Groupe de travail Réseau
Request for Comments: 3459
RFC mise à jour : 3204
Catégorie : En cours de normalisation

E. Burger, SnowShore Networks
janvier 2003

Traduction Claude Brière de L'Isle

Paramètre Contenu critique pour les extensions de messagerie Internet multi-objets (MIME)

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 (2003). Tous droits réservés

Résumé
Le présent document décrit l'utilisation d'un mécanisme pour identifier les parties de corps qu'un envoyeur estime critiques dans un message Internet multi-part. Le mécanisme décrit est un paramètre de Content-Disposition, comme décrit par la [RFC3204].

En sachant quelles parties d'un message l'envoyeur estime critiques, une passerelle de contenu peut traiter intelligemment les messages multi-part lorsque elle fournit des services de passerelle aux systèmes de moindres capacités. Le contenu critique peut aider une passerelle de contenu à décider quelles parties transmettre. Il peut indiquer avec quelle insistance une passerelle devrait essayer de livrer une partie de corps. Il peut aider la passerelle à prendre des parties de corps qu'on peut éliminer en silence en toute sécurité lorsque un système de moindre capacités reçoit un message. De plus, le contenu critique peut aider la passerelle à choisir la stratégie de notification pour le système receveur. De même, si l'envoyeur s'attend à ce que la destination effectue un certain traitement sur une partie de corps, le contenu critique permet à l'envoyeur de marquer les parties de corps que le receveur doit traiter.

Table des Matières

1. Conventions utilisées dans ce document

Le présent document se réfère de façon générique à l'envoyeur d'un message au masculin (il/lui/son) et au receveur du message au féminin (elle/sa). Cette convention n'a qu'un aspect pratique et ne fait aucune hypothèse sur le genre d'un envoyeur ou receveur de message.

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

Le mot "EXIGE" dans ce document ne suit pas la définition de la RFC 2119. Cela parce que le présent document définit un paramètre nommé "REQUIRED" *(exigé)*. Il n'y a pas d'exigence dans ce document qui soit "REQUIRED", afin qu'il n'y ait pas de confusion.

Dans ce document, "l'agent envoyeur" est celui qui génère le message. Il pourrait être un agent d'utilisateur de messagerie (MUA, *mail user agent*) pour un message Internet, ou un client d'agent d'utilisateur (UAC, *User Agent Client*) pour un message SIP [RFC3261]. Le "point d'extrémité" est l'appareil récepteur, de moindre capacité que l'agent envoyeur.

Note : Les notes, comme celle-ci, donnent des informations non essentielles supplémentaires que le lecteur peut sauter sans rien manquer d'essentiel. Le principal objet de ces notes non essentielles est de donner des informations sur les raisons du présent document, ou de replacer ce document dans le propre contexte ou évolution historique. Les lecteurs dont le seul objet est de construire une mise en œuvre conforme peuvent sauter de telles informations. Cependant, elles peuvent être utiles à ceux qui souhaitent comprendre pourquoi ont été faits certains choix de conception.

2. Introduction

La spécification de Contenu critique est courte et compacte. Pour le bénéfice des développeurs, la spécification vient en premier, les raisons suivent.

Un concept qu'une mise en œuvre doit comprendre est celui de passerelle de contenu. La Section 10 décrit la passerelle de contenu. En bref, une passerelle de contenu a connaissance des capacités du système receveur. La passerelle de contenu passe au système receveur les messages qu'il peut traiter, rendre ou mémoriser. La passerelle de contenu peut modifier un message, par exemple en supprimant les parties de corps non restituables ou non mémorisables, pour la livraison au système receveur. Finalement, la passerelle de contenu peut rejeter un message que le système receveur ne peut pas traiter.

Bien que le traitement du contenu critique ne soit pas un service marginal à connexion libre (OPES, *Open Pluggable Edge*

Service) la machinerie de protocole décrite dans le présent document satisfait à toutes les exigences de l'IAB pour un OPES telles qu'établies par la [RFC3238]. La Section 14 décrit cela en détail. En particulier, à la différence de la situation actuelle où les passerelles de contenu modifient en silence les messages, ou ont des règles abstraites pour les modifier (voir les règles de transformation de contenu dans VPIM, par exemple) le mécanisme de contenu critique permet à l'utilisateur envoyeur d'indiquer explicitement le traitement de contenu désiré par la passerelle de contenu.

Note : Le présent document met à jour la [RFC3204] pour séparer le paramètre Handling *(traitement)* du mécanisme de transport ISUP/QSIG. Le protocole décrit ici est identique en fonctionnalité à la RFC3204 par rapport à SIP. De futures versions de la RFC3204 devraient faire référence au présent document pour le paramètre Handling , car il est orthogonal au tunnelage de signalisation.

3. Paramètre Handling

Le paramètre Handling est un paramètre de disposition de contenu [RFC2183] qui est inséré par l'agent envoyeur pour indiquer à la passerelle de contenu si elle doit prendre en considération la partie de corps marquée comme critique.

Une partie de corps REQUIRED est celle que l'envoyeur exige que le système receveur lui livre pour considérer le message comme livré.

Une partie de corps OPTIONAL *(facultatif)* est celle dont l'envoyeur ne se soucie pas que le système receveur la livre ou non. Une passerelle de contenu peut éliminer en silence une telle partie de corps si le système receveur ne peut pas la livrer.

Les termes "entité" et "partie de corps" ont la signification définie dans la [RFC2183].

3.1 REQUIRED

"Handling=REQUIRED" signifie que cette partie de corps est critique pour l'envoyeur.

Si la passerelle de contenu ne peut pas passer une partie de corps marquée REQUIRED, le message entier a alors échoué. Dans ce cas, la passerelle de contenu DOIT prendre l'action appropriée sur échec.

Note : On dit "action appropriée" parce que l'envoyeur peut avoir supprimé toutes les notifications. Dans ce cas, l'action appropriée est d'éliminer le message en silence. De plus, comme paramètre MIME général, la partie de corps MIME peut n'être pas dans un message Internet. De plus, dans le cas de SIP, la notification appropriée est un code de retour d'état, et non une notification de livraison.

