Équipe d'ingénierie de l'Internet (IETF)
Request for Comments : 6409
STD 72
RFC rendue obsolète : 4409
Catégorie : Sur la voie de la normalisation
ISSN: 2070-1721

R. Gellens, QUALCOMM Incorporated
J. Klensin

novembre 2011

Traduction Claude Brière de L'Isle

Soumission de message pour la messagerie

Résumé
Le présent mémoire sépare la soumission de message du relais de message, permettant à chaque service de fonctionner selon ses propres règles (pour la sécurité, la politique, etc.) et spécifie quelles actions sont à effectuer par un serveur de soumission.

Le relais de message n'est pas affecté, et continue d'utiliser SMTP sur l'accès 25.

Lorsque elle se conforme au présent document, la soumission de message utilise le protocole spécifié ici, normalement sur l'accès 587.

Cette séparation des fonctions offre un certain nombre d'avantages, incluant la capacité d'appliquer des exigences de sécurité ou de politique spécifiques.

Statut de ce mémoire
Ceci est un document de l'Internet sur la voie de la normalisation.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Tous les documents approuvés par l'IESG ne sont pas candidats à devenir une norme de l'Internet ; voir la Section 2 de la RFC5741.

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à http://www.rfc-editor.org/info/rfc6409

Table des matières

1. Introduction....2
2. Informations sur le document....3
  2.1 Définitions des termes utilisés dans le présent mémoire....3
  2.2 Conventions utilisées dans le document....3
3. Soumission de message....3
  3.1 Identification de soumission....3
  3.2 Rejet et rebond de message....4
  3.3 Soumission autorisée....4
4. Actions obligatoires....5
  4.1 Code général de rejet de soumission....5
  4.2 S'assurer que tous les domaines sont pleinement qualifiés....5
  4.3 Authentification exigée....5
5. Actions recommandées....5
  5.1 Appliquer la syntaxe d'adresse....5

5.2. Enregistrement des erreurs....6
5.3 Appliquer de plus courtes temporisations....6
6. Actions facultatives....6
6.1 Appliquer les droits de soumission....6
6.2 Appliquer les permissions....6
6.3 Vérifier les données du message....6
6.4 Prise en charge de l'adresse du maître de poste....7
6.5 Ajustement des codages de caractères....7
7. Interaction avec les extensions SMTP....7
8. Modifications de message....8
8.1 Ajout d'envoyeur....8
8.2 Ajout de date....8
8.3 Ajout de l'identifiant de message....8
8.4 Codage de transfert....8
8.5 Signature de message....8
8.6 Chiffrement de message....9
8.7 Résolution des alias....9
8.8 Réécriture d'en-tête....9
9. Considérations sur la sécurité....9
10. Considérations relatives à l'IANA....10
11. Remerciements....10
12. Références....10
12.1 Références normatives....10
12.2 Références pour information....10
Appendice A. Changements majeurs par rapport à la RFC 4409....12
Adresse des auteurs....12

1. Introduction

SMTP [RFC5321] a été défini comme un protocole de *transfert* de message, c'est-à-dire, comme un moyen d'acheminer (si nécessaire) et livrer des messages finis (complets).

Les agents de transfert de message (MTA, *Message Transfer Agent*) ne sont pas supposés altérer le texte du message, sauf pour y ajouter 'Received', 'Return-Path', et autres champs d'en-tête exigés par la [RFC5321]. Cependant, SMTP est maintenant largement utilisé comme protocole de *soumission* de message, c'est-à-dire, un moyen pour les agents d'utilisateur de message (MUA, *Message User Agent*) d'introduire de nouveaux messages dans le réseau d'acheminement du MTA. Le processus qui accepte les soumissions de message à partir des MUA est appelé agent de soumission de message (MSA, *Message Submission Agent*).

Afin de permettre des communications sans contraintes, SMTP n'est souvent pas authentifié durant le relais de message

L'authentification et l'autorisation des soumissions initiales sont devenues d'une importance croissante, amenée par des changements des exigences de sécurité et une augmentation des attentes pour que les serveurs de soumission prennent la responsabilité du trafic de messages qu'ils génèrent.

Par exemple, du fait de la prévalence de machines qui sont infectées de vers, virus, ou autres logiciels malfaisants qui génèrent de grandes quantités de pourriels, de nombreux sites interdisent maintenant le trafic sortant sur l'accès SMTP standard (accès 25) passant en entonnoir toutes les soumissions de messagerie à travers des serveurs de soumission.

