Groupe de travail Réseau
**Request for Comments : 3885**
**RFCmise à jour : 3461**
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

G.E. Allman, Sendmail, Inc.
T. Hansen, AT&T Laboratories

septembre 2004

# Extension au service SMTP pour le suivi de message



**Résumé**
Le présent mémoire définit une extension au service SMTP par laquelle un client peut marquer un message pour le suivre ultérieurement.

## 1. Autres documents et conformité

Le modèle utilisé pour le suivi de message est décrit dans la [RFC3888].

Une interrogation de suivi de message est destinée à être un mécanisme de "dernier recours". Normalement, les notifications d'état de livraison (DSN, *Delivery Status Notification*) [RFC3461] et les notifications de disposition de message (MDN, *Message Disposition Notification*) [RFC3798] devraient fournir le principal état de livraison. C'est seulement si le message n'est pas reçu, ou si il n'y a pas de réponse de l'un de ces mécanismes qu'une interrogation de suivi de message devrait être produite.

La définition du jeton en base64 est importée du paragraphe 6.8 de la [RFC2045]. Formellement,

```
base64 =  %x2b / %x2f / %x30-39 / %x41-5a / %x61-7a
```

La définition du jeton DIGIT *(CHIFFRE)* est importée de la [RFC2822]. Formellement,

```
DIGIT =  %x30-39
```

Dans le présent document, la notation de la syntaxe se conforme à la [RFC2234].

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, [RFC2119].

## 2. Vue d'ensemble de l'extension SMTP

L'extension de service SMTP Suivi de message utilise le mécanisme d'extension de service SMTP décrit dans la [RFC1869]. L'extension de service suivante est définie ici.

(1) Le nom de l'extension de service SMTP est "Suivi de message".

(2) La valeur du mot-clé EHLO associé à cette extension est "MTRK".

(3) Aucun paramètre n'est permis avec cette valeur de mot-clé EHLO. Des documents futurs pourront étendre cette spécification en spécifiant des paramètres pour cette valeur de mot-clé.

(4) Un paramètre facultatif qui utilise le mot-clé "MTRK" est ajouté à la commande MAIL. De plus, le paramètre ENVID de la commande MAIL (telle que définie dans la [RFC3461]) DOIT être pris en charge, avec les extensions décrites ci-dessous. Le paramètre ORCPT de la commande RCPT (telle que définie dans la [RFC3461]) DOIT aussi être pris en charge. Toute la sémantique associée à ENVID et à ORCPT décrite dans la [RFC3461] DOIT être prise en charge au titre de cette extension.

(5) La longueur maximale d'une ligne de commande MAIL est augmentée de 40 caractères par l'ajout possible du mot-clé MTRK et de sa valeur. Noter que l'extension de 507 caractères des commande RCPT pour le paramètre ORCPT et l'extension de 107 caractères des commandes MAIL pour le paramètre ENVID rendues obligatoires par la [RFC3461] doivent aussi être incluses.

(6) Aucun verbe SMTP n'est défini par cette extension.

## 3. Commande MAIL étendue

La commande MAIL étendue est produite par un client SMTP lorsque il souhaite informer un serveur SMTP que les informations de suivi de message devraient être conservées pour des interrogations futures. La commande MAIL étendue est identique à la commande MAIL comme définie dans la [RFC2821], sauf que les paramètres MTRK, ORCPT, et ENVID apparaissent après l'adresse.

### 3.1 Paramètre MTRK sur la commande ESMTP MAIL

Tout envoyeur qui souhaite demander la rétention de données pour le suivi ultérieur de message doit d'abord étiqueter ce message comme traçable en créant deux valeurs A et B :

A = un grand nombre aléatoire
B = SHA1(A)

Le calcul du grand nombre aléatoire A dépend de l'hôte. Voir dans la [RFC1750] une discussion du choix de bons nombres aléatoires. Ce nombre aléatoire DOIT avoir au moins 128 bits mais NE DOIT PAS faire plus de 1024 bits.

Le hachage B de 128 bits de A est alors calculé en utilisant l'algorithme SHA-1 décrit dans [NIST-SHA1].

L'envoyeur code alors en base64 la valeur B et la passe comme mtrk-certifier sur la commande MAIL :

```
mtrk-parameter  = "MTRK=" mtrk-certifier [ ":" mtrk-timeout ]
mtrk-certifier  = base64                          ; authentifiant
mtrk-timeout    = 1*9DIGIT                        ; secondes jusqu'à l'expiration de la temporisation
```

A est mémorisé dans la base de données de suivi de l'origine pour valider les futures demandes de suivi comme décrit dans la [RFC3887]. B est mémorisé dans les bases de données de suivi des MTA receveurs conformes et est utilisé pour authentifier les futures demandes de suivi.