3.2 OPTIONAL

"Handling=OPTIONAL" signifie que l'envoyeur ne se soucie pas des rapports de notification pour cette partie de corps.

Si la passerelle de contenu ne peut pas passer une partie de corps marquée OPTIONAL, le système receveur peut éliminer en silence cette partie de corps. Le système receveur NE DOIT PAS retourner un échec de livraison, sauf si des parties marquées REQUIRED ont aussi échoué.

3.3 Valeurs par défaut

La valeur par défaut de Handling pour une certaine partie de corps est REQUIRED. Cela permet au mécanisme de notification existant de fonctionner pour les agents d'envoi qui ne connaissent pas l'entité de notification de contenu. Toutes les parties de corps sont critiques, parce que elles ont le marquage par défaut de REQUIRED.

Note : Dans le cas de la messagerie Internet, le traitement du contenu critique est une fonction de la passerelle de contenu et non de l'agent de transfert de messagerie (MTA, *mail transfer agent*) ou de l'agent d'utilisateur (UA, *user agent*). Souvent, l'entité qui effectue le traitement de passerelle de contenu est l'UA receveur. Cependant, dans ce cas, l'UA agit comme passerelle de contenu. Donc, l'action par défaut, pour tout agent d'utilisateur conforme à la disposition de contenu de la [RFC2183] d'ignorer les paramètres de disposition non reconnus, assure que ce mécanisme est compatible avec l'architecture de l'Internet.

Note : Ce paramètre est pleinement rétro compatible et fonctionne comme prévu pour la messagerie Internet et SIP.

Note : Certaines mises en œuvre de VPIMv2 peuvent recevoir des messages électroniques arbitraires de l'Internet.

Cependant, ces systèmes agissent réellement comme des systèmes de messagerie vocale Internet. Dans ce cas, on s'attendrait à ce que la mise en œuvre fournisse la sémantique de la messagerie vocale Internet aux messages vocaux Internet.

3.4 Autres valeurs

La passerelle de contenu DOIT traiter les valeurs non reconnues comme REQUIRED. C'est pour assurer la rétro compatibilité avec de futurs usages de l'entité Content-Criticality.

Note : Une nouvelle valeur possible est IMPORTANT. Une partie de corps marquée IMPORTANT est quelque chose que l'envoyeur veut que le receveur obtienne, mais ne voudrait que le message soir complètement rejeté si la partie de corps marquée IMPORTANT échoue, mais il veut la notification de l'échec. Cependant, comme il n'y a pas de mise en œuvre de IMPORTANT, cela n'a pas d'importance pour cette version du présent document.

4. Présentation de la syntaxe

Le format de la syntaxe collectée est conforme à l'ABNF de la [RFC2234]. Noter que selon la [RFC2183], le paramètre de disposition de contenu HANDLING n'est pas sensible à la casse, pas plus que le type de notification.

"handling" "=" notification-type CRLF

notification-type = "REQUIRED" / "OPTIONAL" / other-handling / generic-param

other-handling = jeton

5. Notification

Une application évidente du contenu critique est de générer une notification de (non) livraison dans l'environnement de la messagerie Internet. Si la valeur du champ est OPTIONAL, la passerelle de contenu NE DOIT PAS générer de notification. Si la valeur du champ est REQUIRED, la passerelle de contenu PEUT générer une notification, sur la base des mécanismes normaux de demande de notification. Les mécanismes normaux de demande de notification incluent de spécifier le paramètre NOTIFY à la commande RCPT de SMTP [RFC3461] et l'en-tête Disposition-Notification-To [RFC3464].

Dans SIP, toutes les demandes ont des réponses. Ces réponses fournissent la notification dans le code d'état de la réponse. Pour le cas de la [RFC3204], une passerelle de contenu génère une réponse 415 (Type de support non pris en charge) si le champ est REQUIRED.

Si le système envoyeur demande une notification, et si une partie REQUIRED échoue, la passerelle de contenu DOIT générer une notification pour le message entier. À l'inverse, si la passerelle ne peut pas passer une partie de corps marquée OPTIONAL, la passerelle NE DOIT PAS générer de notification.

Note : Cela implique que la passerelle de contenu doit examiner le message entier pour déterminer si il a besoin de générer une notification. Cependant, la passerelle de contenu n'a pas besoin d'examiner le message si elle sait qu'elle peut mémoriser et transmettre tous les types de supports. Dit autrement, les MTA ou passerelles de la messagerie Internet peuvent, par défaut, traiter tout type arbitraire encapsulé dans MIME. D'un autre côté, certains systèmes de messagerie vocale ne peuvent pas mémoriser du tout des pièces jointes binaires, comme une application/ms-word. La passerelle de contenu de messagerie vocale, dans cet exemple, examinerait dans tous les cas les parties de corps non restituables.

5.1 Génération de DSN ou de MDN

La passerelle de contenu génère une notification d'état de livraison (DSN, *delivery status notification*) [RFC3464] si elle fonctionne comme passerelle. La passerelle de contenu génère une notification de disposition de message (MDN, *Message Disposition Notification*) [RFC2298] si elle fonctionne comme agent d'utilisateur de messagerie. La Section 6 décrit les modes de fonctionnement d'une passerelle de contenu. En bref, si il y a un MTA qui "livre" le message à la passerelle de contenu pour traitement, le MTA prend la responsabilité du traitement de la DSN. Dans ce cas, la seule option disponible pour la passerelle de contenu est de générer des MDN. Si la passerelle de contenu fonctionne comme un MTA, elle génère alors des DSN. La génération de DSN est l'option préférée.

Si la passerelle de contenu fait partie d'un point d'extrémité SIP, elle génère alors le code de réponse de succès ou d'erreur approprié.

5.2 Résumé

Le tableau suivant résume les actions attendues d'une passerelle de contenu conforme.

Note : Ce paragraphe est normatif : il suggère ce qu'une passerelle de contenu devrait mettre en DSN ou MDN.

Note : Dans le cas de SIP, ce paragraphe est pour information. Voir dans la [RFC3204] l'ensemble des actions normatives en cas d'échec.

