Groupe de travail Réseau
Request for Comments : 3428
Catégorie : En cours de normalisation

Traduction Claude Brière de L'Isle

B. Campbell, éditeur
J. Rosenberg, dynamicsoft
H. Schulzrinne, Columbia University
C. Huitema & D. Gurle, Microsoft Corporation
décembre 2002

Protocole d'initialisation de session (SIP) Extension pour la messagerie instantanée

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
La messagerie instantanée (IM, *Instant Messaging*) se réfère au transfert presque en temps réel de messages entre des usagers. Ces messages sont en principe courts, mais ce n'est pas obligé. Les IM sont souvent utilisés dans un mode conversationnel, c'est-à-dire que le transfert des messages de part et d'autre est assez rapide pour que les participants soutiennent une conversation interactive.

Le présent document propose la méthode MESSAGE, une extension au protocole d'initialisation de session (SIP, *Session Initiation Protocol*) qui permet le transfert de messages instantanés. Comme la demande MESSAGE est une extension à SIP, elle hérite de toutes les caractéristiques d'acheminement et de sécurité de la demande dont dispose ce protocole. Les demandes MESSAGE portent le contenu sous la forme de parties de corps MIME. Les demandes MESSAGE n'initient pas elles-mêmes un dialogue SIP ; en utilisation normale, chaque message instantané est autonome, un peu comme les messages de téléavertisseur. Les demandes MESSAGE peuvent être envoyées dans le contexte d'un dialogue initié par une autre demande SIP.

Terminologie
Dans ce document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "NON RECOMMANDÉ", "PEUT" et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14, [RFC2119] et indiquent les niveaux d'exigence pour les mises en œuvre conformes.

Table des matières

1. Introduction

La messagerie instantanée (IM, *Instant Messaging*) est définie comme l'échange presque en temps réel de contenu entre un ensemble de participants. Généralement, le contenu est un court message de texte, bien que cela ne soit pas nécessairement le cas. En général, les messages qui sont échangés ne sont pas mémorisés, mais cela non plus n'est pas forcément le cas. IM diffère de l'utilisation habituelle de la messagerie électronique en ce que les messages instantanés sont généralement groupés en une brève conversation en direct, consistant en de nombreux petits messages envoyés de part et d'autre.

La messagerie instantanée comme service est entrée dans l'existence au sein des intranets et des réseaux IP depuis assez longtemps. Les premières mises en œuvre incluent Zephyr [ZEPHYR], l'application de conversation de UNIX, et IRC. Plus récemment, IM a été utilisé comme un service couplé avec Présence et des listes d'amis ; c'est-à-dire que lorsque un ami vient en ligne, un utilisateur peut en être averti et avoir l'option d'envoyer un message instantané à l'ami. Les protocoles pour accomplir cela sont tous brevetés, ce qui a sérieusement entravé l'interopérabilité.

L'intégration de messagerie instantanée, de présence, et de communications en mode session est très puissante. Le protocole d'initialisation de session (SIP, *Session Initiation Protocol*) [RFC3261] fournit des mécanismes utiles pour les applications de présence, et pour les applications de communications en mode session, mais pas pour les messages instantanés.

Le présent document propose une méthode d'extension pour SIP appelée la méthode MESSAGE. Les demandes MESSAGE portent normalement le contenu du message instantané dans le corps de la demande.

Les [RFC2778] et [RFC2779] donnent un modèle et des exigences pour les protocoles de présence et de messagerie instantanée. Les mises en œuvre de la méthode MESSAGE DEVRONT prendre en charge les exigences de la messagerie instantanée de la [RFC2779] en ce qui concerne son domaine d'application.

2. Domaine d'applicabilité

Le présent document décrit l'utilisation de la méthode MESSAGE pour l'envoi de messages instantanés en utilisant une métaphore similaire à celle d'un télétransmetteur bidirectionnel ou d'un combiné qui a la capacité d'envoyer des SMS. C'est-à-dire qu'il n'y a pas d'association explicite entre les messages. Chaque IM est autonome – l'idée de "conversation" n'existe que dans l'interface d'utilisatur du client, ou peut-être dans la propre imagination de l'utilisateur. On oppose cela au modèle de "session", où il y a une conversation explicite avec un début et une fin bien déterminés. Dans l'environnement SIP, une session IM serait une session sur un support initiée par une transaction INVITE et terminée par une transaction BYE.

