

Groupe de travail Réseau
Request for Comments 3859
 Catégorie : En cours de normalisation

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

Profil commun pour Presence (CPP)

Statut de ce mémoire

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

Notice de copyright

Copyright (C) The Internet Society (2004).

Résumé

Au moment de la rédaction de ce document, de nombreux protocoles de détection de présence étaient en usage (dans une grande mesure comme composants de services commerciaux de messagerie instantanée) et peu d'interopérabilité avait été réalisée entre les services sur la base de ces protocoles. La présente spécification définit une sémantique et des formats de données communs pour la détection de présence pour faciliter la création de passerelles entre les services de détection de présence.

Table des Matières

1. Introduction.....	1
2. Terminologie.....	2
3. Service de présence abstrait.....	2
3.1 Généralités sur le service de présence.....	2
3.2 Identification de PRÉSENTITÉ et de OBSERVATEUR.....	4
3.3 Format des informations de présence.....	4
3.4 Service Presence.....	4
4. Considérations pour la sécurité.....	5
5. Considérations pour l'IANA.....	6
6. Contributeurs.....	6
7. Références.....	6
7.1 Références normatives.....	6
7.2 Références pour information.....	6
Appendice A Gabarit d'enregistrement de l'URI PRES auprès de l'IANA.....	6
A.1 Nom du schéma d'URI.....	7
A.2 Syntaxe du schéma d'URI.....	7
A.3 Considérations de codage des caractères.....	7
A.4 Utilisation prévue.....	7
A.5 Applications et/ou protocoles qui utilisent ce nom de schéma d'URI.....	7
A.6 Considérations d'interopérabilité.....	7
A.7 Considérations de sécurité.....	7
A.8 Publications pertinentes.....	7
A.9 Adresse personnelle et de messagerie à contacter pour des informations complémentaires.....	7
A.10 Auteur/contrôleur de changements.....	7
A.11 Applications et/ou protocoles qui utilisent ce nom de schéma d'URI Scheme Name.....	7
Appendice B Questions intéressantes.....	8
B.1 Transposition d'adresse.....	8
B.2 Transposition de route de source.....	8
Appendice C. Remerciements.....	8

1. Introduction

Presence est défini dans la [RFC2778]. Au moment de la rédaction du présent document, de nombreux protocoles de présence sont utilisés (dans une grande mesure, comme composants de services commerciaux de messagerie instantanée), et peu d'interopérabilité a été réalisée entre les services fondés sur ces protocoles. La présente spécification définit une

sémantique et des formats de données pour des services communs de présence pour faciliter la création de passerelles entre les services de présence : un profil commun pour présence (CPP).

Le comportement du service est décrit de façon abstraite en termes d'opérations invoquées entre l'utilisateur et le fournisseur du service. En conséquence, chaque service de présence doit spécifier comment ce comportement est transposé en ses propres interactions de protocole. Le choix d'une stratégie est une affaire locale, pourvu qu'il y ait une relation claire entre les comportements abstraits du service (comme les spécifie le présent mémoire) et la façon dont il est réalisé par un service de présence particulier. Par exemple, une stratégie pourrait transmettre les informations de présence comme des paires de clés/valeurs, un autre pourrait utiliser une représentation binaire compacte, et une troisième pourrait utiliser des conteneurs incorporés.

Les paramètres pour chaque opération sont définis en utilisant une syntaxe abstraite. Bien que la syntaxe spécifie la gamme de valeurs possibles des données, chaque service de présence doit spécifier comment des instances bien formées de la représentation abstraite sont codées en une série de bits concrète.

Afin de fournir un moyen de préserver les caractéristiques de bout en bout (en particulier de sécurité) pour passer à travers les passerelles d'interfonctionnement de présence, la présente spécification fournit aussi des recommandations pour les formats des documents de présence qui pourraient être employés par les protocoles de présence.

2. Terminologie

Dans ce document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP14, RFC 2119 [1] et indiquent les niveaux d'exigence pour les mises en œuvre conformes.

Le présent mémoire utilise le vocabulaire défini dans la [RFC2778]. Les termes tels que CLOS, BOITE AUX LETTRES INSTANTANÉE, PRESENCE, et OUVERT sont utilisés avec la même signification que celle qui y est définie.