Tableau 1 – Actions attendues

	L'UA envoyeur a marqué la partie de corps	
	REQUIRED	OPTIONAL
La partie de corps est livrable	Action appropriée	ignorer
La partie de corps n'est pas livrable	Échec du message entier	ignorer

"Action appropriée" est l'action que la passerelle de contenu prendra selon le contexte d'exécution. Par exemple, si un envoyeur demande le retour d'un accusé de réception et si le receveur lit une partie de corps HANDLING, L'UA receveur doit générer la MDN appropriée (selon les règles de la MDN). De même, si la passerelle de contenu ne peut pas livrer la partie de corps et si la partie de corps est critique, la passerelle de contenu génèrera la DSN ou MDN appropriée.

"Optional" signifie que la passerelle de contenu ignore la disposition de la partie de corps. La passerelle de contenu traite le message comme si la partie de corps n'était pas présente dans le message.

6. Contenu signé

La [RFC1847] décrit comment appliquer les signatures numériques à une partie de corps MIME. En bref, une partie de corps multipart/signed encapsule la partie de corps intéressante, ou "l'objet contenu", dans une partie de corps MIME et les informations de contrôle nécessaires pour vérifier l'objet, ou le "protocole" dans le lexique de la [RFC1847], dans une seconde partie de corps MIME. Voici un exemple tiré de la RFC1847.

```
Content-Type: multipart/signed; protocol="TYPE/STYPE";
      micalg="MICALG"; boundary="Signed Boundary"

--Signed Boundary
Content-Type: text/plain; charset="us-ascii"
```

C'est du texte à signer mais cela pourrait être n'importe quel type de données, étiqueté en conséquence, évidement.

```
--Signed Boundary
Content-Type: TYPE/STYPE
```

Les informations de contrôle pour le protocole "TYPE/STYPE" se trouveraient ici.

```
--Signed Boundary--
```

Figure 1 - Type MIME Contenu signé

Il y a trois endroits où on peut placer l'indicateur de caractère critique d'une partie de corps multipart/signed. On pourrait marquer l'objet multipart/signed, l'objet contenu, l'objet de contrôle, ou toute combinaison des trois.

La disposition des parties de corps REQUIRED suit les lignes directrices de la [RFC2480].

Un indicateur de contenu critique sur une partie de corps multipart/signed signifie que l'envoyeur exige une vraie vérification de signature de bout en bout. Donc, la passerelle a besoin de passer les objets inclus intacts. Si le système ou le réseau de moindres capacités ne peut pas faire la vérification de signature et si l'inclusion signée est REQUIRED, la passerelle DOIT rejeter le message.

Un indicateur de contenu critique sur une signature signifie soit que le point d'extrémité receveur doit être capable de faire la vérification de la signature, soit que la passerelle doit vérifier la signature avant de transmettre le message. Si le contenu échoue à la vérification, la passerelle DOIT rejeter le message.

Un indicateur de contenu critique sur le matériel inclus spécifie si ce matériel est critique pour le message pris dans son entier. Si la signature est marquée OPTIONAL et si le matériel inclus est marqué REQUIRED, la passerelle PEUT supprimer les informations de signature si le système ou réseau de moindres capacités ne peut pas faire la vérification de signature. Cependant, si possible, on RECOMMANDE fortement que les passerelles fassent la vérification de signature et indiquent les falsifications au receveur.

7. Contenu chiffré

La [RFC1847] décrit comment chiffrer une partie de corps MIME. En bref, une partie de corps multipart/encrypted encapsule les informations de contrôle ("protocole" dans le lexique de la RFC1847) pour l'objet chiffré et la seconde contenant les données chiffrées (application/octet-stream). Voici un exemple tiré de la RFC1847.

```
Content-Type: multipart/encrypted; protocol="TYPE/STYPE";
      boundary="Encrypted Boundary"

--Encrypted Boundary
Content-Type: TYPE/STYPE
```

Les informations de contrôle pour le protocole "TYPE/STYPE" se trouveraient ici.

```
--Encrypted Boundary
Content-Type: application/octet-stream

Content-Type: text/plain; charset="us-ascii"
```

Tout le texte qui viendrait ici, y compris les en-têtes, serait illisible car il aurait été chiffré par le protocole "TYPE/STYPE". Aussi, ces données chiffrées pourraient être de tout type de données, étiqueté en conséquence, évidement.

```
--Encrypted Boundary--
```

On peut raisonnablement placer un indicateur de contenu critique à la lisière de la partie de corps chiffrée (multipart/encrypted). Si le point d'extrémité peut déchiffrer le message, la passerelle transmet alors la partie de corps dans son intégralité.

Si on marque l'objet de contrôle comme REQUIRED, l'UA envoyeur exige alors le chiffrement de bout en bout. Si le point d'extrémité ne peut pas déchiffrer le message, la passerelle DOIT alors rejeter le message.

Si l'objet de contrôle est marqué OPTIONAL, si le point d'extrémité ne peut pas déchiffrer le message, et si la passerelle peut déchiffrer le message, la passerelle PEUT alors déchiffrer le message et le transmettre en clair. L'usager envoyeur a explicitement donné la permission à la passerelle de déchiffrer le message en marquant l'objet de contrôle OPTIONAL. On se rappelle que l'indication par défaut pour les parties de corps MIME est REQUIRED. Donc, si l'usager n'agit pas explicitement, la passerelle de contenu va supposer que l'usager souhaite le chiffrement de bout en bout.

Marquer le contenu chiffré sans marquer le contenant chiffré est problématique. Parce que la passerelle doit déchiffrer les données chiffrées pour retrouver l'en-tête. Cependant, il est peu probable que la passerelle ait la capacité (c'est-à-dire, les clés) pour déchiffrer les données chiffrées. Si un UA envoyeur souhaite marquer les données chiffrées comme non REQUIRED, l'UA envoyeur DOIT marquer le contenu chiffré comme non REQUIRED. Il est clair que si l'UA envoyeur marque le contenu chiffré comme REQUIRED, la passerelle va appliquer les règles de traitement de REQUIRED. De plus, si l'UA envoyeur ne marque pas le contenu chiffré comme REQUIRED, la passerelle, sauf si elle peut déchiffrer les données, va traiter le contenu chiffré comme REQUIRED. Cela se produit parce que les passerelles traitent toujours le contenu non marqué comme REQUIRED (voir le paragraphe 3.3).