En plus des questions d'authentification et d'autorisation, les messages soumis sont dans certains cas des messages finis (complets) et dans d'autres cas, ils sont non finis (incomplets) sous un ou plusieurs aspects. Les messages non finis peuvent devoir être complétés pour s'assurer de leur conformité à la spécification de format de message [RFC5322], et aux exigences qui s'y rapportent. Par exemple, le message peut n'avoir pas de champ d'en-tête 'Date' approprié, et les domaines peuvent n'être pas pleinement qualifiés. Dans certains cas, le MUA peut être incapable de générer des messages finis (par exemple, il pourrait ne pas connaître sa zone horaire). Même lorsque les messages présentés sont complets, la politique du site local peut imposer que le texte du message soit examiné ou modifié d'une certaine façon, par exemple, pour dissimuler le nom local ou les espaces d'adresse. Il a été montré que de tels compléments ou modifications causent des dommages lorsqu'ils sont effectués par les MTA d'aval – c'est-à-dire, les MTA après le MTA de soumission du premier bond – et sont

en général considérés comme en-dehors du domaine de la fonction de MTA normalisé.

Séparer les messages en soumissions et transferts permet aux développeurs et administrateurs de réseau de faire plus facilement ce qui suit :
- o mettre en œuvre les politiques de sécurité et se garder contre le relais de messagerie non autorisé ou l'injection de messagerie brute non sollicitée,
- o mettre en œuvre la soumission authentifiée, y compris la soumission hors site par des utilisateurs autorisés comme les voyageurs,
- o Séparer les différences de code des logiciels pertinents, rendant par là chaque base de code plus directe et permettant des programmes différents pour le relais et la soumission,
- o détecter les problèmes de configuration avec les clients de messagerie d'un site,
- o fournir à l'avenir une base pour l'ajout de services de soumission améliorés.

Le présent mémoire décrit des moyens déterministes de faible coût pour identifier les messages comme soumissions, et spécifie les actions à prendre par un serveur de soumission.

2. Informations sur le document

2.1 Définitions des termes utilisés dans le présent mémoire

Beaucoup des concepts et termes utilisés dans ce document sont définis dans la [RFC5321] ; on suppose que le lecteur s'est familiarisé avec ces documents.

Pleinement qualifié : contenant ou consistant en un domaine qui peut être globalement résolu en utilisant le service de nom de domaine ; c'est à dire, pas un alias local, ni une spécification partielle.

Agent de soumission de message (MAS, *Message Submission Agent*) : processus qui se conforme à la présente spécification. Un MSA agit comme serveur de soumission pour accepter des messages des MUA, et les livre ou agit comme un client SMTP pour les relayer à un MTA.

Agent de transfert de message (MTA, *Message Transfer Agent*) : processus qui se conforme à la [RFC5321]. Un MTA agit comme un serveur SMTP pour accepter des messages d'un MSA ou d'un autre MTA, et soit les livre, soit agit comme un client SMTP pour les relayer à un autre MTA.

Agent d'utilisateur de message (MUA, *Message User Agent*) : processus qui agit (souvent au nom d'un utilisateur et avec une interface d'utilisateur) pour composer et soumettre de nouveaux messages, et traite les messages livrés.

Pour les messages délivrés, le MUA receveur peut obtenir le message et le traiter conformément aux conventions locales, ou bien, dans ce qu'on appelle habituellement le modèle MUA partagé, le protocole Post Office [RFC1939] ou IMAP [RFC3501] est utilisé pour accéder aux messages livrés, tandis que le protocole défini ici (ou SMTP) est utilisé pour soumettre les messages.

2.2 Conventions utilisées dans le document

Les exemples utilisent le domaine 'exemple.net'.

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

3. Soumission de message

3.1 Identification de soumission

L'accès 587 est réservé aux soumissions de messages électroniques comme spécifié dans le présent document. Les messages reçus sur cet accès sont définis comme des soumissions. Le protocole utilisé est ESMTP [RFC5321], avec des restrictions ou tolérances supplémentaires comme spécifié ici.

Bien que la plupart des clients et serveurs de messagerie électronique puissent être configurés pour utiliser l'accès 587 au lieu de 25, il y a des cas où cela n'est pas possible ou pratique. Un site PEUT choisir d'utiliser l'accès 25 pour la soumission de message, en désignant certains hôtes comme des MSA et d'autres comme des MTA.

3.2 Rejet et rebond de message

Les MTA et MSA PEUVENT mettre en œuvre des règles de rejet de message qui s'appuient en partie sur le fait que le message est en soumission ou en relais.

Par exemple, certains sites peuvent configurer leurs MTA à rejeter toutes les commandes RCPT pour les messages qui ne font pas référence aux utilisateurs locaux, et configurer leur MSA à rejeter toutes les soumissions de message qui ne proviennent pas d'utilisateurs autorisés, avec une autorisation fondée soit sur l'identité authentifiée, soit sur le fait que le point d'extrémité de soumission est au sein d'un environnement IP protégé.