Le champ mtrk-timeout indique le nombre de secondes pendant lequel le client demande que ces informations de suivi soient conservées sur les serveurs intermédiaires, comme mesuré à partir de la demande initiale du message chez ce serveur. Les serveurs PEUVENT ignorer cette valeur si elle viole la politique locale. En particulier, les serveurs PEUVENT appliquer en silence une limite supérieure au temps qu'il vont conserver les données de suivi ; cette limite DOIT être d'au moins un jour.

Si aucun champ mtrk-timeout n'est spécifié, le serveur devrait alors utiliser une valeur par défaut locale. Cette valeur par défaut DEVRAIT être de 8 à 10 jours et DOIT être d'au moins un jour. Malgré cette clause, les informations NE DOIVENT PAS être éliminées alors que le message reste dans la file d'attente pour ce serveur : c'est-à-dire qu'un serveur MTQP NE DOIT PAS dénier la connaissance d'un message alors que ce message se tient dans la file d'attente du MTA.

Si le message est relayé à un autre serveur SMTP conforme, le MTA qui agit comme client DEVRAIT passer un champ mtrk-timeout égal à la durée de vie restante de ces informations de suivi de message. Précisément, la fin de temporisation de suivi est décrémentée du nombre de secondes pendant lesquelles le message a subsisté chez ce MTA et ensuite passé au MTA suivant. Si la temporisation de suivi décrémentée est inférieure ou égale à zéro, le paramètre MTRK entier NE DOIT PAS être passé au prochain MTA ; en fait, le chemin de suivi entier est alors considéré comme perdu.

Voir à la Section 4 de la [RFC2852] une explication de la raison pour laquelle une temporisation est utilisée plutôt qu'un temps absolu.

### 3.2 Utilisation de ENVID

Pour fonctionner correctement, le suivi de message exige que chaque message ait un identifiant unique qui n'est jamais réutilisé par aucun autre message. À cette fin, si le paramètre MTRK est donné, un paramètre ENVID DOIT être inclus, et la syntaxe de ENVID d'après la [RFC3461] est étendue comme suit :

```
envid-parameter = "ENVID=" unique-envid
unique-envid    = local-envid "@" fqhn
local-envid     = xtext
fqhn            = xtext
```

Le unique-envid DOIT être choisi de telle manière que le même ENVID ne soit jamais utilisé par aucun autre message envoyé de ce système ou d'aucun autre système. Dans la plupart des cas, cela signifie de régler fqhn comme étant le nom d'hôte pleinement qualifié du système qui génère cet ENVID, et local-envid comme un identifiant qui ne sera jamais réutilisé par cet hôte.

Dans certains cas, la longueur totale de (local-envid + fqhn + 1) (pour le signe `@') peut excéder la longueur totale acceptable de ENVID (100). Dans ce cas, le fqhn DEVRAIT être remplacé par le SHA1(fqhn) codé en BASE64. Après codage, le SHA-1 de 160 bits sera une chaîne de 27 octets, qui limite local-envid à 72 octets. Les mises en œuvre sont invitées à utiliser pour le local-envid un algorithme qui soit raisonnablement unique. Par exemple, des entiers qui se suivent ont une forte probabilité d'intersection avec des entiers en séquence générés par un hôte différent, mais un SHA-1 de l'heure actuelle enchaîné avec l'adresse IP de l'hôte et un nombre aléatoire a peu de chance de se recouper avec le même algorithme généré par un hôte différent.

Toute resoumission de ce message dans le système de transmission de message DOIT allouer un nouvel ENVID. Dans ce contexte, "resoumission" inclut la transmission ou le renvoi d'un message à partir d'un agent d'utilisateur, mais n'inclut pas l'utilisation d'un nom d'emprunt au niveau du MTA ou la transmission où le message ne quitte et ne réentre pas le système de transmission de message.

### 3.3 Transmission des certificats de suivi

Les MTA DEVRAIENT transmettre des certificats de suivi non expirés aux envoyeurs de message conformes lorsque le message est transféré durant les transferts réguliers de bond en bond. Si le MTA "aval" n'est pas conforme à MTRK, le paramètre MTRK= DOIT être supprimé. Si le MTA aval est conforme à DSN-, les paramètres ENVID et ORCPT NE DOIVENT PAS être supprimés.