8. Code d'état

L'indication de contenu critique, par elle-même, ne garantit aucune notification. La notification suit les règles décrites dans les [RFC3261], [RFC3461], et [RFC3464].

Note : Le contenu des DSN ou MDN réelles sort du domaine d'application du présent document. Il spécifie seulement comment marquer une partie de corps critique. D'un autre côté, on envisage bien des contenus intelligents de DSN et de MDN. Par exemple, les DSN devraient inclure le code d'échec approprié comme énumérés dans la [RFC3463]. De même, les MDN devraient inclure le code d'échec dans le champ de MDN "Échec:".

Si le système receveur doit générer une notification sur la base de son incapacité à restituer ou mémoriser le type de support, la notification devrait utiliser le code d'état 561, "Support non pris en charge", de la [RFC2298].

Pour le cas de SIP, toutes les demandes ont une notification fournie par le message de réponse d'état. Selon la [RFC3204], une passerelle de contenu génère une réponse 415 (Type de support non accepté).

9. Exigences pour Contenu critique

Cette section est informative.

9.1 Besoins

Le besoin d'un mécanisme d'identification de contenu critique apparaît à cause de l'inter-réseautage des systèmes de messagerie de l'Internet avec les systèmes de messagerie qui ne respectent pas pleinement toute la sémantique de la messagerie Internet. De tels systèmes traditionnels ont une capacité limitée à rendre ou mémoriser toutes les parties d'un certain message. Le présent document utilisera le cas d'un système de messagerie Internet qui échange des messages électroniques avec un système traditionnel de messagerie vocale pour illustrer notre propos.

La messagerie électronique a été historiquement centrée sur le texte. Des extensions telles que MIME [RFC2045] permettent aux agents d'utilisateur d'envoyer et recevoir des messages multi-parties multimédia. Les types populaires de données multimédia incluent des traitements de textes binaires, des graphiques binaires de traitement d'affaires, de la voix, et de la vidéo.

La messagerie vocale a été historiquement centrée sur l'audio. De nombreux systèmes de messagerie vocale ne rendent que la voix. Des extensions telles que la télécopie permettent au système de messagerie vocale d'envoyer et recevoir des images de télécopie ainsi que de créer des messages multi-part vocaux et de télécopie. Quelques systèmes de messagerie vocale peuvent rendre du texte en utilisant une technologie de conversion de texte en parole ou de texte en télécopie. Bien que théoriquement possible, aucune ne peut aujourd'hui rendre de la vidéo.

Un important aspect de l'échange entre les services de messagerie vocale et les applications de client de messagerie électronique sur ordinateur de bureau est que la capacité de rendu de la plateforme de messagerie vocale est souvent bien moindre que la capacité de rendu du client de messagerie électronique de l'ordinateur. Dans le cas de la messagerie électronique, l'envoyeur s'attend à ce que le destinataire reçoive tous les composants d'un message multimédia. Il en est ainsi même si le receveur ne peut pas rendre toutes les parties de corps. Dans la plupart des cas, le receveur peut soit trouver l'outil de rendu approprié, soit dire à l'envoyeur qu'il ne peut pas lire une certaine pièce jointe.

C'est une question importante. Par définition, un agent d'utilisateur à capacité MIME, conforme à la [RFC2046], va présenter ou rendre disponible toutes les parties de corps au receveur. Cependant, un système de messagerie vocale peut n'être pas capable de mémoriser des objets non vocaux. De plus, le système de messagerie vocale peut n'être pas capable de notifier au receveur qu'il y a des parties du message qui ne sont pas livrables.

L'incapacité du système receveur à rendre une partie de corps est habituellement une défaillance permanente. La retransmission du message ne va pas améliorer la probabilité d'une réussite future de la livraison. Cela s'oppose au cas normal de livraison des données. Les échecs traditionnels de message, comme un message déstructuré ou une liaison défaillante vont bénéficier d'une retransmission.

Cette situation est fondamentalement différente de la messagerie Internet normale. Dans le cas de la messagerie Internet, soit le système livre le message, soit il ne le livre pas. Il n'existe pas de concept d'un système qui livre partiellement un message.

De plus, il y a de nombreuses situations où l'envoyeur ne se soucierait pas que le système n'ait pas livré des parties non critiques d'un message. Par exemple, l'agent d'utilisateur de l'envoyeur peut ajouter à un message des parties de corps qui restent ignorées de l'envoyeur. Si le système receveur a rejeté le message parce qu'il ne pouvait pas rendre une partie de corps cachée, l'envoyeur serait dans la confusion et l'embarras, de façon compréhensible.

Donc, il y a besoin d'une méthode pour indiquer à un agent de transfert de messagerie (MTA, *Mail Transfer Agent*) ou à un agent d'utilisateur (UA, *User Agent*) que l'envoyeur considère des parties d'un message comme critiques. Du point de vue de l'envoyeur, le message ne sera pas considéré comme livré si le système n'a pas livré les parties critiques.

9.2 Approches courantes

Une méthode pour indiquer un contenu critique d'un message est de définir un profil. Le profil définit les règles pour supprimer en silence les parties de corps de message sur la base de la connaissance des capacités de l'UA. En reprenant l'exemple ci-dessus, un profil vocal peut facilement déclarer que les MTA ou les UA peuvent éliminer en silence les données TNEF et considérer quand même le message comme livré avec succès. C'est, en fait, l'approche retenue par VPIMv2 [RFC2421].

Comme un aspect de la question est de décider quand notifier à l'envoyeur que le système ne peut pas livrer une partie d'un message, on pourrait utiliser un mécanisme de notification de non livraison partielle pour indiquer un problème de livraison d'une certaine partie de corps. Cependant, cela exige que l'usager demande une notification de livraison. De plus, l'envoyeur peut ne pas être au courant de parties ajoutées par l'agent d'utilisateur envoyeur. Dans ce cas, une notice de défaillance rendrait perplexe l'envoyeur.