Le terme de 'passerelle' utilisé dans le présent document note un élément de réseau chargé de l'interfonctionnement entre divers protocoles de présence. Bien que les protocoles de présence soient eux-mêmes divers, sous le modèle du présent document, ces protocoles peuvent porter une charge utile commune qui est relayée par la passerelle. On peut donc débattre de la question de savoir si ces intermédiaires d'interfonctionnement devraient être appelés des 'passerelles' ou des 'relais' ; pour les besoins du présent document, on les appelle 'passerelles CPP'.

Le terme de 'service de présence' dérive aussi de la RFC2778, mais sa signification change légèrement à cause de l'existence de passerelles dans le modèle CPP. Lorsque un client envoie une opération à un service de présence, ce service peut soit être un point d'extrémité, soit un intermédiaire tel qu'une passerelle CPP – en fait, le client ne devrait pas avoir à connaître auquel il s'adresse, car les réponses de l'un ou l'autre vont paraître les mêmes.

Le présent document définit des opérations et des attributs d'un protocole de présence abstrait. Afin qu'un protocole conforme s'interface avec une passerelle de présence, il doit prendre en charge toutes les opérations décrites dans le présent document (c'est-à-dire que le protocole de présence doit avoir un message ou capacité qui fournit la fonction décrite par toutes les opérations concernées). De même, les attributs définis pour ces opérations doivent correspondre aux informations disponibles dans le protocole de présence afin que le protocole s'interface avec les passerelles définies par la présente spécification. Noter que ces attributs ne fournissent que le minimum d'informations possibles qui ont besoin d'être spécifiées pour l'interopérabilité – dans un protocole de présence, les fonctions qui correspondent aux opérations décrites dans le présent document peuvent contenir des informations supplémentaires qui ne seront pas transposées par CPP.

3. Service de présence abstrait

3.1 Généralités sur le service de présence

Lorsque une application veut souscrire aux informations de présence associées à une PRÉSENTITÉ (afin de recevoir les notifications périodiques d'informations de présence) elle invoque l'opération subscribe, par exemple,

```
+-----+
|         |
|application| -- subscribe ----> |service |
|         |                       | de     |
|         |                       |présence|
+-----+                       +-----+
```

L'opération subscribe a les attributs suivants : observateur, cible, durée, SubscriptID et TransID. Les attributs 'observateur'

et 'cible' identifient respectivement OBSERVATEUR et PRÉSENTITÉ, en utilisant les identifiants décrits au paragraphe 3.2. L'attribut durée spécifie le nombre maximum de secondes pendant lequel la SOUSCRIPTION devrait être active (qui peut être zéro, auquel cas c'est une demande à usage unique pour les informations de présence). L'attribut SubscriptID crée une référence à la SOUSCRIPTION qui est utilisée lors du désabonnement. L'attribut TransID est un identifiant unique utilisé pour corréler l'opération subscribe avec une opération de réponse. Les passerelles devraient être capables de traiter les TransID et les SubscriptID jusqu'à 40 octets de long.

À réception d'une opération subscribe, le service répond immédiatement en invoquant l'opération de réponse qui contient le même TransID, par exemple,

```

+-----+
|         |
|application| <-- réponse ---- |service |
|         |                       | de     |
|         |                       |présence|
+-----+

```

L'opération de réponse a les attributs suivants : état, TransID, et durée. L'attribut 'état' indique si l'opération subscribe a réussi ou échoué. L'attribut TransID de l'opération de réponse correspond au TransID de l'opération subscription à laquelle il répond. L'attribut 'durée' spécifie le nombre de secondes pendant lequel la souscription sera active (qui peut différer de la valeur demandée dans l'opération subscribe).

Si l'opération de réponse indique le succès, le service invoque immédiatement l'opération notifie pour communiquer les informations de présence à l'OBSERVATEUR, par exemple,

```

+-----+
|         |
|application| <---- notifie ---- |service |
|         |                       | de     |
|         |                       |présence|
+-----+

```

L'opération notifie a les attributs suivants : observateur, cible, et TransID. Les valeurs de 'observateur' et de 'cible' sont identiques à celles données dans l'opération subscribe qui déclenchent cette opération notifie. L'attribut TransID est un identifiant unique pour cette notification.