Note : Il est préférable de rejeter un message que de courir le risque d'en envoyer un endommagé. Ceci est particulièrement vrai pour les problèmes qui peuvent être corrigés par le MUA, par exemple, un champ 'From' invalide.

Si un MSA n'est pas capable de déterminer un chemin de retour vers l'utilisateur de soumission, à partir d'un MAIL FROM valide, d'une adresse IP de source valide, ou fondé sur une identité authentifiée, le MSA DEVRAIT alors immédiatement rejeter le message. Un message peut être immédiatement rejeté en retournant un code 550 à la commande MAIL.

Noter qu'un chemin de retour nul, c'est-à-dire, MAIL FROM:<>, est permis et NE DOIT PAS être par lui-même cause du rejet d'un message. (Les MUA n'ont pas besoin de générer de messages de chemin de retour nul pour diverses raisons, y compris les notifications de disposition.)

Excepté dans le cas où le MSA est incapable de déterminer un chemin de retour valide pour le message présenté, le texte de la présente spécification qui donne pour instruction à un MSA de produire un code de rejet PEUT être respecté en acceptant le message et en générant ensuite un message en rebond. (C'est à dire que si le MSA va rejeter un message pour toute raison excepté celle d'être incapable de déterminer un chemin de retour, il a la faculté de faire un rejet immédiat ou d'accepter le message et d'envoyer ensuite un rebond.)

Note : Dans le cas normal de soumission de message, on préfère le rejet immédiat du message, car cela donne à l'utilisateur et au MUA un retour d'information direct. Pour traiter correctement les rebonds différés, le MUA client a besoin d'entretenir une file d'attente des messages qu'il a soumis, et de leur confronter les rebonds. Noter que beaucoup de MUA actuels n'ont pas cette capacité.

3.3 Soumission autorisée

De nombreuses méthodes ont été utilisées pour s'assurer que seuls les utilisateurs autorisés sont capables de soumettre des messages. Parmi ces méthodes figurent SMTP authentifié, les restrictions d'adresse IP, IP sécurisé et autres tunnels, et l'authentification POP préalable.

SMTP authentifié [RFC4954] a connu un large développement. Il permet au MSA de déterminer une identité d'autorisation pour la soumission du message, qui n'est pas liée à d'autres protocoles.

Les restrictions d'adresse IP sont très largement mises en œuvre, mais ne permettent pas les situations de voyage et similaires, et peuvent être facilement usurpées si tous les chemins de transport entre le MUA et le MSA ne sont pas de confiance.

IP sécurisé [RFC4301], et autres techniques de tunnelage chiffré et authentifié, peut aussi être utilisé et procure les avantages supplémentaires de la protection contre l'espionnage et l'analyse de trafic.

Exiger une authentification POP [RFC1939] (à partir de la même adresse IP) dans un certain délai (par exemple, 20 minutes) avant le début d'une session de soumission de message a aussi été utilisé, mais cela impose des restrictions sur les clients aussi bien que sur les serveurs, ce qui peut causer des difficultés. En particulier, le client doit faire une authentification POP avant une session de soumission SMTP, et tous les clients ne sont pas capables de le faire ni configurés pour cela. De plus, le MSA doit se coordonner avec le serveur POP, ce qui peut être difficile. Il y a aussi une

fenêtre pendant laquelle un utilisateur non autorisé peut soumettre des messages et apparaître ensuite comme un utilisateur précédemment autorisé. Comme cela dépend des adresses IP du MUA, cette technique est par nature aussi sujette à usurpation d'adresse IP que la validation fondée sur les seules adresses IP connues (voir ci-dessus).

4. Actions obligatoires

Un MSA DOIT faire tout ce qui suit :

4.1 Code général de rejet de soumission

Sauf s'il est couvert par un code de réponse plus précis, le code de réponse 554 doit être utilisé pour rejeter une commande MAIL, RCPT, ou DATA qui contient quelque chose d'impropre.

4.2 S'assurer que tous les domaines sont pleinement qualifiés

Le MSA DOIT s'assurer que tous les domaines de l'enveloppe SMTP sont pleinement qualifiés.

Si le MSA examine ou altère de quelque façon le texte du message, sauf pour ajouter des champs d'en-tête trace [RFC5321], il DOIT s'assurer que tous les domaines dans les champs d'en-tête d'adresse sont pleinement qualifiés.

Le code de réponse 554 est à utiliser pour rejeter une commande MAIL, RCPT, ou DATA qui contient des références de domaine impropres.