Une méthode de mise en œuvre de remplacement directe pour marquer comme critique une partie de corps est d'utiliser l'entité MIME Critical-Content. Cela a l'avantage que ce caractère critique est une méta information pour la partie de corps. Cependant, les serveurs IMAP en particulier vont avoir besoin soit de mettre Critical-Content dans la méthode BODYSTRUCTURE, soit de créer une nouvelle méthode pour restituer des entités MIME arbitraires. Étant donnée l'expérience de l'essai de faire accepter Content-Location par les fabricants de IMAP, on choisit de ne pas suivre ce chemin.

Ce dont on a besoin est un moyen de faire indiquer par l'envoyeur quelles parties de corps il considère comme critiques. Le mécanisme ne doit pas surcharger l'envoyeur avec des notifications d'échec pour des parties de corps non critiques. Le mécanisme doit se conformer au mécanisme général de demande d'état de notification pour des notifications positives ou négatives. Lorsque il est demandé, le mécanisme doit indiquer à l'envoyeur quand un système receveur ne peut pas livrer une partie de corps critique.

10. Passerelle de contenu

Cette section est informative.

Dans cette section, on utilise la définition qui figure dans la [RFC2156] pour le terme "passerelle".

On utilise pas strictement la définition de la [RFC2821] pour le terme "passerelle". En particulier, la RFC2821 discute d'une passerelle qui ne devrait pas examiner le message lui-même. Une passerelle de la RFC2821 est une passerelle de transport, qui a principalement à voir avec les transformations des informations SMTP.

Une passerelle de contenu est une passerelle qui connecte un premier réseau à un second réseau. Le second réseau a souvent des capacités moindres que le premier réseau. La topologie canonique suit. "[MTA]", entre crochets, signifie un composant facultatif.

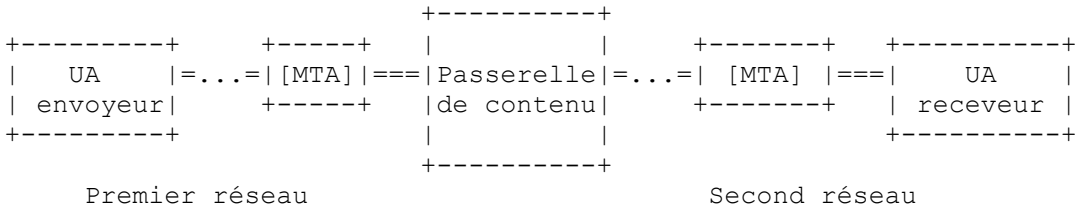

Figure 2 – Topologie de passerelle de contenu

La passerelle de contenu peut être le dernier bond avant le MTA receveur. La passerelle de contenu peut être entre les réseaux, et donc n'être pas le dernier bond avant le MTA receveur. La passerelle de contenu peut être le premier MTA que contacte l'UA envoyeur. Finalement, la passerelle de contenu peut être un composant intégré du MTA receveur.

Pour le cas de SIP, on considère chaque MTA comme un mandataire SIP, l'UA envoyeur comme un client d'agent d'utilisateur SIP, et l'UA receveur comme un serveur d'agent d'utilisateur SIP.

10.1 Passerelle de contenu intégré

Dans cette situation, l'agent d'utilisateur receveur est intégré à la passerelle de contenu. La passerelle de contenu intégrée connaît les capacités de l'agent d'utilisateur. La topologie est la suivante :

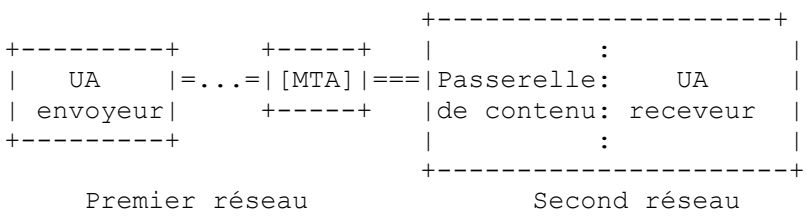

Figure 3 - Passerelle de contenu intégré

Le traitement des objets ISUP et QSIG, comme décrit dans la [RFC3204], est un exemple de passerelle intégrée.

10.2 Réseaux de livraison désagrégée

Un cas extrême, mais qui s'est produit, est celui d'une passerelle de contenu qui se tient derrière le MTA final. Cela arrive lorsque on met en œuvre la passerelle de contenu comme étape de post-traitement d'une livraison normale. Par exemple, on pourrait configurer un système de traitement de messagerie pour qu'il livre le message à une file d'attente ou à un répertoire, et où le processeur de la passerelle de contenu prend le message. Si il y a des directives pour le traitement des DSN, le MTA de livraison va les exécuter. Par exemple, le message pourrait avoir demandé la notification de la réussite de la livraison. Le MTA de livraison qui a mis le message dans la file d'attente va considérer que le message est livré et va donc notifier cela à l'envoyeur. Cependant, le processeur de la passerelle de contenu va alors découvrir que l'UA de réception ne peut pas restituer le message. Dans ce cas, la passerelle de contenu génère une notification de non livraison (NDN, *Non-Delivery Notice*) car c'est la seule option disponible.

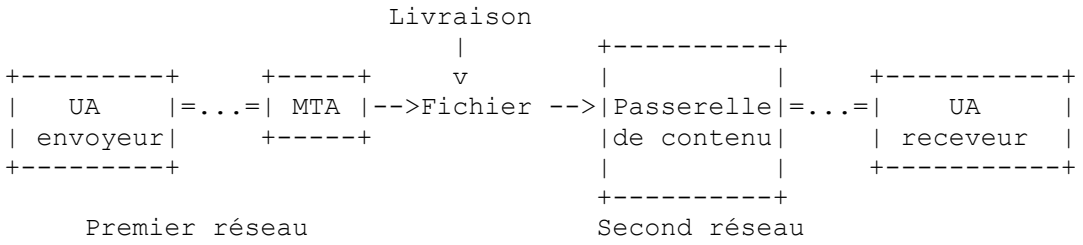

Figure 4 - Réseau de livraison désagrégée

11. Considérations sur la rétro compatibilité

Les DSN exigent ESMTP. Si les MTA sur le chemin de l'UA envoyeur à l'UA receveur ne prennent pas en charge ESMTP, ce MTA va alors rejeter la demande de DSN. De plus, le message va revenir par défaut à la notification sur retard ou échec. Bien que ce ne soit pas idéal, l'envoyeur saura que la DSN n'est pas disponible, et que le contenu critique qui échoue sera notifié.

