Groupe de travail Réseau
Request for Comments : 3860
Catégorie : En cours de normalisation

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

Profil commun pour la messagerie instantanée (CPIM)

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 "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Au moment de la rédaction du présent document, de nombreux protocoles de messagerie instantanée étaient utilisés, et il y avait peu d'interopérabilité entre les services fondés sur ces protocoles. La présente spécification définit une sémantique commune et des formats de données pour la messagerie instantanée (IM, *Instant Messaging*) pour faciliter la création de passerelles entre les services de messagerie instantanée.

Table desMatières

1. Introduction

La messagerie instantanée est définie dans la [RFC2778]. Au moment de la rédaction du présent document, de nombreux protocoles de messagerie instantanée étaient utilisés, et il y avait peu d'interopérabilité entre les services fondés sur ces

protocoles. La présente spécification définit une sémantique commune et des formats de données pour les services communs de messagerie instantanée pour faciliter la création de passerelles entre les services de messagerie instantanée : un profil commun pour la messagerie instantanée (CPIM, *common profile for instant messaging*).

Le comportement du service est décrit de façon abstraite en termes d'opérations invoquées entre le consommateur et le fournisseur d'un service. En conséquence, chaque service IM doit spécifier comment ce comportement est transposé en ses propres interactions de protocole. Le choix de la stratégie est une affaire locale, pourvu qu'il y ait une relation claire entre les comportements abstraits du service (comme spécifié dans le présent mémoire) et la façon dont il est réalisé de bonne foi par un service particulier de messagerie instantanée. Par exemple, une stratégie pourrait transmettre un message instantané comme des paires de clé/valeur textuelles, une autre pourrait utiliser une représentation binaire compacte, et une troisième pourrait utiliser des conteneurs incorporés.

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

Afin de fournir un moyen pour la préservation des caractéristiques de bout en bout (en particulier la sécurité) aux passerelles d'interopérabilité de messagerie instantanée traversées, la présente spécification donne aussi des recommandations pour les formats de document de messagerie instantanée qui pourraient être employés par les protocoles de messagerie instantanée.

2. Terminologie

Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14, [RFC 2119] et indiquent les niveaux d'exigence pour les mises en œuvre conformes.

Le présent mémoire utilise le vocabulaire défini dans la [RFC2778]. Des termes comme CLOS, BOÎTE AUX LETTRES INSTANTANÉE, MESSAGE INSTANTANÉ, et OUVERT sont utilisés avec la même signification que dans celle ci.

Le terme 'passerelle' utilisé dans le présent document note un élément de réseau chargé d'interopérer entre divers protocoles de messagerie instantanée. Bien que les protocoles de messagerie instantanée eux-mêmes soient divers, sous le modèle utilisé dans le présent document, ces protocoles peuvent porter une charge utile commune qui est relayée par la passerelle. On peut donc discuter de l'opportunité d'appeler ces intermédiaires d'interfonctionnement des 'passerelles' plutôt que des 'relais' ; pour les besoins du présent document, on les appelle 'passerelles CPIM'.

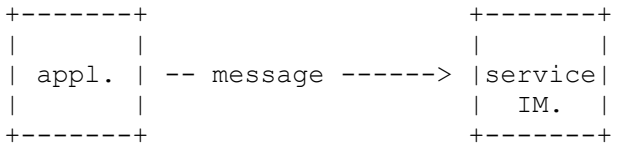
Le terme de 'service de messagerie instantanée' est lui aussi emprunté à la [RFC2778], mais sa signification change légèrement à cause de l'existence des passerelles dans le modèle CPIM. Lorsque un client envoie une opération à un service de messagerie instantanée, ce service peut être un point d'extrémité ou un intermédiaire tel qu'une passerelle CPIM – en fait, le client ne devrait pas avoir à savoir auquel il s'adresse, car les réponses de l'un ou de l'autre vont paraître les mêmes.

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

3. Service abstrait de messagerie instantanée

3.1 Généralités sur le service de messagerie instantanée

Lorsque une application veut envoyer un message à une BOÎTE AUX LETTRES INSTANTANÉE, elle invoque l'opération Message, par exemple,

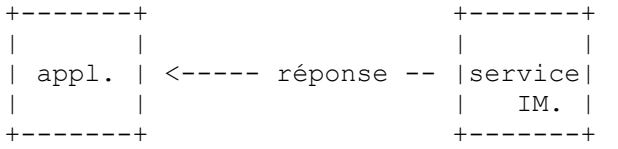


L'opération Message a les attributs suivants : source, destination, MaxForwards et TransID. 'source' et 'destination' identifient respectivement l'origine et le receveur d'un message instantané, et consistent en un identifiant de BOÎTE AUX LETTRES INSTANTANÉE (comme décrit au paragraphe 3.2). L'attribut MaxForwards est un compteur de bonds pour éviter des boucles à travers les passerelles, dont l'usage est précisé au paragraphe 3.4.2 ; sa valeur initiale est réglée par l'origine. L'attribut TransID est un identifiant univoque utilisé pour corréler les opérations Message aux opérations Réponse ; les passerelles devraient être capables de traiter des TransID jusqu'à une longueur de 40 octets.