L'opération notifie a aussi un contenu, à savoir PRESENCE INFORMATION. Les détails du contenu sont spécifiés au paragraphe 3.3.

Si le paramètre durée est différent de zéro, alors pour jusqu'à la durée spécifiée, le service invoque l'opération notifie chaque fois qu'il y a un changement dans les informations de présence de la PRÉSENTITÉ. Autrement, exactement une opération notifie est invoquée, réalisant une interrogation à usage unique des informations de présence. Néanmoins, il n'y a pas de réponse de l'application à l'opération notifie (c'est-à-dire, l'application n'invoque pas une opération de réponse lorsque une opération notifie survient) définie dans CPP.

L'application peut annuler prématurément une souscription en invoquant à nouveau l'opération subscribe (comme décrit ci-dessus) avec une durée de 0 et le même SubscriptID que dans l'opération subscribe d'origine, par exemple,

```

+-----+
|         |
|application| -- subscribe 0 ---> |service |
|         |                       | de     |
|         |                       |présence|
+-----+

```

Noter qu'une opération notifie sera invoquée lorsque une souscription est annulée prématurément de cette façon ; cette notification peut être annulée par l'observateur.

Le service répond immédiatement en invoquant l'opération de réponse contenant le même TransID ; par exemple,

```

+-----+
|         |
|application| <--- réponse ----> |service |
|         |                       | de     |
|         |                       |présence|
+-----+

```

Noter que la présente spécification suppose que les protocoles de présence conformes à CPP fournissent une livraison fiable de messages ; il n'y a pas de dispositions d'assurance de livraison de message de couche application dans la présente spécification.

3.2 Identification de PRÉSENTITÉ et de OBSERVATEUR

Une PRÉSENTITÉ est spécifiée en utilisant le schéma d'URI PRES, qui est décrit plus en détails dans l'Appendice A. Un exemple serait : "pres:fred@exemple.com"

Un OBSERVATEUR s'identifie lui-même de la même manière qu'une PRÉSENTITÉ ; c'est-à-dire, avec un URI pres.

3.2.1 Résolution d'adresse

Un client de service de présence détermine le prochain bond pour transmettre une opération en résolvant la portion de nom de domaine de la destination du service. Les mises en œuvre conformes DEVRAIENT suivre les lignes directrices pour le déréférencement des URI données dans la [RFC3861].

3.3 Format des informations de présence

La présente spécification définit un mécanisme abstrait d'interopérabilité pour les protocoles de présence; la définition du contenu de message donnée ici relève de la sémantique plutôt que de la syntaxe. Cependant, certaines propriétés importantes pour l'interopérabilité ne peuvent être fournies que si un format commun de bout en bout pour la présence est employé par les protocoles de présence qui interopèrent, en particulier par rapport à la sécurité. Afin de conserver les propriétés de sécurité de bout en bout, les applications qui envoient des opérations de notification à travers une passerelle CPP DOIVENT prendre en charge le format défini dans PIDF [RFC3863]. Les applications PEUVENT prendre en charge d'autres formats de contenu.

Les passerelles CPP DOIVENT être capables de relayer le corps d'une opération de notification entre les protocoles de présence pris en charge sans avoir besoin de modifier ou inspecter le contenu.

3.4 Service Presence

Une mise en œuvre du service doit conserver les informations à la fois sur la présence et sur les opérations continues (comme les notifications périodiques) dans une mémorisation persistante.

Noter que l'attribut abonnement-identifiant utilisé par l'opération subscribe (*s'abonner*) est potentiellement de longue durée. En conséquence, les valeurs générées pour ce paramètre devraient être uniques sur une durée significative. Le paramètre SubscriptID devrait être intrinsèquement unique au monde dans la durée, et pas simplement unique parmi les opérations envoyées de ou vers un OBSERVATEUR et PRÉSENTITÉ particulier.

3.4.1 Opération Subscribe

Lorsque une application veut s'abonner aux informations de présence associées à une PRÉSENTITÉ, elle invoque l'opération subscribe.