12. Interactions MIME

12.1 multipart/alternative

Comme il est vrai pour tous les paramètres Content-Disposition, le traitement n'est effectif que pour la solution de remplacement choisie. Si la solution de remplacement choisie a l'indicateur de contenu critique, c'est la solution de remplacement toute entière qui prend le caractère critique indiqué. C'est-à-dire que si la solution de remplacement choisie a HANDLING=OPTIONAL, la passerelle de contenu NE DOIT alors générer aucune notification de livraison.

Note : Cette déclaration montre explicitement que HANDLING outrepasse les mécanismes de demande de DSN et de MDN.

Il est peu probable qu'une solution de remplacement choisie échoue, car la passerelle de contenu est supposée prendre spécifiquement la solution de remplacement parce qu'elle peut la restituer.

Si la solution de remplacement choisie est un message/rfc822 qui incorpore un message multipart MIME ou si la solution de remplacement est elle-même un type multipart MIME, les parties de corps individuelles de niveau supérieur suivent le mécanisme HANDLING décrit dans le présent document.

Note : Cela signifie que le caractère critique d'un message transmis ne va pas affecter les intentions de l'agent de transmission.

12.2 multipart/related

Le caractère critique va assez bien avec la construction multipart/related. Par exemple, considérons un message multipart/related consistant en une fourche de données Macintosh et en une fourche de ressources Macintosh. Pour un document Microsoft Word, la fourche de données va probablement être critique. Le système receveur peut en toute sécurité ignorer la fourche de ressource.

12.3 message/rfc822

Le caractère critique n'affecte que le niveau le plus externe de message ou, dans le cas de multipart/alternative, le niveau le plus externe de la solution de remplacement choisie. Précisément, le système receveur ignore les indicateurs de criticité dans les parties de corps incorporées. Cela évite la situation d'un message transmis qui déclanche ou supprime un rapport non désiré. Cela met simplement en œuvre les procédures décrites dans la [RFC2183].

12.4 multipart/signed

Voir la Section 6.

12.5 multipart/encrypted

Voir la Section 7.

13. Exemples de mise en œuvre

La présente section est une partie informative de la définition de Criticité. On espère qu'elle aide les mises en œuvre à comprendre le mécanisme du traitement de Handling.

On va examiner deux cas. Ce sont comment une passerelle de contenu traite un message et comment une passerelle de contenu désagrégé traite un message.

13.1 Passerelle de contenu

Les passerelles de contenu examinent le contenu d'un message provenant d'un premier réseau avant que la passerelle transmette le message à un second réseau. Pour les besoins de cet exemple, on suppose que le second réseau à moins de capacités que le premier réseau. En particulier, on s'attend à ce qu'il y ait certains types de corps de message que la passerelle ne peut pas passer au second réseau.

Considérons une passerelle entre l'Internet et un service de messages courts de texte uniquement. Un message arrive à travers la passerelle contenant un partie texte et une partie tnef. L'envoyeur marque la partie texte REQUIRED. La passerelle, sachant les capacités du service de messages courts, supprime en silence la partie non critique, tnef, passant le contenu critique au réseau du service de messages courts. Toutes les notifications ultérieures, comme les notices d'échec ou les notices de livraison, suivent les règles normales de notification.

Noter que la passerelle, en supprimant en silence le contenu non critique, peut affecter les schémas propriétaires de corrélation de message. On peut envisager que l'UA envoyeur a inséré une partie de corps pour des besoins de traçage. En supprimant le contenu non critique, la passerelle de contenu va casser ce schéma. Si un UA envoyeur comprend comment marquer le contenu critique, il devrait utiliser les mécanismes standard de l'Internet pour retracer les messages, comme un identifiant de message de la [RFC0822].

Que se passe t-il si aucune partie de corps n'a d'indicateur de contenu critique ? Dans ce cas, le message entier est critique.

Donc, lorsque la passerelle voit la partie tnef, elle va rejeter le message entier, générant une DSN avec un code d'état de 5.6.1, "Support non accepté".

De même, considérons un message en trois parties avec une annotation textuelle (partie 1) à un message vocal (partie 2) avec une vCard [RFC2426] (partie 3). L'envoyeur marque les deux premières parties REQUIRED. Maintenant, supposons que le MTA receveur (passerelle) soit un système seulement vocal, sans même la capacité de mémoriser le texte. Dans ce cas, la passerelle agit comme MTA receveur, et va rejeter le message, générer une DSN avec le code d'état 5.6.1, "Support non accepté".

13.2 Passerelle de contenu désagrégé

Pour cet exemple, on va examiner le traitement d'un message en trois parties. La première partie est une annotation textuelle de la seconde partie, un message audio. La troisième partie est la vCard de l'envoyeur. L'envoyeur marque la première et la seconde parties comme REQUIRED. De plus, l'envoyeur marque le message pour réception lecture.

Pour les besoins de cet exemple, l'interface d'utilisateur téléphonique (TUI, *telephone user interface*) n'effectue pas de conversion de texte en parole. Une TUI est un agent d'utilisateur de messagerie qui utilise les chiffres de touche de tonalité DTMF pour l'entrée et d'audio pour la sortie (affichage).

La TUI est incapable de rendre la première partie du message, la partie texte. De plus, elle est incapable de rendre la troisième partie du message, la partie vCard. Comme l'envoyeur n'a pas marqué la troisième partie du message comme REQUIRED, le système ignore l'échec de la TUI à rendre la troisième partie du message. Cependant, comme l'envoyeur à marqué la première partie REQUIRED, et comme la TUI est incapable de rendre le texte, le message échoue.

Ce qui se passe ensuite dépend de la mise en œuvre. Si la TUI fait partie d'un système unifié de messagerie, une action raisonnable est de conserver le message pour l'usager. L'usager peut accéder au message ultérieurement à partir d'un terminal capable de rendre toutes les parties de corps critiques. Il serait raisonnable pour la TUI de notifier à l'usager ce qu'il en est de la partie de corps non livrable.