Chaque modèle a ses vertus. La plupart des clients IM modernes offrent les deux expériences d'utilisateur. Celui-ci peut choisir d'envoyer un IM à un contact, ou peut choisir d'inviter un ou plusieurs contacts à se joindre à une conversation. Le modèle du télétransmetteur *(pager)* prend son sens lorsque l'utilisateur souhaite envoyer un petit nombre de courts messages instantanés à un seul receveur (ou à un petit nombre de receveurs). Le modèle de session prend son sens pour des conversations étendues, réunissant des groupes de discussion, si se fait sentir le besoin d'associer une conversation à une autre session SIP, etc.

Le présent document ne vise que le modèle du télétransmetteur *(pager)*. Tout en reconnaissant la valeur du modèle de session, celui-ci ne sera pas défini ici. Une telle solution exigera des travaux supplémentaires qui vont au delà des capacités du présent document. Le groupe de travail SIMPLE prévoit actuellement de traiter des sessions IM dans un autre document.

Il peut être tentant de simuler une session de IM en initiant un dialogue, puis d'envoyer des demandes MESSAGE dans le contexte de ce dialogue. Ceci n'est pas une solution adéquate pour les sessions IM, en ce que cette approche force les demandes MESSAGE à suivre le même chemin réseau que toutes les autres demandes SIP, même si les demandes MESSAGE portent plutôt du message que de la signalisation. Les applications d'IM sont normalement de fort volume, et on s'attend à ce que le volume d'IM dans les sessions soit encore plus élevé. Cela va vraisemblablement causer des problèmes d'encombrement si ils sont envoyés sur un transport sans contrôle d'encombrement, et il n'y a pas de mécanisme évident dans SIP pour empêcher certains bonds de transmettre une demande MESSAGE sur UDP.

De plus, les demandes MESSAGE envoyées sur un dialogue existant doivent, de par la nature de SIP, aller à la même

destination que toute autre demande envoyée dans ce dialogue. Cela empêche toute séparation entre le point d'extrémité IM et le point d'extrémité de signalisation. Ce n'est pas une limitation acceptable pour le modèle de session de la messagerie instantanée.

Les auteurs reconnaissent qu'il peut y avoir des raisons valides pour envoyer des demandes MESSAGE dans le contexte d'un dialogue. Par exemple, un participant à une session vocale peut souhaiter envoyer un IM à un autre participant, et associer cet IM à la session. Mais les mises en œuvre NE DEVRAIENT PAS créer des dialogues dans le but principal d'associer des demandes MESSAGE les unes avec les autres.

Noter que cette déclaration n'interdit pas d'utiliser SIP pour initier une session support faite d'IM, tout comme n'importe quelle autre session. Bien sûr, on s'attend à la solution de sessions IM qui utilisent cette métaphore. Le lecteur devrait éviter de confondre les concepts de dialogue SIP et de session support.

3. Généralités sur le fonctionnement

Lorsque un usager souhaite envoyer un message instantané à un autre usager, l'envoyeur formule et produit une demande SIP en utilisant la nouvelle méthode MESSAGE définie dans le présent document. L'URI de demande de cette demande va normalement être "l'adresse d'enregistrement" pour le receveur du message instantané, mais cela peut être l'adresse d'un appareil dans les situations où le client a les informations actuelles sur la localisation du receveur. Par exemple, le client pourrait être couplé avec un système de présence qui fournit un contact d'appareil à jour pour une certaine adresse d'enregistrement. Le corps de la demande va contenir le message à délivrer. Ce corps peut être de n'importe quel type MIME, y compris message/cpim [RFC3862]. Comme le format message/cpim est supposé être accepté par les autres protocoles de message instantané, les points d'extrémité qui utilisent des protocoles IM différents, mais acceptent par ailleurs les types de corps message/cpim devraient être capables d'échanger des messages sans modification du contenu à travers une passerelle ou autre intermédiaire. Cela aide à activer la sécurité de bout en bout entre des points d'extrémité qui utilisent des protocoles IM différents.

La demande peut traverser un ensemble de mandataires SIP, en utilisant divers transports, avant d'atteindre sa destination. La destination pour chaque bond est localisée en utilisant les règles de résolution d'adresse précisées dans le profil commun pour la messagerie instantanée (CPIM, *Common Profile for Instant Messaging*) [ARIMP] et dans les spécifications SIP. Durant la traversée, chaque mandataire peut réécrire l'URI de demande sur la base des informations d'acheminement disponibles.

Les réponses provisoire et finale à la demande seront retournées à l'envoyeur comme pour toute autre demande SIP. Normalement, une réponse 200 OK sera générée par l'agent d'utilisateur du receveur final de la demande. Noter que cela indique que l'agent d'utilisateur a accepté le message, et non que l'usager l'a vu.