Lorsque le service est informé de l'opération subscribe, il effectue les étapes suivantes :

1. Si le paramètre observateur ou cible ne se réfère pas à une PRÉSENTITÉ valide, une opération de réponse ayant l'état de "échec" est invoquée.
2. Si le contrôle d'accès ne permet pas à l'application de demander cette opération, une opération de réponse ayant l'état de "échec" est invoquée.
3. Si le paramètre durée est différent de zéro, et si les paramètres observateur et cible se réfèrent à une opération subscribe en cours pour l'application, une opération de réponse ayant l'état de "échec" est invoquée.
4. Autrement, si le service est capable de réussir à livrer le message :
 - Une opération réponse ayant l'état de "succès" est immédiatement invoquée. (Si le service choisit une durée différente pour l'abonnement, elle transporte alors cette information dans l'opération de réponse.)
 - Une opération notifie, correspondant aux informations de présence de la cible est immédiatement invoquée pour l(observateur.
 - Pour jusqu'à la quantité de temps indiquée par le paramètre durée de l'opération notifie (mesurée à partir du moment où l'opération d'abonnement a été reçue) et les informations de présence de la cible changent, et si le contrôle d'accès le permet, une opération notifie est invoquée pour l'observateur.

Noter que si le paramètre durée a la valeur zéro, l'opération d'abonnement fait alors une interrogation à usage unique des

informations de présence. En conséquence, la dernière étape ci-dessus (notifications continues pour la durée de l'abonnement) ne se fait pas.

Lorsque le service invoque une opération de réponse par suite de ce traitement, le paramètre transID est identique à la valeur qui se trouve dans l'opération d'abonnement invoquée par l'application.

3.4.2 Opération Notifie

Le service invoque l'opération notifie chaque fois que changent les opérations de présence associées à une PRÉSENTITÉ et qu'il y a des abonnés qui demandent des notifications pour cette PRÉSENTITÉ.

Il n'y a pas de réponse d'application à l'opération notifie.

3.4.3 Opération Subscribe (avec durée zéro)

Lorsque une application veut terminer un abonnement, elle produit un SUBSCRIBE 0 avec le SubscriptID d'un abonnement existant. Noter qu'une opération notifie sera invoquée par la présentité lorsque un abonnement est annulé de cette façon ; cette notification peut être supprimée par l'observateur. Il n'y a pas d'opération UNSUBSCRIBE indépendante.

Lorsque une application veut demander directement que des informations de présence soient fournies immédiatement sans initier d'abonnement persistant, elle produit un SUBSCRIBE 0 avec un nouveau SubscriptID. Il n'y a pas d'opération FETCH (*aller chercher*) indépendante.

4. Considérations pour la sécurité

Les considérations détaillées de sécurité pour les protocoles de présence sont données dans la [RFC2779] (en particulier, les exigences figurent dans les paragraphes 5.1 à 5.3 avec un exposé des motivations en 8.2).

CPP définit une fonction d'interopérabilité qui est employée par les passerelles entre les protocoles de présence. Les passerelles CPP DOIVENT se conformer aux exigences minimum de sécurité des protocoles de présence avec lesquels elles s'interfacent.

L'introduction de passerelles au modèle de sécurité de présence dans la RFC2779 introduit aussi de nouveaux risques. Les propriétés de sécurité de bout en bout (en particulier la confidentialité et l'intégrité) entre les présentités et les observateurs qui s'interfacent à travers une passerelle CPP ne peuvent être fournies que si un format de présence commun (tel que celui décrit dans la [RFC3863]) est pris en charge par les protocoles qui s'interfacent avec la passerelle CPP.

Lorsque la sécurité de bout en bout est exigée, l'opération notifie DOIT utiliser PIDF, et DOIT sécuriser le corps MIME PIDF avec S/MIME [RFC3851], avec le chiffrement (CMS EnvelopeData) et/ou des signatures S/MIME (CMS SignedData).

Les algorithmes S/MIME sont établis par CMS [RFC3852]. L'algorithme AES [RFC3565] devrait être préféré, car on pense qu'il convient le mieux aux capacités de nombreuses plateformes. Les mises en œuvre PEUVENT utiliser AES comme algorithme de chiffrement, mais il est EXIGÉ qu'elle prennent seulement en charge les algorithmes de base rendus obligatoires par S/MIME et CMS.