Si la TUI fait partie d'un système de messagerie vocale, ou si l'usager n'est pas abonné à un service de transcription de texte en parole, une action raisonnable est que la TUI retourne une MDN avec la disposition "échec" et le modificateur sur échec de "5.6.1 (Support non accepté)".

14. Considérations d'OPES

Le traitement du contenu critique n'est pas un service de la Toile. Cependant, certaine dans la communauté de l'Internet peuvent tirer un parallèle entre les services de la toile qui modifient les contenus et une messagerie électronique, SIP, ou autre service à transport MIME qui modifie le contenu.

Cette section analyse la machinerie du protocole de contenu critique par rapport aux exigences énoncées dans la [RFC3238]. En résumé, le protocole décrit dans le présent document satisfait à toutes les exigences de la RFC3238.

14.1 Considération (2.1) : Consentement unilatéral

C'est le cœur de Contenu critique. Contenu critique permet à l'envoyeur de donner son consentement à la modification du message. Les passerelles qui se conforment au présent document vont s'assurer qu'elles ne modifient que les messages dont l'envoyeur a donné son consentement à leur modification.

14.2 Considération (2.2) : Communications de couche IP

La passerelle de contenu est une entité qui peut avoir une adresse IP. De plus, tous les protocoles pertinents (SMTP, SIP, HTTP, etc.) font connaître explicitement la présence de la passerelle aux points d'extrémité.

14.3 Considération (3.1) : Notification - Envoyeur

Là encore, c'est l'objet même du présent document. L'envoyeur obtient explicitement la notification de si la passerelle va retirer une partie de corps marquée comme contenu critique.

14.4 Considération (3.2) : Notification - Receveur

La nature du système receveur impose que les utilisateurs finaux comprennent que les messages ont été changés.

14.5 Considération (3.3) : Non blocage

Par définition, le point d'extrémité ne peut pas recevoir de contenu non modifié, de sorte que cette exigence ne s'applique pas.

14.6 Considération (4.1) : Résolution d'URI

On voit clairement que l'un envoie de la messagerie (SMTP), un message (SIP), ou va chercher un document (HTTP). La machinerie décrite dans ce document n'altère pas le contenu lui-même ni le mécanisme d'accès. Donc, il est conforme à cette exigence.

14.7 Considération (4.2) : Validité de référence

Comme le protocole décrit dans le présent document n'altère pas le contenu lui-même, les références inter- et intra-document ne sont pas altérées. Cependant, les références intra-document à des parties de corps supprimées vont échouer. D'un autre côté, l'envoyeur a marqué explicitement ces parties de corps comme pouvant être éliminées. Donc, l'envoyeur est conscient de la possibilité que ces parties n'arrivent pas au receveur.

14.8 Considération (4.3) : Extensions d'architecture

Comme le protocole décrit dans le présent document satisfait aux considérations 4.1 et 4.2, cette exigence ne s'applique pas.

14.9 Considération (5.1) : Confidentialité

La politique de confidentialité de ce protocole est explicite. En particulier, le protocole respecte la sécurité de bout en bout.

15. Considérations sur la sécurité

Les UA envoyeurs peuvent utiliser des signatures sur les indicateurs de contenu critique pour assurer l'intégrité de l'indicateur.

La passerelle DOIT respecter le traitement de signature. En particulier, si l'UA envoyeur marque les composants de la signature comme REQUIRED, et si le point d'extrémité ne peut pas faire le traitement de signature MIME, la passerelle DOIT établir un mécanisme de signature approprié entre la passerelle et le point d'extrémité. Dans ce cas, la passerelle doit être sûre, car elle peut devenir une cible pour altérer les composants signés du message.

Les systèmes receveurs et les usagers ne devraient pas placer de valeur d'authentification dans le paramètre Handling.

Noter que par conception, et à la demande de l'utilisateur envoyeur, une passerelle de contenu va éliminer en silence les parties de corps sans importance. Le contenu critique donne à l'envoyeur la capacité de déterminer le niveau acceptable d'intégrité du message livré. C'est-à-dire que le message, tel que la passerelle de contenu le passe réellement, est en fait représentatif des intentions de l'envoyeur.

16. Considérations à propos de l'IANA

La [RFC3204] a déjà enregistré le paramètre Handling. Il n'est repris ici que pour référence et comme rappel pour l'utiliser pour une expansion éventuelle à l'avenir et comme référence normative pour d'autres documents qui auraient besoin de faire référence au paramètre Handling.

Selon la section 9 de la [RFC2183], voici l'enregistrement IANA pour Handling.

To: IANA@IANA.ORG
Sujet : Enregistrement d'un nouveau paramètre de Content-Disposition
Nom du paramètre Content-Disposition : HANDLING
Valeurs admissibles pour ce paramètre : REQUIRED OPTIONAL
Description : Marque la partie de corps comme exigée pour la livraison (REQUIRED) ou comme pouvant être éliminée en

silence (OPTIONAL). Voir la RFC3459 et la RFC 3204.

Selon la RFC2183, le nom du paramètre de Content-Disposition n'est pas sensible à la casse. Selon la RFC3459, les valeurs du paramètre ne sont pas non plus sensibles à la casse.

17. Références

17.1 Références normatives

[RFC0822] D. Crocker, "Norme pour le format des messages de texte de l'ARPA-Internet", STD 11, août 1982. (*Obsolète, remplacée par la RFC*5322)

[RFC1847] J. Galvin, S. Murphy, S. Crocker, N. Freed, "Sécurité multiparties pour MIME : multipartie/signée et multipartie/chiffrée", octobre 1995. *(P.S.)*

[RFC2026] S. Bradner, "Le processus de normalisation de l'Internet -- Révision 3", (BCP0009) octobre 1996. *(Remplace* RFC1602, RFC1871) (*MàJ par* RFC3667, RFC3668, RFC3932, RFC3979, RFC3978, RFC5378, RFC6410)

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

[RFC2046] N. Freed et N. Borenstein, "Extensions de messagerie Internet multi-objets (MIME) Partie 2 : Types de support", novembre 1996. *(D. S., MàJ par* 2646, 3798, 5147, 6657*.)*