Les demandes MESSAGE n'établissent pas de dialogue.

4. Traitement de client d'agent d'utilisateur

Sauf mention contraire dans le présent document, les demandes MESSAGE et les réponses associées sont construites conformément aux règles du paragraphe 8.1 de la spécification SIP [RFC3261].

Tous les clients d'agent d'utilisateur (UAC, *User Agent Client*) qui prennent en charge la méthode MESSAGE DOIVENT être prêts à envoyer des demandes MESSAGE avec un corps de type text/plain. Ils peuvent envoyer des corps de type message/cpim [RFC3862].

Les demandes MESSAGE n'initient pas de dialogue. Les agents d'utilisateur NE DOIVENT PAS insérer de champs d'en-tête Contact dans les demandes MESSAGE.

Un UAC PEUT associer une demande MESSAGE à un dialogue existant. Si une demande MESSAGE est envoyée au sein d'un dialogue, elle est "associée" à toute session support sur les sessions associées à ce dialogue.

Si l'UAC reçoit une réponse 200 OK à une demande MESSAGE, elle peut supposer que le message a été délivré à la destination finale. Elle NE DOIT PAS supposer que le receveur a en fait lu le message instantané. Si l'UAC reçoit une réponse 202 Accepté, le message a été livré à une passerelle, à un serveur de transmission indirecte, ou quelque autre service qui peut finalement délivrer le message. Dans ce cas, l'UAC NE DOIT PAS supposer que le message a été délivré à la destination finale. Si la confirmation de la livraison est exigée pour un message auquel il a été répondu par un 202 Accepté, cette confirmation doit être délivrée via quelque autre mécanisme, ce qui sort du domaine d'application de la

présente spécification.

Noter qu'un mandataire aval pourrait dupliquer une demande MESSAGE. Si cela arrive, le mandataire duplicateur va transmettre une réponse finale en amont, même si il se peut qu'il reçoive plusieurs réponses finales. L'UAC n'aura aucun moyen de détecter si une duplication se produit ou non. Donc, l'UAC NE DOIT PAS supposer qu'une certaine réponse finale représente le seul serveur d'agent d'utilisateur (UAS, *User Agent Server*) qui a reçu la demande. Par exemple, plusieurs branches d'une déviation pourraient avoir résulté en réponses 2xx. Même si l'UAC ne voit qu'une de ces réponses, la demande a en fait été reçue aussi par le second appareil.

L'UAC PEUT ajouter un champ d'en-tête Expire pour limiter la validité du contenu du message. Si l'UAC ajoute un champ d'en-tête Expire avec une valeur différente de zéro, il DEVRAIT aussi ajouter un champ d'en-tête Date contenant l'heure d'envoi du message.

5. Utilisation des URI de message instantané

Une boîte aux lettres instantanée peut être très généralement référencée par un URI de message instantané [ARIMP] sous la forme de "im:usager@domaine". Les URI IM sont abstraits, et vont finalement être traduits en URI concrets, selon le protocole.

Si un UA est présenté avec un URI IM comme l'adresse pour un message instantané, il DEVRAIT le résoudre en un URI SIP, et placer l'URI résultant dans l'URI-de-demande de la demande MESSAGE avant l'envoi. Si l'UA est incapable de résoudre l'URI IM, il PEUT placer l'URI IM dans l'URI-de-demande, délégant ainsi la résolution à un appareil aval tel qu'un mandataire ou une passerelle. Effectuer cette traduction aussitôt que possible permet aux mandataires SIP, qui peuvent n'être pas au courant de l'espace de noms im:, d'acheminer normalement les demandes.

Les demandes MESSAGE contiennent aussi des identifiants logiques de l'envoyeur et du receveur prévu, sous la forme des champs d'en-tête From et To. Ces identifiants DEVRAIENT contenir des URI SIP (ou SIPS) mais PEUVENT inclure des URI IM si les URI SIP ne sont pas connus au moment de la construction de la demande.

Les champs d'en-tête Record-Route et Route NE DOIVENT PAS contenir des URI IM. Ces champs d'en-tête contiennent des URI SIP ou SIPS concrets conformément aux règles de SIP [RFC3261].

6. Traitement de mandataire

Les mandataires acheminent les demandes MESSAGE conformément aux règles de SIP [RFC3261]. Noter que la demande MESSAGE PEUT être dupliquée ; cela permet la livraison du message à plusieurs terminaux possibles où pourrait se trouver l'utilisateur. Un mandataire qui duplique une demande de MESSAGE suit les règles SIP normales pour la duplication d'une demande non INVITE. En particulier, même si la fourche résulte en plusieurs livraisons réussies, le mandataire duplicateur va seulement transmettre une seule réponse finale en amont.

