

Groupe de travail Réseau
Request for Comments : 4409
 RFC rendue obsolète : 2476
 Catégorie : En cours de normalisation

R. Gellens, QUALCOMM
 J. Klensin
 avril 2006
 Traduction Claude Brière de L'Isle, décembre 2007

Présentation de message pour la messagerie

Statut de ce mémoire

Le présent document spécifie un protocole de normalisation Internet pour la communauté de l'Internet, qui appelle à la discussion et à des suggestions pour son amélioration. Prière de se reporter à l'édition en cours des "Normes de protocole officielles de l'Internet" (STD 1) sur l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de Copyright

Copyright (C) Le Internet Society (2006).

Résumé

Le présent mémo partage la présentation de message à partir du relais de message, permettant à chaque service de fonctionner conformément à ses propres règles (pour la sécurité, la politique, etc.), et spécifie les actions à entreprendre par un serveur de présentation. Le relais de message et la livraison finale ne sont pas affectés, et continuent d'utiliser SMTP sur l'accès 25. Quand elle se conforme au présent document, la présentation de message utilise le protocole spécifié ici, normalement sur l'accès 587. Cette séparation des fonctions offre un certain nombre d'avantages, y compris la capacité d'appliquer des exigences spécifiques de sécurité ou de politique.

Table des matières

1	Introduction.....	2
2	Information sur le document.....	3
2.1	Définitions des termes utilisés dans le présent mémo.....	3
2.2	Conventions utilisées dans ce document.....	3
3	Présentation de message.....	3
3.1	Identification de présentation.....	3
3.2	Rejet et rebond de message.....	3
3.3	Présentation autorisée.....	4
4	Actions obligatoires.....	4
4.1	Code général de rejet de présentation.....	4
4.2	S'assurer que tous les domaines sont pleinement qualifiés.....	5
4.3	Exiger l'authentification.....	5
5	Actions recommandées.....	5
5.1	Appliquer la syntaxe d'adresse.....	5
5.2	Enregistrement des erreurs.....	5
6	Actions facultatives.....	6
6.1	Mettre en application les droits de présentation.....	6
6.2	Mettre en application les permissions.....	6
6.3	Vérifier les données du message.....	6
6.4	Prise en charge de l'adresse du maître de poste.....	6
7	Interaction avec les extensions SMTP.....	6
8	Modifications de message.....	7
8.1	Ajout du 'Sender'.....	7
8.2	Ajout de 'Date'.....	7
8.3	Ajout de 'Message-ID'.....	7
8.4	Codage de transfert.....	8
8.5	Signer le message.....	8
8.6	Chiffrer le message.....	8
8.7	Résoudre les alias.....	8
8.8	Réécriture d'en-tête.....	8
9	Considérations pour la sécurité.....	8
10	Considérations relatives à l'IANA.....	9
11	Remerciements.....	9

12 Références normatives.....	9
13 Références informatives.....	9

1 Introduction

SMTP 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 [SMTP-MTA].

Cependant, SMTP est maintenant largement utilisé comme protocole de *présentation* 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 présentations de message à partir des MUA est appelé agent de présentation de message (MSA, *Message Submission Agent*).

Afin de permettre des communications sans limitations, SMTP n'est souvent pas authentifié durant le relais de message. L'authentification et l'autorisation des présentations 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 présentation 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 malveillants qui génèrent de grandes quantités de pourriels, de nombreux sites interdisent maintenant le trafic sortant sur l'accès SMTP standard (port 25), passant en entonnoir toutes les présentations de messagerie à travers des serveurs de présentation.

En plus des questions d'authentification et d'autorisation, les messages présentés 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 [MESSAGE-FORMAT], et à des exigences ultérieures. 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 de 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 présentation du premier bond – et sont en général considérés comme en-dehors du domaine de la fonction de MTA normalisé.

Séparer les messages en présentations et transferts permet aux développeurs et administrateurs de réseau de faire plus facilement ce qui suit :

- * 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,
- * mettre en œuvre la présentation authentifiée, y compris la présentation hors site par des utilisateurs autorisés comme les personnels en déplacement,
- * Séparer les différences de code des logiciels pertinents, rendant par là chaque base de code plus directe et permettant différents programmes pour le relais et la présentation,
- * détecter les problèmes de configuration avec les clients de messagerie d'un site,
- * fournir à l'avenir une base pour l'ajout de services de présentation améliorés.

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

2 Information 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 [SMTP-MTA] ; 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 présentation de message (MAS, *Message Submission Agent*)

Processus qui se conforme à la présente spécification. Un MSA agit comme serveur de présentation pour accepter des messages des MUA, et les délivre 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 [SMTP-MTA]. Un MTA agit comme un serveur SMTP pour accepter des messages d'un MSA ou d'un autre MTA, et soit les délivre, 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 présenter de nouveaux messages, et traite les messages délivrés.

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, Post Office Protocol [POP3] ou IMAP [IMAP4] est utilisé pour accéder aux messages délivrés, tandis que le protocole défini ici (ou SMTP) est utilisé pour présenter les messages.