L'opération Message a aussi un contenu, le message instantané lui-même, qui peut être textuel, ou peut consister en d'autres données. Les détails du contenu sont spécifiés au paragraphe 3.3.

Noter que la présente spécification suppose que les protocoles de messagerie instantanée assurent une livraison fiable du message ; il n'y a pas de disposition d'assurance de livraison du message de couche application dans cette spécification.

À réception d'une opération Message, le service répond immédiatement en invoquant l'opération Réponse qui contient le même identifiant de transaction, par exemple,



L'opération Réponse contient les attributs suivants : TransID et État. L'attribut TransID est utilisé pour corréler la réponse à un message instantané particulier. État indique si la livraison du message a réussi ou échoué. Les valeurs d'état valides sont décrites au paragraphe 3.4.1.

3.2 Identification des INSTANT INBOX

Une BOÎTE AUX LETTRES INSTANTANÉE est spécifiée en utilisant un URI de messagerie instantanée avec le schéma d'URI 'im:'. La syntaxe complète de l'URI IM est donnée à l'Appendice A. Un exemple serait: "im:fred@exemple.com"

3.2.1 Résolution d'adresse

Un client de service IM détermine le prochain bond pour transmettre l'IM en résolvant la portion 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 messages instantanés

La présente spécification définit un mécanisme abstrait d'interopérabilité pour les protocoles de messagerie instantanée ; 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 est employé pour la messagerie instantanée par les protocoles de messagerie instantanée interopérant, en particulier à l'égard de la sécurité. Pour conserver les propriétés de sécurité de bout en bout, les applications qui envoient des opérations Message à une passerelle CPIM DOIVENT mettre en œuvre le format défini dans MSGFMT [RFC3862]. Les applications PEUVENT prendre en charge d'autres formats de contenu.

Les passerelles CPIM DOIVENT être capables de relayer le contenu d'une opération Message entre les protocoles de messagerie instantanée sans avoir besoin de modifier ou inspecter le contenu.

3.4 Service de messagerie

3.4.1 Opération Message

Lorsque une application veut envoyer un MESSAGE INSTANTANÉ, elle invoque l'opération Message.

Lorsque un service de messagerie instantanée reçoit l'opération Message, il effectue les vérifications préliminaires suivantes :

1. Si la source ou la destination ne se réfère pas à une BOÎTE AUX LETTRES INSTANTANÉE syntaxiquement valide, une opération Réponse ayant l'état "échec" est invoquée.
2. Si la destination de l'opération ne peut pas être résolue par le receveur, et si celui-ci n'est pas le receveur final, une opération Réponse avec l'état "échec" est invoquée.
3. Si le contrôle d'accès ne permet pas à l'application de demander cette opération, une opération Réponse ayant l'état "échec" est invoquée.
4. Dans le cas où ces vérifications réussissent :
   Si le service de messagerie instantanée est capable de réussir à livrer le message, une opération Réponse ayant l'état "succès" est invoquée.
   Si le service n'est pas capable de réussir à livrer le message, une opération Réponse ayant l'état "échec" est invoquée.
   Si le service doit déléguer la responsabilité de la livraison (c'est-à-dire, si il agit comme une passerelle ou un mandataire de l'opération) et si la délégation ne va pas résulter en une future indication d'autorité au service, une opération Réponse ayant l'état "indéterminé" est invoquée.
   Si le service doit déléguer la responsabilité de la livraison, et si la délégation va résulter en une future indication d'autorité au service, une opération Réponse est alors invoquée immédiatement après que l'indication est reçue.

Lorsque le service invoque l'opération Réponse, le paramètre transID est identique à la valeur trouvée dans l'opération Message invoquée par l'application.

3.4.2 Boucle

L'acheminement dynamique des messages instantanés peut résulter en boucles d'un message à travers un relais. La détection des boucles n'est pas toujours évidente, car l'utilisation d'alias et les expansions de listes de groupe peuvent être légitimement cause qu'un message passe plus d'une fois à travers un relais.

Le présent document suppose que les protocoles de messagerie instantanée qui peuvent se faire relayer au moyen de CPIM prennent en charge une sémantique équivalente à une valeur d'entier qui indique le nombre maximum de bonds que peut franchir un message. Lorsque ce nombre de bonds a été atteint, le message est supposé être en boucle.

Lorsque une passerelle CPIM relaye un message instantané, elle diminue la valeur de l'attribut MaxForwards. Le présent document ne rend obligatoire aucun réglage initial particulier pour l'élément MaxForwards dans les protocoles de messagerie instantanée, mais il est recommandé que cette valeur soit raisonnablement grande (plus de cent).

Si une passerelle CPIM reçoit une opération de message instantané qui a l'attribut MaxForwards réglé à 0, elle élimine le message et invoque une opération Échec.

4. Considérations pour la sécurité

Des considérations pour la sécurité détaillées pour les protocoles de messagerie instantanée sont données dans la [RFC2779] (en particulier, les exigence sont données au paragraphe 5.4 et une discussion motivante dans 8.1).