7. Traitement du serveur d'agent d'utilisateur

Un UAS qui reçoit une demande MESSAGE la traite suivant les règles de SIP [RFC3261].

Un UAS qui reçoit une demande MESSAGE DEVRAIT répondre immédiatement par une réponse finale. Noter, cependant, que l'UAS n'est pas obligé d'afficher le message à l'usager avant ou après avoir répondu par un 200 OK. C'est à dire que la réponse 200 OK ne signifie pas nécessairement que l'usager a lu le message.

Une réponse 2xx à une demande MESSAGE NE DOIT PAS contenir de corps. Un UAS NE DOIT PAS insérer un champ d'en-tête Contact dans une réponse 2xx.

Un UAS qui est, en fait, un relais de message, qui mémorise le message et le transmet plus tard, ou le transmet dans un domaine non SIP, DEVRAIT retourner une réponse 202 (Accepté) [RFC3265] qui indique que le message a été accepté, mais que la livraison de bout en bout n'est pas garantie.

Une réponse 4xx ou 5xx indique que le message n'a pas réussi à être délivré. Une réponse 6xx signifie qu'il a bien été délivré, mais a été refusé.

Un UAS qui prend en charge la méthode MESSAGE DOIT être prêt à recevoir et restituer des corps de type "text/plain", et peut prendre en charge la réception et la restitution de corps de type "message/cpim" [RFC3862].

Une demande MESSAGE est dite être arrivée à expiration si l'heure d'expiration est passée. L'heure d'expiration est déterminée en examinait le champ d'en-tête Expire, si il est présent. Les demandes MESSAGE sans champ d'en-tête Expire n'expirent pas. Si la demande MESSAGE qui contient un champ d'en-tête Expire contient aussi un champ d'en-tête Date, l'UAS DEVRAIT interpréter la valeur du champ d'en-tête Expire comme un delta de temps à partir de la valeur du champ d'en-tête Date. Si la demande ne contient pas de champ d'en-tête Date, l'UAS DEVRAIT interpréter la valeur de l'en-tête Expire comme un delta de temps à partir de l'heure à laquelle l'UAS a reçu la demande.

Si le MESSAGE expire avant que l'UAS soit capable de présenter le message à l'usager, l'UAS DEVRAIT traiter le message sur la base de la politique locale. Cette politique pourrait signifier que le message est supprimé sans être affiché, que le message est quand même affiché à l'usager, ou quelque autre politique peut être invoquée. Si le message est affiché, l'UAS DEVRAIT indiquer clairement à l'usager que le message est arrivé à expiration.

Si l'UAS agit comme relais de message, et si il est incapable de délivrer le message avant expiration, il choisit une action sur la base de la politique locale. Cette action pourrait impliquer de supprimer le message sans le livrer, de le livrer tel quel, d'enregistrer le message expiré, ou toute autre politique locale.

8. Contrôle de l'encombrement

Les services IM existants ont un passé d'utilisation de très gros volume. De plus, les demandes MESSAGE diffèrent des autres sortes de demandes SIP en ce qu'elles portent une charge utile sous la forme de messages instantanés. Les charges utiles SIP conventionnelles portent des informations de signalisation au sujet des supports mais pas les supports eux-mêmes. Il y a une éventualité que si une infrastructure SIP est partagée entre de la signalisation d'appel et de la messagerie instantanée, le trafic IM interfère avec le trafic de signalisation d'appel. Le contrôle d'encombrement en général est un problème qui devrait être traité au niveau de la spécification SIP plutôt que pour une méthode individuelle. Mais comme les schémas de trafic vont vraisemblablement être différents pour MESSAGE que pour la plupart des autres méthodes, il paraît raisonnable de porter une considération particulière à MESSAGE.

Chaque fois que possible, les demandes MESSAGE DEVRAIENT être envoyées sur des transports qui mettent en œuvre le contrôle d'encombrement de bout en bout, comme TCP ou SCTP. Cependant, SIP ne fournit pas de mécanisme pour empêcher un bond aval d'envoyer une demande sur UDP. Même l'exigence d'utiliser TCP pour les demandes au delà d'une certaine taille peut être outrepassée par le receveur. Donc, l'utilisation par l'UAC d'un transport à contrôle d'encombrement n'est pas suffisante.