Une convention locale fréquente est d'accepter des domaines d'un seul niveau (par exemple, 'soldes') et ensuite d'étendre la référence en ajoutant la portion restante du nom de domaine (par exemple, à 'soldes.exemple.net'). Les conventions locales qui permettent des domaines à un seul niveau DEVRAIENT rejeter, plutôt qu'étendre, les domaines multi niveaux incomplets (par exemple, 'criardes.soldes') car des telles extensions sont particulièrement risquées.

4.3 Authentification exigée

Le MSA DOIT, par défaut, produire une réponse d'erreur à la commandse MAIL si la session n'a pas été authentifiée en utilisant la [RFC4954], sauf si elle a déjà établi de façon indépendante l'authentification ou l'autorisation (comme en étant dans un sous réseau protégé).

Le paragraphe 3.3 discute les mécanismes d'authentification.

Le code de réponse 530 [RFC4954] est utilisé à cette fin.

5. Actions recommandées

Le MSA DEVRAIT faire tout ce qui suit.

5.1 Appliquer la syntaxe d'adresse

Un MSA DEVRAIT rejeter les messages qui ont une syntaxe illégale dans l'adresse d'enveloppe SMTP d'envoyeur ou de receveur.

Si le MSA examine ou altère de quelque façon le texte du message, excepté pour ajouter des champs d'en-tête Trace, il DEVRAIT rejeter les messages avec une syntaxe d'adresse illégale dans les champs d'en-tête d'adresse.

Le code de réponse 501 est à utiliser pour rejeter une commande MAIL ou RCPT qui contient une adresse impropre détectable.

Lorsque les adresses sont résolues après soumission du corps de message, le code de réponse 554 (avec un code d'état

amélioré convenable d'après la [RFC3463]) est utilisé après la fin des données, si le message contient des adresses invalides dans l'en-tête.

5.2. Enregistrement des erreurs

Le MSA DEVRAIT enregistrer les erreurs de message, et en particulier les mauvaises configurations apparentes de logiciel client.

Il peut être très utile de notifier à l'administrateur le moment où des problèmes sont détectés avec des clients de messagerie locaux. C'est un des autres avantages de la distinction entre soumission et relais : les administrateurs de système peuvent s'intéresser aux problèmes de configuration locale, mais sans s'occuper des problèmes des clients sur d'autres sites.

Noter qu'il est important d'imposer des limites à de tels enregistrements pour empêcher certaines formes d'attaque de déni de service (DoS).

5.3 Appliquer de plus courtes temporisations

Les temporisations spécifiées au paragraphe 4.5.3.2 de la [RFC5321] sont conçus pour traiter les nombreux types de situations qui peuvent se rencontrer dans l'Internet public. La relation entre les clients et les serveurs qui correspondent à la présente spécification est normalement beaucoup plus étroite et plus prévisible. Les clients de soumission se comportent différemment des client de relais dans certains domaines, en particulier la tolérance aux fins de temporisation. En pratique, les clients de soumission de messages tendent à avoir de courtes temporisations (peut-être de 2 à 5 minutes pour une réponse à toute commande). Les serveurs de soumission DEVRAIENT répondre à toute commande (même DATA) en moins de 2 minutes.

Quand le serveur de soumission a une fermeture administrative et/ou une relation réseau avec le ou les clients de soumission – par exemple, avec une interface de messagerie électronique qui appelle sur un serveur de soumission étroitement lié – un accord mutuel sur des temporisations beaucoup plus courtes PEUT être approprié.

6. Actions facultatives

Le MSA PEUT faire tout ce qui suit :

6.1 Appliquer les droits de soumission

Le MSA PEUT produire une réponse d'erreur à une commande MAIL si l'adresse dans MAIL FROM paraît avoir des droits de soumission insuffisants, ou n'est pas autorisée avec l'authentification utilisée (si la session a été authentifiée).

Le code de réponse 550 avec un code d'état amélioré approprié selon la [RFC3463], comme 5.7.1, est utilisé à cette fin.

6.2 Appliquer les permissions

Le MSA PEUT produire une réponse d'erreur à une commande RCPT si elle n'est pas cohérente avec les permissions données à l'utilisateur (si la session a été authentifiée).

Le code de réponse 550 avec un code d'état amélioré approprié selon la [RFC3463], comme 5.7.1, est utilisé à cette fin.

6.3 Vérifier les données du message

Le MSA PEUT produire une réponse d'erreur à la commande DATA ou envoyer un résultat d'échec après fin des données si le message présenté est syntaxiquement invalide, semble incohérent avec les permissions données à l'utilisateur (si elles sont connues) ou viole d'une façon ou d'une autre la politique du site.