Si il survient une dénomination par pseudonyme, une transmission, ou une autre redirection d'un receveur, et si le résultat de la redirection est exactement un receveur, alors le MTA DEVRAIT traiter cela comme un transfert de bond à bond ordinaire et transmettre les valeurs MTRK=, ENVID=, et ORCPT= ; ces valeurs NE DOIVENT PAS être modifiées sauf pour décrémenter le champ mtrk-timeout de la valeur MTRK= , qui DOIT être modifiée comme décrit au paragraphe 4.1.

Les MTA NE DOIVENT PAS copier les certifieurs de MTRK lorsque un receveur utilise un pseudonyme, est retransmis ou autrement redirigé et que la redirection résulte en plus d'un receveur. Cependant, un MTA PEUT désigner un receveur parmi plusieurs comme receveur "principal" auquel les demandes de suivi devront être transmises ; les autres adresses NE DOIVENT PAS recevoir les certificats de suivi. Les MTA NE DOIVENT PAS transmettre les certificats MTRK lorsque ils font une expansion de liste de diffusion.

## 4. Considérations sur la sécurité

### 4.1 Déni de service

Un attaquant pourrait tenter de submerger la base de données d'un serveur en soumettant un grand nombre de petits messages suivis. Dans ce cas, un site peut choisir de diminuer rétroactivement sa période de rétention maximum.

### 4.2 Confidentialité

La valeur mtrk-authenticator ("A") doit être difficile à prédire et ne doit pas être réutilisée.

Le client d'origine doit prendre des précautions raisonnables pour protéger le secret. Par exemple, si le secret est mémorisé dans un magasin de messages (par exemple, un fichier "Envoi") le client doit s'assurer que le secret n'est pas accessible à des attaquants, en particulier sur un magasin partagé.

De nombreux administrateurs de site croient que cacher les noms et la topologie des systèmes et réseaux internes est un dispositif de sécurité important. Les MTA doivent mettre en balance un tel désir avec le besoin de fournir des informations de suivi adéquates.

Dans certains cas, les administrateurs de site peuvent vouloir traiter la livraison à un alias comme une livraison finale afin de séparer les rôles entre les individus. Par exemple, les sites qui utilisent "postmaster" ou "webmaster" comme alias peuvent ne pas souhaiter exposer l'identité de ces individus en permettant le suivi à travers ces alias. Dans d'autres cas, fournir les informations de suivi pour un alias est important, comme lorsque l'alias pointe sur l'adresse publique préférée de l'utilisateur.

Donc, les mises en œuvre sont encouragées à fournir des mécanismes pour que les administrateurs de site puissent choisir entre ces alternatives.

## 5. Considérations relatives à l'IANA

L'IANA a enregistré l'extension SMTP définie à la Section 3.

## 6. Remerciements

Plusieurs personnes ont commenté et ont amélioré le présent document, parmi lesquelles Philip Hazel, Alexey Melnikov, Lyndon Nerenberg, Chris Newman, et Gregory Neil Shapiro.

## 7. Références

### 7.1 Références normatives

[NIST-SHA1] NIST FIPS PUB 180-1, "Secure Hash Standard", National Institute of Standards and Technology, U.S. Department of Commerce, mai 1994.

[RFC1869] J. Klensin, N. Freed, M. Rose, E. Stefferud, D. Crocker, "Extensions de service à SMTP", novembre 1995. (*Obsolète, voir* RFC5321)

[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*.)*

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

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

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

[RFC2822] P. Resnick, "Format de message Internet", avril 2001. *(Remplace la* RFC0822*, STD 11, Remplacée par* RFC5322*)*

[RFC3887] T. Hansen, "Protocole d'interrogation de suivi de message", septembre 2004. *(P.S.)*

[RFC3888] T. Hansen, "Modèle et exigences du suivi de message", septembre 2004. *(Information)*

### 7.2 Références pour information

[RFC1750] D. Eastlake 3rd et autres, "Recommandations d'aléa pour la sécurité", décembre 1994. *(Info., remplacée par la* RFC4086)

[RFC2852] D. Newman, "Extension de service SMTP Livraison par", juin 2000. *(P.S.)*

[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.)*

[RFC3798] T. Hansen et G. Vaudreuil, éd., "Notification de disposition de message", mai 2004. (*MàJ par* RFC5337, RFC6533) *(D.S.)*

## 8. Adresses des auteurs

Eric Allman
Sendmail, Inc.
6425 Christie Ave, 4th Floor
Emeryville, CA 94608
U.S.A.
téléphone : +1 510 594 5501
Fax: +1 510 594 5429
mél : eric@Sendmail.COM

Tony Hansen
AT&T Laboratories
Middletown, NJ 07748
U.S.A.
téléphone : +1 732 420 8934
mél : tony+msgtrk@maillennium.att.com

## 9. Déclaration complète de droits de reproduction



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