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

[RFC2156] S. Kille, "MIXER (Relais amélioré Mime Internet X.400) : transposition entre X.400 et la RFC0822/MIME ", janvier 1998. *(Remplace* RFC0987, RFC1026, RFC1138, RFC1148, RFC1327, RFC1495) *(P.S.)*

[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.)*

[RFC2234] D. Crocker et P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", novembre 1997. (*Obsolète, voir* RFC5234)

[RFC2298] R. Fajman, "Format de message extensible pour les notifications de disposition de message", mars 1998. (*Obsolète, voir* RFC3798) *(P.S.)*

[RFC2421] G. Vaudreuil, G. Parsons, "Profil vocal pour la messagerie Internet - version 2", septembre 1998. (*Obsolète, voir* RFC3801) *(P.S.)*

[RFC2480] N. Freed, "Les routeurs et le traitement de multiparties de sécurité MIME", janvier 1999. *(P.S.)*

[RFC2821] J. Klensin, éditeur, "Protocole simple de transfert de messagerie", STD 10, avril 2001. *(Obsolète, voir* RFC5321*)*

[RFC3204] E. Zimmerer et autres, "Types de support MIME pour objets ISUP et QSIG", décembre 2001. (*MàJ par* RFC3459) *(P.S.)*

[RFC3238] S. Floyd, L. Daigle, "Considérations architecturales et de politique de l'IAB pour des services marginaux à connexion libre (OPES)", janvier 2002. *(Information)*

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

[RFC3461] K. Moore, "Extension de service du protocole simple de transfert de messagerie (SMTP) pour les notifications d'état de livraison (DSN)", janvier 2003. (*MàJ par* RFC3798, RFC3885, RFC5337, RFC6533) *(D.S.)*

[RFC3463] G. Vaudreuil, "Codes d'état améliorés du système de messagerie", janvier 2003. (*MàJ par* RFC3886, RFC4468, RFC4865, RFC4954, RFC5248) *(D.S.)*

[RFC3464] K. Moore, G. Vaudreuil, "Format extensible de message pour les notifications d'état de livraison", janvier 2003. (*MàJ par* RFC4865, RFC5337, RFC6533) *(D.S.)*

17.2 Référence pour information

[RFC2426] F. Dawson, T. Howes, "Profil de répertoire MIME vCard", septembre 1998. *(P.S.)*

18. Remerciements

Emily Candell de Comverse Network Systems a apporté une aide considérable pour creuser les questions de base du document -00 à Adelaide.

Ned Freed a montré que ce mécanisme porté sur la criticité, et non sur la notification. Cette idée a rendu le concept et la descriptions infiniment plus évidents. Si il y a encore une certaine confusion, c'est de ma faute ! Ned Freed a été aussi d'une aide capitale pour structurer les paragraphes sur multipart/signed et multipart/encrypted. Comme AD, il a fourni des commentaires précieux qui ont fait progresser le document.

Keith Moore a aidé à préciser les explications, et a approuvé l'utilisation de Content-Disposition.

L'abondons du type de contenu critique IMPORTANT a supprimé une des raison de la notification de non livraison partielle. Cela rend Jutta Degener très heureuse !

Harald Alvestrand et Chris Newman ont suggéré des exemples de mise en œuvre.

Greg White a posé La question clé qui nous a fait réaliser que le traitement du contenu critique était une fonction de passerelle, et non une fonction de MTA ou d'UA.

Jon Peterson a éclairci comment le traitement fonctionne en fait dans l'environnement SIP.

Un énorme merci à Michelle S. Cotton de l'IANA pour son aide à structurer la section IANA d'origine en 2000, et pour avoir saisi le recouvrement fonctionnel avec la RFC3204 en janvier 2002.

Toutes les erreurs, omissions, ou maladresses sont de ma faute.

19. Considérations sur la propriété intellectuelle

Une revendication de droits de propriété intellectuelle a été notifiée à l'IETF à l'égard de tout ou partie de la spécification contenue dans le présent document. Pour d'autres informations, consulter la liste en ligne des revendications de droits.

L'IETF ne prend position sur la validité ou la portée d'aucun droit de propriété intellectuelle ou d'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 non disponible ; pas plus qu'elle ne prétend qu'elle ait fait aucun effort pour identifier de tels droits. Des informations sur les procédures de l'IETF au sujet des droits dans la documentation en cours de normalisation et en rapport avec les normes peuvent être trouvées dans le BCP-11. Des copies des revendications de droits peuvent être disponibles à la publication et toutes les assurances de licences peuvent être rendues disponibles, ou le résultat de tentatives d'obtention d'une licence ou permission générale pour l'utilisation de tels droits de propriété par les mises en œuvre ou utilisateurs de la présente spécification peuvent être obtenus auprès du secrétariat de l'IETF.

L'IETF invite toute partie intéressée à porter à son attention tous droits de reproduction, brevets ou applications de brevets, ou autres droits de propriété qui pourraient couvrir une technologie qui pourrait être nécessaire pour mettre en pratique la présente norme. Prière d'adresser les information au Directeur Général de l'IETF.

20. Adresse de l'auteur

Eric Burger
SnowShore Networks, Inc.
285 Billerica Rd.
Chelmsford, MA 01824-4120
USA

téléphone : +1 978 367 8400
Fax : +1 603 457 5944
mél : e.burger@ieee.org

21. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2003). Tous droits réservés.

Le présent document et ses traductions peuvent être copiés et fournis aux tiers, et les travaux dérivés qui les commentent ou les expliquent ou aident à leur mise en œuvre peuvent être préparés, copiés, publiés et distribués, en tout ou partie, sans restriction d'aucune sorte, pourvu que la déclaration de droits de reproduction ci-dessus et le présent paragraphe soient inclus dans toutes telles copies et travaux dérivés. Cependant, le présent document lui-même ne peut être modifié d'aucune façon, en particulier en retirant la notice de droits de reproduction ou les références à la Internet Society ou aux autres organisations Internet, excepté autant qu'il est nécessaire pour le besoin du développement des normes Internet, auquel cas les procédures de droits de reproduction définies dans les procédures des normes Internet doivent être suivies, ou pour les besoins de la traduction dans 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 y contenues sont fournies 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 ci encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Remerciement

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