Le code de réponse 554 est utilisé pour des problèmes de syntaxe dans les données. Le code de réponse 501 est utilisé si la commande elle-même n'est pas syntaxiquement valide. Le code de réponse 550 avec un code d'état amélioré approprié

selon la [RFC3463] (comme 5.7.1) est utilisé pour rejeter sur la base de l'utilisateur qui soumet. Le code de réponse 550 avec un code d'état amélioré approprié (comme 5.7.0) est utilisé si le message viole la politique du site.

6.4 Prise en charge de l'adresse du maître de poste

Si c'est approprié d'après les conditions locales et pour faciliter la conformité aux exigences du "maître de poste" de la [RFC5321], le MSA PEUT permettre un degré réduit d'authentification pour la messagerie adressée au "maître de poste" (ou une de ses appellations équivalentes, voir la [RFC5321]) dans un ou plusieurs domaines, par rapport aux exigences mises en application pour les autres adresses. Entre autres avantages, cela donne une adresse qui peut être utilisée en dernier ressort par les utilisateurs autorisés pour rapporter des problèmes qui les empêcheraient autrement de présenter des messages.

6.5 Ajustement des codages de caractères

Sous réserves des limites imposées par d'autres protocoles et spécifications, le MSA PEUT convertir les jeux de caractères ou codages de chaînes pour améliorer l'utilité des messages, la probabilité de livraison, ou la conformité à d'autres spécifications ou recommandations. De telles conversions PEUVENT inclure, quand nécessaire, le remplacement des adresses dont le codage ne se conforme pas à la RFC 5321, par d'autres qui s'y conforment, en utilisant des informations disponibles hors bande.

7. Interaction avec les extensions SMTP

Le tableau suivant fait la liste des extensions SMTP actuellement sur la voie de la normalisation et expérimentales dont les documents ne spécifient pas explicitement leur applicabilité au présent protocole. Figurent sur la liste le mot clé du EHLO, le nom et une indication sur l'utilisation de l'extension sur l'accès de soumission, et une référence.

Mot clé	**Nom**	**Soumission**	**Référence**
PIPELINING	Intubage	DEVRAIT	[RFC2920]
ENHANCEDSTATUSCODES	Codes d'état améliorés	DEVRAIT	[RFC2034]
ETRN	Extension de tour	NE DOIT PAS	[RFC1985
...	Extension de codes	DEVRAIT	[RFC3463]
DSN	Notification d'état de livraison	DEVRAIT	[RFC3461]
SIZE	Taille de message	PEUT	[RFC1870]
...	Code de réponse 521	NE DOIT PAS	[RFC1870]
CHECKPOINT	Point de vérifiation/Redémarrage	PEUT	[RFC1845]
BINARYMIME	MIME binaire	PEUT	[RFC3030]
CHUNKING	Tronquage	PEUT	[RFC3030]
8BITMIME	Usage de données en 8 bits	DEVRAIT	[RFC6152]
AUTH	Authentification	DOIT	[RFC4904]
STARTTLS	Débuter TLS	PEUT	[RFC3207]
NO-SOLICITING	Notification de non sollicitation	PEUT	[RFC3865]
MTRK	Traçage de message	PEUT	[RFC3885]
ATRN	Relais à la demande	NE DOIT PAS	[RFC2645]
DELIVERBY	Livré par	PEUT	[RFC2852]
CONPERM	Permission de conversion de contenu	PEUT	[RFC4141]
CONNEG	Négociation de conversion de contenu	PEUT	[RFC4141]

Tableau 1

Les futures extensions SMTP DEVRAIENT explicitement spécifier si elles sont valides sur l'accès de soumission.

Certaines extensions SMTP sont particulièrement utiles pour la soumission de message.

Les codes d'état étendu [RFC3463] DEVRAIENT être pris en charge et utilisés conformément à la [RFC2034]. Cela permet au MSA de notifier au client des problèmes spécifiques de configuration ou autres avec plus de détails que dans les codes de réponse dont la liste figure dans le présent mémoire. Comme certaines causes de rejet sont en rapport avec la politique de sécurité du site, il faut veiller à ne pas divulguer plus de détails que nécessaire à des envoyeurs non

authentifiés.

La [RFC2920] DEVRAIT être prise en charge par le MSA.

La [RFC4954] permet au MSA de valider l'autorité et de déterminer l'identité de l'usager soumettant et DOIT être prise en charge par le MSA.

La [RFC3207] est le mécanisme le plus largement utilisé, au moment de la rédaction du présent document, qui permet au MUA et MSA de protéger l'intégrité et la confidentialité de la soumission de message.

Toute référence à la commande DATA dans le présent mémoire se réfère aussi à tout substitut pour DATA, comme la commande BDAT utilisée avec la [RFC3030].