Lorsque des URI PRES sont utilisés dans les protocoles de présence, ils transportent l'identité des observateurs et/ou des présentités. Les certificats qui sont utilisés pour les opérations de présence S/MIME DEVRAIENT, pour les besoins de l'intégrité de référence, contenir un champ subjectAltName contenant l'URI PRES de leur sujet. Noter que de tels certificats peuvent aussi contenir d'autres identifiants, y compris ceux qui sont spécifiques de protocoles de présence particuliers. Pour faciliter encore l'interopérabilité des services de présence sécurisés à travers les passerelles CPP, les usagers et les fournisseurs de services sont invités à employer pour les certificats des ancres de confiance largement acceptées plutôt que des ancres de confiance spécifiques d'un service de présence ou fournisseur particulier.

Dans certains cas, des services de présence anonymes peuvent être souhaités. Une telle facilité sort du domaine d'application de la présente spécification.

5. Considérations pour l'IANA

L'IANA a alloué le schéma d'URT "pres".

Le schéma d'URI Presence (PRES) désigne une ressource Internet, à savoir PRESENTITY ou WATCHER.

La syntaxe d'un URI PRES est donnée en Appendice A.

6. Contributeurs

Dave Crocker a édité les versions antérieures de ce document.

Les personnes suivantes ont apporté des textes de contributions substantiels à ce document :

Athanasios Diacakis (thanos.diacakis@openwave.com)
Florencio Mazzoldi (flo@networkprojects.com)
Christian Huitema (huitema@microsoft.com)
Graham Klyne (gk@ninebynine.org)
Jonathan Rosenberg (jdrosen@dynamicsoft.com)
Robert Sparks (rsparks@dynamicsoft.com)
Hiroyasu Sugano (suga@flab.fujitsu.co.jp)

7. Références

7.1 Références normatives

- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.
- [RFC2396] T. Berners-Lee, R. Fielding et L. Masinter, "Identifiants de ressource uniformes (URI) : Syntaxe générique", août 1998. (*Obsolète, voir RFC3986*)
- [RFC2778] M. Day, J. Rosenberg et H. Sugano, "[Modèle pour Presence et la messagerie instantanée](#)", février 2000.
- [RFC2779] M. Day et autres, "[Exigences des protocoles Messagerie instantanée / Presence](#)", février 2000. (*Information*)
- [RFC2822] P. Resnick, "[Format de message Internet](#)", avril 2001. (*Remplace la RFC0822, STD 11, Remplacée par RFC5322*)
- [RFC2846] C. Allocchio, "Extensions d'élément d'adresse GSTN dans les services de messagerie électronique", juin 2000. (*MàJ par RFC3191, RFC3192*) (*P.S.*)
- [RFC3851] B. Ramsdell, "Spécification du message d'extensions de messagerie Internet multi-objets/sécurisé (S/MIME) version 3.1", juillet 2004. (*Remplacée par RFC5751*)
- [RFC3852] R. Housley, "Syntaxe de message cryptographique (CMS)", juillet 2004. (*Remplacée par la RFC5652*)
- [RFC3861] J. Peterson, "[Résolution d'adresse pour la messagerie](#) instantanée et les services de présence", août 2004. (*P.S.*)
- [RFC3863] H. Sugano et autres, "Format des [données d'information de présence](#) (PIDF)", août 2004.

7.2 Références pour information

- [RFC3565] J. Schaad, "[Utilisation de l'algorithme de chiffrement](#) de la norme de chiffrement évolué (AES) dans la syntaxe de message cryptographique (CMS)", juillet 2003. (*P.S.*)

Appendice A Gabarit d'enregistrement de l'URI PRES auprès de l'IANA

Cette section donne les informations pour enregistrer l'URI de présence pres.:

A.1 Nom du schéma d'URI

pres

A.2 Syntaxe du schéma d'URI

La syntaxe suit celle qui existe pour l'URI mailto: spécifiée dans la RFC2368. L'ABNF est :

```

PRES-URI    = "pres:" [ à ] [ en-têtes ]
à           = boîte-aux-lettres
en-têtes    = "?" en-tête *( "&" en-tête )
en-tête     = hnom "=" hvaleur
hnom        = *uric
hvaleur     = *uric

```

Ici, le symbole "boîte-aux-lettres" représente un nom codé de boîte-aux-lettres comme défini dans la [RFC2822], et le symbole "uric" note tout caractère valide dans un URL (défini dans la [RFC2396]).