La taille des demandes MESSAGE en dehors d'une session support NE DOIT PAS excéder 1300 octets, sauf si l'UAC sait positivement que le message ne traversera à aucun bond de liaison à fort risque d'encombrement, ou que la taille du message est d'au moins 200 octets inférieure à la plus basse valeur de MTU trouvée en route vers l'UAS. De plus grosses charges utiles peuvent être envoyées au titre d'une session support ou en utilisant un type de masquage de contenu.

Au moment de la rédaction du présent document, il n'y a pas de mécanisme permettant à un UAC d'obtenir cette connaissance en dehors des architectures de réseau triviales, ou de réseaux qui sont totalement contrôlés par un seul domaine administratif. Mais si est créé à l'avenir un mécanisme assurant le contrôle d'encombrement à chaque bond, les clients MESSAGE pourront assouplir les limites de taille sans exiger de changement de la présente spécification. Les auteurs s'attendent à ce qu'un tel mécanisme soit bientôt créé.

L'idée d'appuyer la limite de 1300 octets sur la MTU du chemin vers l'appareil SIP du prochain bond a été discutée. La spécification SIP fait exactement cela, en choisissant la limite à 200 octets en dessous de la MTU du chemin, ou 1300 octets si l'appareil ne connaît pas la MTU du chemin. Les décisions de transport sont prises bond par bond. Cependant, l'objet de cette limite est de s'assurer qu'aucun mandataire amont ne choisit d'envoyer une demande MESSAGE avec un gros contenu sur UDP. Comme, sauf dans des circonstances triviales, un client MESSAGE a très peu de chances de connaître la MTU pour les appareils en amont au delà du prochain bond, une limite fondés sur la MTU n'est pas très utile.

Un UAC NE DOIT PAS initier un nouvelle transaction MESSAGE hors dialogue pour un certain URI si il y a déjà une précédente transaction hors dialogue en cours pour le même URI. De même, un UAC NE DEVRAIT PAS initier de transactions MESSAGE qui se chevauchent à l'intérieur d'un dialogue, et NE DOIT PAS le faire à moins que le chemin établi pour ce dialogue utilise à chaque bond un transport à contrôle d'encombrement.

L'interdiction du chevauchement de demandes MESSAGE donne un certain degré de comportement libre d'encombrement. Une demande et sa réponse associée doivent chacune traverser la totalité du chemin entre l'UAC et l'UAS. Le temps exigé

pour cela va augmenter avec l'encombrement du réseau. Cela donne un mécanisme adaptatif pour ralentir l'introduction de nouvelles demandes MESSAGE pour la même destination.

Il a été suggéré que des réponses provisoires ne devraient pas être admises pour les demandes MESSAGE du modèle télétransmetteur. Cependant, il n'est pas possible d'exiger un traitement particulier pour MESSAGE, car de nombreux serveurs mandataires ignoreront la méthode MESSAGE. Donc, les demandes MESSAGE vont recevoir le même traitement de réponse provisoire que tout autre méthode non INVITE, comme décrit dans la spécification SIP.

9. Définition de la méthode

La présente spécification définit une nouvelle méthode SIP, MESSAGE. Le BNF pour cette méthode est :

MESSAGEm = %x4D.45.53.53.41.47.45 ; MESSAGE en majuscules

Comme avec toutes les autres méthodes, le nom de la méthode MESSAGE est sensible à la casse.

Les tableaux 1 et 2 étendent les tableaux 2 et 3 de la section 20 de SIP [RFC3261] en ajoutant une colonne supplémentaire pour définir les champs d'en-tête qui peuvent être utilisés dans les demandes et réponses MESSAGE.

Champ d'en-tête	**où**	**mandataire**	**MESSAGE**
Accept	R		-
Accept	2xx		-
Accept	415		m*
Accept-Encoding	R		-
Accept-Encoding	2xx		-
Accept-Encoding	415		m*
Accept-Language	R		-
Accept-Language	2xx		-
Accept-Language	415		m*
Alert-Info	R		-
Alert-Info	180		-
Allow	R		o
Allow	2xx		o
Allow		r	o
Allow	405		m
Authentication-Info	2xx		o
Authorization	R		o
Call-ID	c	r	m
Call-Info		ar	o
Contact	R		-
Contact	1xx		-
Contact	2xx		-
Contact	3xx		o
Contact	485		o
Content-Disposition			o
Content-Encoding			o
Content-Language			o
Content-Length		ar	t
Content-Type			*
Cseq	c	r	m
Date		a	o
Error-Info	300-699	a	o
Expires			o
From	c	r	m
In-Reply-To	R		o
Max-Forwards	R	amr	m
Organization		a	o