8. Modifications de message

Les sites PEUVENT modifier les soumissions pour s'assurer de la conformité aux normes et à la politique du site. La présente section décrit un certain nombre de ces modifications qui sont souvent considérées comme utiles.

Note : À titre de guide pour que les décisions locales mettent en œuvre les modifications de message, une règle très importante est de limiter de telles actions à remédier à des problèmes spécifiques qui ont des solutions claires. Ceci est particulièrement vrai avec les éléments d'adresse. Par exemple, ajouter sans discrimination un domaine à une adresse ou élément d'adresse qui n'en a pas a pour résultat typique une augmentation des adresses qui ne vont pas. Une adresse non qualifiée doit être vérifiée comme étant une partie locale valide dans le domaine avant de pouvoir ajouter le domaine en toute sécurité.

Tout message transmis ou livré par le MSA DOIT se conformer aux exigences des [RFC5321] et [RFC5322] ou aux exigences permises par les extensions qui sont supportées par le MSA et acceptées par le serveur de prochain bond.

La modification de message peut affecter la validité d'une signature d'un message existant, comme par la messagerie identifiée par clés de domaines (DKIM, *DomainKeys Identified Mail*) [RFC6376], Pretty Good Privacy (PGP) [RFC4880], ou MIME sécurisé (S/MIME) [RFC5751], et peur rendre la signature invalide. Cela à son tour, peut affecter le traitement du message par les receveurs ultérieurs, comme les moteurs de filtrage qui examinent la présence ou l'absence d'une signature valide.

8.1 Ajout d'envoyeur

Le MSA PEUT ajouter ou remplacer le champ 'Sender' *(envoyeur)*, si l'identité de l'envoyeur est connue et n'est pas donnée dans le champ 'From' *(en provenance de)*.

Le MSA DOIT s'assurer que toute adresse qu'il place dans un champ 'Sender' est en fait une adresse de messagerie valide.

8.2 Ajout de date

Le MSA PEUT ajouter un champ 'Date' au message soumis, s'il n'en a pas, ou corriger le champ 'Date' s'il ne se conforme pas à la syntaxe de la [RFC5322].

8.3 Ajout de l'identifiant de message

Le MSA DEVRAIT ajouter ou remplacer le champ 'Message-ID' *(identifiant de message)*, s'il n'en a pas, ou si sa syntaxe n'est pas valide (comme défini dans la [RFC5322]). Noter qu'un certain nombre de clients ne génèrent toujours pas de champs Message-ID.

8.4 Codage de transfert

Le MSA PEUT appliquer le codage de transfert au message conformément aux conventions MIME, si nécessaire et non dommageable au type MIME.

8.5 Signature de message

Le MSA PEUT (numériquement) signer ou ajouter autrement des informations d'authentification au message.

8.6 Chiffrement de message

Le MSA PEUT chiffrer le message pour le transport pour refléter les politiques organisationnelles.

Note : Pour être utile, l'ajout d'une signature et/ou du chiffrement par le MSA implique généralement que la connexion entre le MUA et le MSA doive être elle-même sécurisée par d'autres moyens, par exemple, en fonctionnant à l'intérieur d'un environnement de confiance, en sécurisant la connexion de soumission à la couche transport, ou en utilisant un mécanisme de la [RFC4954] qui fournisse l'intégrité de session.

8.7 Résolution des alias

Le MSA PEUT résoudre et réécrire les alias (par exemple, les enregistrements de nom canonique (CNAME)) pour les noms de domaine, dans l'enveloppe SMTP et/ou dans les champs d'adresse de l'en-tête, sous réserve de la politique locale.

Note : SMTP [RFC5321] interdit l'utilisation d'alias de nom de domaine dans les adresses et dans l'annonce d'ouverture de session. Comme avec les autres exigences SMTP, la RFC 5321 interdit effectivement à un MSA de transmettre de tels messages dans l'Internet public. Néanmoins, la résolution inconditionnelle des alias pourrait être dommageable. Par exemple, si www.exemple.net et ftp.exemple.net sont tous deux des alias pour mail.exemple.net, les réécrire pourrait perdre des informations utiles.

8.8 Réécriture d'en-tête

Le MSA PEUT réécrire les parties locales et/ou de domaines dans l'enveloppe SMTP, et facultativement dans les champs d'adresse de l'en-tête, conformément à la politique locale. Par exemple, un site peut préférer réécrire 'JRU' sous la forme 'J.Random.User' afin de cacher les noms de connexion, et/ou de réécrire 'criardes.soldes.exemple.net' sous la forme 'zyx.exemple.net' pour cacher les noms de machines et rouler plus facilement les usagers.