A.3 Considérations de codage des caractères

La représentation de jeux de caractères non ASCII dans les chaîne de partie locale est limitée aux méthodes standard fournies comme extensions à la [RFC2822].

A.4 Utilisation prévue

L'utilisation de l'URI pres: suit de près celle de l'URI mailto:. C'est-à-dire que l'invocation d'un URI PRES va causer le lancement de l'application de messagerie instantanée de l'utilisateur, avec l'adresse de destination et les en-têtes de message remplis conformément aux informations fournies dans l'URI.

A.5 Applications et/ou protocoles qui utilisent ce nom de schéma d'URI

Il est prévu que les protocoles conformes à la RFC2779, et qui satisfont aux exigences d'interopérabilité spécifiées ici, utiliseront ce nom de schéma d'URI.

A.6 Considérations d'interopérabilité

Le protocole d'échange sous-jacent utilisé pour envoyer un message instantané peut varier d'un service à l'autre. Donc l'interopérabilité complète, à l'échelle de l'Internet, ne peut être garantie. Cependant, un service conforme à la présente spécification permet aux passerelles de réaliser une interopérabilité suffisante pour les exigences de la RFC2779.

A.7 Considérations de sécurité

Voir la Section 4.

A.8 Publications pertinentes

RFC 2779, RFC 2778

A.9 Adresse personnelle et de messagerie à contacter pour des informations complémentaires

Jon Peterson [mailto:jon.peterson@neustar.biz]

A.10 Auteur/contrôleur de changements

Ce schéma est enregistré dans l'arborescence de l'IETF. À ce titre, l'IETF assure le contrôle des changements.

A.11 Applications et/ou protocoles qui utilisent ce nom de schéma d'URI Scheme Name

Service de messagerie instantanée, service de présence.

Appendice B Questions intéressantes

Le présent appendice expose brièvement des questions qui peuvent être intéressantes lors de la conception d'une passerelle d'inter fonctionnement.

B.1 Transposition d'adresse

Lors de la transposition du service décrit dans le présent mémoire, les transpositions qui placent des informations spéciales dans la partie locale im: address DOIVENT utiliser la métasyntaxe définie dans la [RFC2846].

B.2 Transposition de route de source

La technique de transposition la plus facile est une forme d'acheminement de source qui est habituellement la moins familière aux humains qui doivent entrer la chaîne au clavier. L'acheminement de source a aussi une longue histoire de problèmes de fonctionnement.

L'utilisation de l'acheminement de source pour les échanges entre différents services se fait par une transformation qui place la chaîne entière d'adresse d'origine dans la partie locale im: address et désigne la passerelle dans la partie domaine.

Par exemple, si la destination INSTANT INBOX est "pepp://example.com/fred", alors, après avoir effectué les conversions de caractères nécessaires, la transposition résultante est :

```
im:pepp=example.com/fred@relay-domain
```

où "relay-domain" est déduit des informations de configuration locale.

L'expérience montre qu'il est largement préférable de cacher – si possible – cette transposition aux utilisateurs finaux, le logiciel sous-jacent devrait effectuer automatiquement la transposition.

Appendice C. Remerciements

L'auteur tient à remercier John Ramsdell de ses commentaires, de ses suggestions et de son enthousiasme. Merci à Derek Atkins pour ses corrections rédactionnelles.

Adresse de l'auteur

Jon Peterson
NeuStar, Inc.
1800 Sutter St
Suite 570
Concord, CA 94520
US
téléphone : +1 925/363-8720
mél : jon.peterson@neustar.biz

Déclaration de copyright

Copyright (C) The Internet Society (2004)

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

Le présent document et les informations qui y sont 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, le IETF TRUST et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur 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 assuré par la Internet Society.