Tableau 1 : Résumé des champs d'en-tête, A--O

Champ d'en-tête	où	mandataire	MESSAGE
Priority	R	ar	o
Proxy-Authenticate	407	ar	m
Proxy-Authenticate	401	ar	o
Proxy-Authorization	R	dr	o
Proxy-Require	R	a	o
Record-Route		ar	-
Reply-To			o
Require		ar	c
Retry-After	404,413,480,486		o
	500,503		o
	600,603		o
Route	R	adr	o
Server		r	o
Subject	R		o
Timestamp			o
To	c(1)	r	m
Unsupported	420		o
User-Agent			o
Via	R	amr	m
Via	rc	dr	m
Warning		r	o
WWW-Authenticate	401	ar	m
WWW-Authenticate	407	ar	o

(1) : copié avec ajout possible d'une étiquette

Tableau 2 : Résumé des champs d'en-tête, P--Z

Une demande MESSAGE PEUT contenir un corps, en utilisant les champs d'en-tête standard MIME pour identifier le contenu.

10. Exemple de messages

Un exemple de flux de message est donné à la Figure 1. Le flux de message montre un IM initial envoyé de l'usager 1 à l'usager 2, tous deux usagers dans le même domaine, "domain", à travers un seul mandataire.

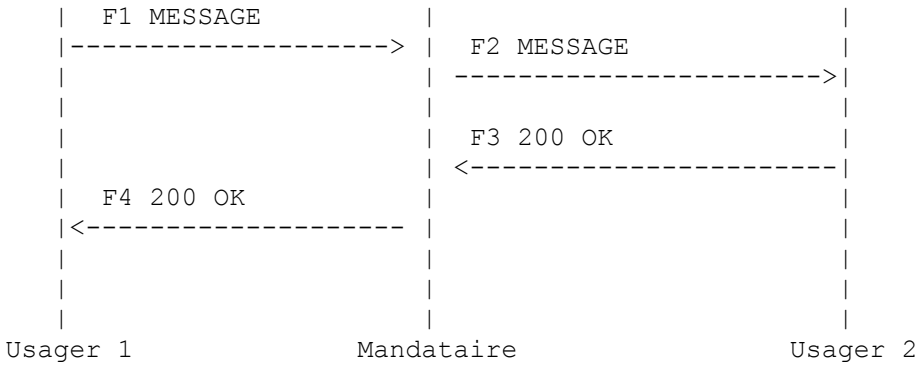

Figure 1: Exemple de flux de messages

Le message F1 ressemble à :
MESSAGE sip:user2@domain.com SIP/2.0
Via: SIP/2.0/TCP user1pc.domain.com;branch=z9hG4bK776sgdkse
Max-Forwards: 70
From: sip:user1@domain.com;tag=49583
To: sip:user2@domain.com
Call-ID: asd88asd77a@1.2.3.4
CSeq: 1 MESSAGE
Content-Type: text/plain

Content-Length: 18

Watson, viens ici.

L'usager1 transmet ce message au serveur pour domain.com. Le mandataire reçoit cette demande, et reconnaît que c'est le serveur pour domain.com. Il cherche l'usager2 dans sa base de données (construite à partir des enregistrements) et trouve un lien entre sip:user2@domain.com et sip:user2@user2pc.domain.com. Il transmet la demande à l'usager2. Le message résultant, F2, ressemble à :

MESSAGE sip:user2@domain.com SIP/2.0
Via: SIP/2.0/TCP proxy.domain.com;branch=z9hG4bK123dsghds
Via: SIP/2.0/TCP user1pc.domain.com;branch=z9hG4bK776sgdkse; received=1.2.3.4
Max-Forwards: 69
From: sip:user1@domain.com;tag=49394
To: sip:user2@domain.com
Call-ID: asd88asd77a@1.2.3.4
CSeq: 1 MESSAGE
Content-Type: text/plain
Content-Length: 18

Watson, viens ici.

Le message est reçu par user2, affiché, et une réponse est générée, le message F3, et envoyé au mandataire :

SIP/2.0 200 OK
Via: SIP/2.0/TCP proxy.domain.com;branch=z9hG4bK123dsghds; received=192.0.2.1
Via: SIP/2.0/TCP user1pc.domain.com;;branch=z9hG4bK776sgdkse; received=1.2.3.4
From: sip:user1@domain.com;tag=49394
To: sip:user2@domain.com;tag=ab8asdasd9
Call-ID: asd88asd77a@1.2.3.4
CSeq: 1 MESSAGE
Content-Length: 0