Cependant, seules les adresses, les parties locales, ou les domaines qui correspondent à des réglages spécifiques de configuration de MSA locale devraient être altérés. Il serait très dangereux pour le MSA d'appliquer des règles de réécriture indépendantes des données, comme de toujours supprimer le premier élément d'un nom de domaine. Ainsi, par exemple, une règle qui ôte l'élément le plus à gauche du domaine, si le nom de domaine complet correspond à '*.foo.exemple.net', serait acceptable.

Le MSA NE DOIT PAS réécrire une adresse (de destination) pointant vers l'avant d'une façon qui viole les contraintes de la [RFC5321] sur la modification des parties locales. Les changements à l'adressage et au codage, effectués en conjonction avec l'action du paragraphe 6.5, ne violent pas ce principe si le MSA a des informations suffisantes disponibles pour appliquer la substitution avec succès et précision.

9. Considérations sur la sécurité

La séparation de la soumission et du relais des messages permet à un site de mettre en œuvre des politiques différentes pour les deux types de services, y compris de requérir l'utilisation de mécanismes de sécurité supplémentaires pour l'un ou pour les deux. Il peut faire cela d'une façon plus simple, à la fois techniquement et administrativement. Cela accroît la probabilité d'une application correcte des politiques.

La séparation peut aussi aider à traquer et prévenir les envois de messagerie électronique en vrac non sollicités.

Par exemple, un site pourrait configurer ses serveurs de messagerie de telle façon que le MSA exige l'authentification avant d'accepter un message, et que le MTA rejette toutes les commandes RCPT pour les utilisateurs non locaux. Ceci peut être un élément important de la politique de sécurité totale de messagerie d'un site.

Si un site ne parvient pas à exiger une forme quelconque d'autorisation pour les soumissions de message (voir l'exposé au paragraphe 3.3) il permet l'usage ouvert de ses ressources et de son nom ; de la messagerie électronique en vrac non sollicitée peut être injectée en utilisant ses facilités.

La Section 3 comporte un exposé plus détaillé des problèmes de certaines méthodes d'authentification.

Le paragraphe 5.2 comporte une note d'avertissement sur le fait que l'absence de limitations de connexion peut permettre certaines formes d'attaques de déni de service.

10. Considérations relatives à l'IANA

Les entrées du Tableau 1 ont été corrigées (référence pour NO-SOLICITING) et étendues (ATRN, DELIVERBY, CONPERM, et CONNEG). Le registre des "Extensions de service SMTP" a été mis à jour pour refléter les entrées changées et nouvelles. Les entrées du registre qui n'apparaissent pas dans le tableau ci-dessus sont correctes et ne devraient pas être altérées.

L'entrée dans le registre des "Extensions de service SMTP" pour la RFC 4409 a été mis à jour pour faire référence au présent document. La référence originale pour la soumission (RFC2476) qui aurait dû être corrigée plus tôt, a aussi été mise à jour pour pointer sur le présent document.

L'entrée dans le "Registre des noms de service et des numéros d'accès de protocole de transport" pour l'accès 587 a été mise à jour pour pointer sur le présent document.

11. Remerciements

La préparation et le développement de la version actuelle de cette spécification a été stimulée par les discussions au sein des groupes de travail YAM et EAI de l'IETF. Dave Crocker, Subramanian Moonesamy, Barry Leiba, John Levine, et d'autres ont fourni du texte qui apparaît dans ce document ou dans les versions qui y ont conduit.
Nathaniel Borenstein et Barry Leiba ont été les instruments du développement de la RFC 4409, la mise à jour de la RFC2476.
Le mémoire original (RFC 2476) a été développé, en partie, sur la base des commentaires et discussions qui ont eu lieu sur la liste de diffusion IETF-Submit. L'aide de ceux qui ont pris de leur temps pour relire ce document et faire des suggestions a été appréciée, en partieculier celle de Dave Crocker, Ned Freed, Keith Moore, John Myers, et Chris Newman.
Des remerciements particuliers à Harald Alvestrand, qui est au démarrage de cet effort.

12. Références

12.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC4954] R. Siemborski et A. Melnikov, éd., "Extension de service à SMTP pour l'authentification", juillet 2007. (*Remplace* RFC2554) (*MàJ* RFC3463) (*MàJ par* RFC5248) *(P.S.)*

[RFC5321] J. Klensin, "Protocole simple de transfert de messagerie (SMTP)", octobre 2008. (*Remplace* RFC2821) (*MàJ* RFC1123) *(D.S.)*

12.2 Références pour information

[RFC1845] D. Crocker, N. Freed, A. Cargille, "Extension de service SMTP pour point de contrôle/redémarrage", septembre 1995. *(Expérimentale)*

