD_MISS :	Élément de politique obligatoire manquant (un PE vide dans l'objet PD)
15 = ERR_NO_RSC :	Le PEP n'a plus de ressources pour traiter les politiques.
16 = ERR_RSVP :	Le PDP a rencontré de mauvais objets (ou syntaxe) RSVP
17 = ERR_SERVICE :	Le type de service a été rejeté
18 = ERR_STYLE :	Le style de réservation a été rejeté
19 = ERR_FL_SPEC :	La FlowSpec a été rejetée (trop grande)

Les valeurs entre 2^15 et 2^16-1 peuvent être utilisées pour les valeurs d'erreur de site et/ou de fabricant.

Appendice B : Calcul de INTÉGRITÉ pour les objets POLICY_DATA

La calcul de l'option INTÉGRITÉ se fonde sur les règles établies dans la [RFC2747], avec les modifications suivantes :

Paragraphe 4.1 :

Plutôt que de calculer le résumé pour un message RSVP, le résumé est calculé pour un objet POLICY_DATA de la manière suivante :

(1) L'objet INTÉGRITÉ est inséré à l'endroit approprié de l'objet POLICY_DATA et sa localisation dans le message est mémorisée pour son utilisation ultérieure.

(2) Le PDP, à sa discrétion, et sur la base du PEP/PDP de destination ou d'un autre critère, choisit une clé d'authentification et l'algorithme de hachage à utiliser.

(3) Une copie de l'objet RSVP SESSION est temporairement ajoutée à la fin de l'objet PD (pour les seuls besoins du calcul, sans changer la longueur de l'objet POLICY_DATA). Le champ Fanions de l'objet SESSION est réglé à 0. Cet enchaînement est considéré comme le message pour lequel un résumé est à calculer.

(4) Le reste des étapes du paragraphe 4.1 (de (4) à (9)) reste inchangé pour le calcul sur le message concaténé.

Note : Lorsque le calcul est achevé, l'objet SESSION est ignoré et ne fait pas partie de l'objet POLICY_DATA.

Autres dispositions :
Le traitement d'un objet POLICY_DATA reçu ainsi qu'une mise au défi-réponse de l'objet INTÉGRITÉ au sein de l'objet POLICY_DATA est effectué de la manière décrite dans la [RFC2747]. Ce traitement est l'objet de l'algorithme de calcul modifié comme décrit au début du présent appendice (pour le paragraphe 4.1 de la [RFC2747]).

Déclaration complète de droits de reproduction

processus des normes de l'Internet doivent être suivies, ou si nécessaire pour le traduire dans des langues autres que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Société Internet ou ses successeurs ou ayants droit.

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