Noter que la plupart des champs d'en-tête sont simplement reflétés dans la réponse. Le mandataire reçoit cette réponse, retire le Via du sommet, et transmet à l'adresse dans le Via suivant, user1pc.domain.com, le résultat étant le message F4:

SIP/2.0 200 OK
Via: SIP/2.0/TCP user1pc.domain.com;branch=z9hG4bK776sgdkse; received=1.2.3.4
From: sip:user1@domain.com;;tag=49394
To: sip:user2@domain.com;tag=ab8asdasd9
Call-ID: asd88asd77a@1.2.3.4
CSeq: 1 MESSAGE
Content-Length: 0

11. Considérations pour la sécurité

En utilisation normale, la plupart des demandes SIP sont utilisées pour établir et modifier les sessions de communication. La communication réelle entre les participants se fait dans les sessions de support, et non dans les demandes SIP elles mêmes. La méthode MESSAGE change cette hypothèse ; les demandes MESSAGE portent normalement la communication réelle entre les participants comme charge utile. Cela implique que les demandes MESSAGE ont un plus grand besoin de sécurité que la plupart des autres demandes SIP. En particulier, les UA qui prennent en charge la demande MESSAGE DOIVENT mettre en œuvre des mécanismes d'authentification de bout en bout, d'intégrité du corps, et de confidentialité du corps.

11.1 Authentification en sortie

Lorsque des mandataires locaux sont utilisés pour la transmission de messages sortants, l'authentification du mandataire, comme spécifiée dans la [RFC3261], est RECOMMANDÉE. Cela est utile pour vérifier l'identité de l'origine, et empêche l'usurpation d'identité et l'émission de pourriels sur le réseau d'origine.

11.2 URI SIPS

Le mécanisme d'URI SIPS [RFC3261] permet à un UA de certifier que chaque bond doit survenir sur une connexion sûre. Cela donne un certain niveau de protection de l'intégrité et de la confidentialité. Cependant, cela exige des utilisateurs qu'ils aient confiance que chaque mandataire sur le chemin de la demande se comportera bien, c'est-à-dire, qu'ils ne violent pas les règles d'acheminement des URI SIPS. Aussi, tout corps non chiffré est entièrement exposé aux mandataires.

De plus, la possibilité d'un mandataire fourcheur permet à une demande MESSAGE d'être livrée aux points d'extrémité supplémentaires à l'insu de l'UAC. Si seule une protection bond par bond est utilisée, les utilisateurs doivent avoir confiance que tous les mandataires de la chaîne ne dévieront pas les demandes vers des destinations non autorisées.

11.3 Protection de bout en bout

Lorsque l'objectif est de remédier aux problèmes exposés ci-dessus, les corps de MESSAGE DOIVENT être sécurisés avec S/MIME. Si les corps spécifiés à l'avenir pour être portés par la méthode MESSAGE ont des moyens différents pour fournir la sécurité de bout en bout, leur spécification DEVRA décrire leur utilisation. Les points d'extrémité de MESSAGE SIP DOIVENT prendre en charge le chiffrement (EnvelopeData CMS) et les signatures S/MIME (SignedData CMS).

Les algorithmes S/MIME sont établis par la [RFC3369]. l'algorithme AES [AES] devrait être préféré, car il est estimé que AES convient le mieux aux capacités de nombreuses plates-formes. Cependant, une spécification de l'IETF sur ce sujet est encore inachevée au moment de la rédaction du présent mémoire.

11.4 Prévention de la répétition

Pour empêcher la répétition de vieilles demandes SIP, toutes les demandes et réponses MESSAGE signées DOIVENT contenir un champ d'en-tête Date couvert par la signature du message. Tout message avec une date plus ancienne que plusieurs minutes dans le passé, ou qui est de plus de quelques minutes dans le futur, DEVRAIT avoir pour réponse un message 400 (Date ou heure incorrecte) sauf si un tel message arrive de façon répétée de la même source, auquel cas il PEUT être éliminé sans envoyer de réponse. Évidemment, ce mécanisme de prévention des attaques en répétition ne fonctionne pas pour les appareils sans horloge.

Noter qu'il y a des situations où un champ d'en-tête Date périmé est normal. Par exemple, la demande MESSAGE peut avoir été mémorisée dans un serveur de transmission différée pendant que le receveur était hors ligne. Lorsque le receveur revient en ligne, ce serveur peut alors transmettre le message. La réception finale du message va alors survenir un certain temps après son envoi original.