[RFC1846] A. Durand, F. Dupont, "Code de réponse SMTP 521", septembre 1995. *(Expérimentale)*

[RFC1870] J. Klensin, N. Freed, K. Moore, "Extensions de service à SMTP pour déclaration de taille de message", novembre 1995. (STD0010)

[RFC1939] J. Myers, M. Rose, "Protocole Post Office - version 3", mai 1996. (*MàJ par* RFC1957, 2449, 8314) (STD0053)

[RFC1985] J. De Winter, "Extension de service SMTP pour débuter la file d'attente de messages distants", août 1996. *(P.S.)*

[RFC2034] N. Freed, "Extension de service SMTP pour le retour de codes d'erreur améliorés", octobre 1996. *(P.S.)*

[RFC2645] R. Gellens, "Relais de messagerie à la demande (ODMR) pour SMTP avec adresses IP dynamiques", août 1999. *(P.S.)*

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

[RFC2920] N. Freed, "Extension de service SMTP pour le traitement de commandes en parallèle", septembre 2000. (STD0060)

[RFC3030] G. Vaudreuil, "Extensions de service SMTP pour la transmission de grands messages MIME binaires", décembre 2000. *(P.S.)*

[RFC3207] P. Hoffman, "Extension de service SMTP pour un SMTP sécurisé sur TLS", février 2002. *(P.S., MàJ par* RFC7817)

[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, RFC8098) *(D.S.)*

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

[RFC3501] M. Crispin, "Protocole d'accès au message Internet - version 4rev1", mars 2003. *(P.S. ; MàJ par* RFC4466, 4469, 4551, 5032, 5182, 7817, 8314, 8437, 8474)

[RFC3865] C. Malamud, "Extension de service Pas de démarchage du protocole simple de transfert de messagerie (SMTP)", septembre 2004. *(P.S.)*

[RFC3885] E. Allman, T. Hansen, "Extension de service SMTP pour le suivi de message", septembre 2004. *(P.S.)*

[RFC4141] K. Toyoda, D. Crocker, "Extensions SMTP et MIME pour conversion de contenu", novembre 2005. *(P.S.)*

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005. *(P.S.) (Remplace la* RFC2401)

[RFC4880] J. Callas et autres, "Format de message OpenPGP", novembre 2007. (*Remplace* RFC1991, RFC2440) *(P.S.)*

[RFC5322] P. Resnick, éd., "Format du message Internet", octobre 2008. (*Remplace* RFC2822) (MàJ RFC4021) *(D.S.)*

[RFC5751] B. Ramsdell, S. Turner, "Spécification du message des extensions de messagerie Internet multi objets sécurisée (S/MIME) version 3.2", janvier 2010. (*Remplace* RFC3851). *(P. S. ; Remplacée par* RFC8551*)*

[RFC6152] J. Klensin et autres, "Extension du service SMTP pour le transport MIME à 8 bits", mars 2011. (*Remplace la* RFC1652) (aussi STD0071)

[RFC6376] D. Crocker, T. Hansen, M. Kucherawy, "Signatures de messagerie identifiées par clés de domaine (DKIM)", septembre 2011. (*Remplace les* RFC4871 et RFC5672) *(D.S. ; MàJ par* RFC8301)

Appendice A. Changements majeurs par rapport à la RFC 4409

Le protocole spécifié par ce document n'est pas substantiellement différent de celui de la RFC 4409. Cependant, la présente spécification contient plusieurs précisions et mises à jour pour refléter des changements et des révisions sur d'autres documents ultérieurs à la publication de la RFC 4409. Les changements spécifiques suivants pourront intéreser certains lecteurs.

- Mise à jour de plusieurs références pour refléter des versions plus récentes des diverses spécifications. À ce titre, la reclassification de la RFC 4954 comme référence normative (SMTP AUTH est un DOIT pour la RFC 4409 et la présente spécification).

- Mise à jour du texte de la Section 7 pour refléter l'existence et le remplissage partiel du registre et du tableau inclus (Tableau 1) pour corriger une entrée et en ajouter d'autres. Voir plus d'informations à la Section 10.

- Ajout de nouveau texte (au paragraphe 5.3) pour préciser que les serveurs de soumission devraient répondre rapidement.

- Ajout de texte pour dire explicitement que des changements de codage de caractère sont permis.

- Ajout de texte pour préciser que les modifications aux messages signés peuvent causer des problèmes et qu'elles devraient être considérées avec prudence.

Adresse des auteurs

Randall Gellens
QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, CA 92121-2779
USA
mél : rg+ietf@qualcomm.com

John C Klensin
1770 Massachusetts Ave, #322
Cambridge, MA 02140
USA
téléphone : +1 617 491 5735
mél : john-ietf@jck.com