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

L'introduction de passerelles dans le modèle de sécurité de la messagerie instantanée dans la [RFC2779] introduit aussi de nouveaux risques. Les propriétés de sécurité de bout en bout (en particulier la confidentialité et l'intégrité) entre agents d'usager de messagerie instantanée qui s'interfacent à travers une passerelle CPIM ne peuvent être fournies que si un format commun de messagerie instantanée (tels que le format décrit dans MSGFMT [RFC3862]) est accepté par les protocoles qui s'interfacent avec la passerelle CPIM.

Lorsque la sécurité de bout en bout est requise, l'opération Message DOIT utiliser MSGFMT, et DOIT sécuriser le corps MIME MSGFMT avec S/MIME [RFC3851], avec le chiffrement (CMS EnvelopeData) et/ou les signatures S/MIME (CMS SignedData).
Les algorithmes S/MIME sont établis par CMS [RFC3852]. L'algorithme AES [RFC3565] devrait être préféré, car on pense que AES convient mieux aux capacités de nombreuses plateformes. Les mises en œuvre PEUVENT utiliser AES comme algorithme de chiffrement, mais il est EXIGÉ qu'elles prennent en charge seulement les algorithmes de base rendus obligatoires par S/MIME et CMS.

Lorsque les URI IM sont placés dans les protocoles de messagerie instantanée, ils portent l'identité de l'envoyeur et/ou du receveur. Les certificats qui sont utilisés pour les opérations IM S/MIME DEVRAIENT, pour les besoins de l'intégrité de référence, contenir un champ subjectAltName contenant l'URI IM de leur sujet. Noter que de tels certificats peuvent aussi contenir d'autres identifiants, y compris ceux qui sont spécifiques de protocoles de messagerie instantanée particuliers. Afin de faciliter plus avant l'interopérabilité d'une messagerie sûre à travers les passerelles CPIM, les usagers et les fournisseurs de services sont invités à employer des ancres de confiance pour les certificats qui sont largement acceptés plutôt que des ancres de confiance spécifiques d'un service ou fournisseur particulier de messagerie instantanée.

Dans certains cas, il peut être désiré que la messagerie soit anonyme. Une telle capacité sort du domaine d'application de la présente spécification.

5. Considérations relatives à l'IANA

L'IANA a alloué le schéma "im".

5.1 Schéma d'URI IM

Le schéma d'URI messagerie instantanée (IM) désigne une ressource Internet, à savoir une BOÎTE AUX LETTRES INSTANTANÉE.

La syntaxe d'un URI IM est donnée à l'Appendice A.

6. Contributeurs

Dave Crocker a édité les versions antérieures du présent document.

Les personnes suivantes ont fait des contributions substantielles au texte du présent document :
Athanassios 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.)*

[RFC3862] G. Klyne, D. Atkins, "Profil commun pour la messagerie instantanée (CPIM) : format de message ", août 2004. *(P.S.)*

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 IANA d'enregistrement de l'URI IM

La présente section donne des informations pour enregistrer l'URI im: de messagerie instantanée.

A.1 Nom de schéma d'URI

im

A.2 Syntaxe du schéma d'URI

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

```
IM-URI      = "im:" [ to ] [ headers ]
to          =  mailbox
headers     =  "?" header *( "&" header )
header      =  hname "=" hvalue
hname       =  *uric
hvalue      =  *uric
```

Ici le symbole "mailbox" 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 sur le codage des caractères

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

A.4 Usage prévu

L'utilisation de l'URI im: suit étroitement celle de l'URI mailto:. C'est-à-dire que l'invocation d'un URI IM va causer le démarrage de l'application de messagerie instantanée de l'usager, 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 de non de schéma d'URI.

A.6 Considérations de sécurité

Voir la Section 4.

A.7 Publications pertinentes

RFC 2779, RFC 2778

A.8 Personne & adresse de messagerie à contacter pour des informations complémentaires

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

A.9 Auteur/contrôleur des changements

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

A.10 Applications et/ou protocoles qui utilisent ce nom de schéma d'URI

Service de messagerie instantanée.

Appendice B. Questions intéressantes

Cet appendice discute brièvement les questions qui peuvent être intéressantes lors de la conception d'une passerelle d'interfonctionnement.

B.1 Transposition d'adresse

Lorsque on transpose le service décrit dans ce mémoire, les transpositions qui placent des informations particulières dans la partie locale de l'adresse im: DOIVENT utiliser la méta syntaxe 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 et elle est habituellement peu agréable à la personne qui doit taper la chaîne. L'acheminement de source a aussi toute une histoire de problèmes de fonctionnement.
L'utilisation de l'acheminement de source pour les échanges entre différents services est fait par une transformation qui place la chaîne d'adresse d'origine entière dans la partie locale de l'adresse im: et désigne la passerelle dans la partie domaine.
Par exemple, si la BOÎTE AUX LETTRES INSTANTANÉE de destination 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 locales.

L'expérience montre qu'il est finalement préférable de cacher cette transposition aux utilisateurs finaux – si possible, 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
USA
téléphone : +1 925/363-8720
mél : jon.peterson@neustar.biz

Déclaration complète de droits de reproduction

Propriété intellectuelle

Remerciement

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