Si un UAS reçoit un message périmé qui peut être confirmé comme venant d'un serveur connu de transmission différée (peut-être sur une connexion TLS) il est raisonnable d'accepter le message normalement. Aussi, si un ou plusieurs messages périmés arrivent peu après une période hors ligne, l'UAS PEUT accepter le message, mais DEVRAIT avertir l'usager qu'il y a un risque que le message ait été répété.

11.5 Utilisation des corps de message/cpim

Le format message/cpim [RFC3862] permet la protection de métadonnées S/MIME en plus de celle de la charge utile du message lui-même. Dans de nombreux cas, ces métadonnées sont redondantes avec les champs d'en-tête SIP. Cependant, message/cpim ajoute de la valeur en ce que la protection des métadonnées peut s'étendre au travers des frontières du protocole. Par exemple, un corps message/cpim signé peut assurer l'authentification de l'envoyeur en utilisant le champ d'en-tête message/cpim From, même si le message traverse une passerelle vers un autre service de message instantané conforme à CPIM qui ne comprend pas les champs d'en-tête SIP.

12. Considérations relatives à l'IANA

La présente spécification enregistre la méthode MESSAGE dans le registre http://www.iana.org/assignments/sip-parameters/Method, conformément aux informations suivantes :

MESSAGE [RFC3428]

13. Contributeurs

Les personnes suivantes ont apporté des contributions substantielles au présent travail :

Bernard Aboba	Microsoft
Steve Donovan	dynamicsoft
Jonathan Lennox	Columbia University
Dave Oran	Cisco
Robert Sparks	dynamicsoft
Dean Willis	dynamicsoft

14. Remerciements

Les auteurs tiennent à remercier les personnes suivantes de leur soutien au concept de SIP pour IM, de leur soutien au présent travail et de leur utiles commentaires et conseils :

Jon Peterson	NeuStar
Sean Olson	Microsoft
Adam Roach	dynamicsoft
Billy Biggs	University of Waterloo
Stuart Barkley	UUNet
Mauricio Arango	SUN
Richard Shockey	NeuStar
Jorgen Bjorker	Hotsip
Henry Sinnreich	MCI Worldcom
Ronald Akers	Motorola
Torrey Searle	Indigo Software
Rohan Mahy	Cisco
Christian Groves	Ericsson
Allison Mankin	ISI
Tan Ya-Ching	Siemens

15. Références normatives

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

[RFC2778] M. Day, J. Rosenberg et H. Sugano, "Modèle pour Presence et la messagerie instantanée", février 2000. *(Info)*

[RFC2779] M. Day et autres, "Exigences des protocoles Messagerie instantanée / Presence", février 2000. *(Information)*

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

[RFC3265] A.B. Roach, "Notification d'événement spécifique du protocole d'initialisation de session (SIP)", juin 2002.

[RFC3369] R. Housley, "Syntaxe de message cryptographique (CMS)", août 2002. (*Obsolète, voir* RFC3852) *(P.S.)*

16. Références pour information

[AES] Schaad, J. et R. Housley, "Use of the AES Encryption Algorithm and RSA-OAEP Key Transport in CMS", non publiée.

[ARIMP] Crocker, D., Diacakis, A., Mazzoldi, F., Huitema, C., Klyne, G., Rose, M., Rosenberg, J., Sparks, R., Sugano, H. et J. Peterson, "Address Resolution for Instant Messaging and Presence", non publiée.

[RFC3840] J. Rosenberg, H. Schulzrinne et P. Kyzivat, "Indication des capacités d'agent d'utilisateur dans le protocole d'initialisation de session (SIP)", août 2004.

[RFC3841] J. Rosenberg, H. Schulzrinne, P. Kyzivat, "Préférences de l'appelant pour le protocole d'initialisation de session (SIP)", août 2004. *(P.S.)*

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

[ZEPHYR] DellaFera, C., Eichin, M., French, R., Jedlinski, D., Kohl, J. et W. Sommerfeld, "The Zephyr notification service", in USENIX Winter Conference (Dallas, Texas), février 1988.

17. Adresse des auteurs

Ben Campbell
dynamicsoft
5100 Tennyson Parkway
Suite 1200
Plano, TX 75024
mél : bcampbell@dynamicsoft.com

Jonathan Rosenberg
dynamicsoft
72 Eagle Rock Avenue
First Floor
East Hanover, NJ 07936
mél : jdrosen@dynamicsoft.com

Henning Schulzrinne
Columbia University
M/S 0401
1214 Amsterdam Ave.
New York, NY 10027-7003
mél : schulzrinne@cs.columbia.edu

Christian Huitema
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399
mél : huitema@microsoft.com

David Gurle
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399
mél : dgurle@microsoft.com

18. Déclaration complète de droits de reproduction

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