2.2 Conventions utilisées dans ce document

Dans les exemples, "C:" est utilisé pour indiquer les lignes envoyées par le client, et "S:" indique celles envoyées par le serveur. Les coupures de ligne au sein d'un exemple de commande ne sont là que pour faciliter la lecture.

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 défini dans [KEYWORDS].

3 Présentation de message

3.1 Identification de présentation

L'accès 587 est réservé aux présentations de messages électroniques comme spécifié dans le présent document. Les messages reçus sur cet accès sont définis comme des présentations. Le protocole utilisé est ESMTP [SMTP-MTA, ESMTP], 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 présentation de message, en désignant des hôtes comme MSA et d'autres comme 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 présentation ou en relais.

Par exemple, certains sites peuvent configurer leurs MTA pour rejeter toutes les commandes RCPT pour les messages qui ne font pas référence aux utilisateurs locaux, et configurer leur MSA pour rejeter toutes les présentations 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 présentation soit 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 présentation, à partir d'une MAIL FROM valide, d'une adresse IP de source valide, ou fondée 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 ordonne à un MSA de produire un code de rejet PEUT se conformer à l'acceptation du message et générer 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 présentation 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 présenté, et de leur confronter les rebonds. Noter que beaucoup de MUA actuels n'ont pas cette capacité.

3.3 Présentation autorisée

De nombreuses méthodes ont été utilisées pour s'assurer que seuls les utilisateurs autorisés sont capable de présenter 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 [SMTP-AUTH] a connu un large développement. Il permet au MSA de déterminer une identité d'autorisation pour la présentation du message, qui n'est pas liée à d'autres protocoles.

Les restrictions d'adresse IP connaissent un très large développement, 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 [IPSEC], et autres techniques de tunnelage chiffrées et authentifiées, peut aussi être utilisé et procure les avantages supplémentaires de la protection contre l'espionnage et l'analyse de trafic.

Exiger une authentification POP [POP3] (à partir de la même adresse IP) dans un certain délai (par exemple, 20 minutes) avant le début d'une session de présentation 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 présentation 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 présenter 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 (voir ci-dessus).

4 Actions obligatoires

Un MSA DOIT faire tout ce qui suit :

4.1 Code général de rejet de présentation

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 [SMTP-MTA], 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 niveau incomplets (par exemple, 'criard.soldes'), car des telles extensions sont particulièrement risquées.

4.3 Exiger l'authentification

Le MSA DOIT par défaut produire une réponse d'erreur à la commande MAIL si la session n'a pas été authentifiée en utilisant [SMTP-AUTH], à moins qu'ait été déjà établie de façon indépendante l'authentification ou l'autorisation (comme cela se produit derrière un sous réseau protégé).

Le paragraphe 3.3 expose les mécanismes d'authentification.

Le code de réponse 530 [SMTP-AUTH] 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'expéditeur ou de destinataire.

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 présentation du corps de message, le code de réponse 554 (avec un code d'état amélioré convenable d'après [SMTP-CODES]) 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 présentation et relais : les administrateurs de système peuvent s'intéresser aux problèmes de configuration locale, mais pas aux problèmes des clients sur d'autres sites.

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

6 Actions facultatives

Le MSA PEUT faire tout ce qui suit :

6.1 Mettre en application les droits de présentation

Le MSA PEUT produire une réponse d'erreur à une commande MAIL si l'adresse dans MAIL FROM paraît avoir des droits de présentation insuffisants, on 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 [SMTP-CODES], comme 5.7.1, est utilisé à cette fin.

6.2 Mettre en application 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 [SMTP-CODES], 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, ou semble incohérent avec les permissions données à l'utilisateur (s'il est connu), 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 [SMTP-CODES] (comme 5.7.1) est utilisé pour rejeter sur la base de l'utilisateur qui présente. 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 [SMTP-MTA], le MSA PEUT permettre un degré réduit d'authentification pour la messagerie adressée au "maître de poste" (ou une de ses appellations équivalentes, voir [SMTP-MTA]), 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.

7 Interaction avec les extensions SMTP

Le tableau suivant fait la liste des extensions SMTP actuellement en cours de normalisation et expérimentales. Figurent sur la liste le mot clé du EHLO, le nom et une indication sur l'utilisation de l'extension sur le port de présentation, et une référence :

Mot clé	Nom	Présentation	Référence
PIPELINING	Intubage	DEVRAIT	[PIPELINING]
ENHANCEDSTATUSCODES	Codes d'état améliorés	DEVRAIT	[CODES-EXTENSION]
ETRN	Extension de tour	NE DOIT PAS	[ETRN]
...	Extension de codes	DEVRAIT	[SMTP-CODES]
DSN	Notification d'état de livraison	DEVRAIT	[DSN]
SIZE	Taille de message	PEUT	[SIZE]
...	Code de réponse 521	NE DOIT PAS	[521REPLY]
CHECKPOINT	Point de vérification/Redémarrage	PEUT	[CHECKPOINT]
BINARYMIME	MIME binaire	PEUT	[CHUNKING]
CHUNKING	Tronquage	PEUT	[CHUNKING]
8BITMIME	Usage de données en 8 bits	DEVRAIT	[8BITMIME]
AUTH	Authentification	DOIT	[SMTP-AUTH]
STARTTLS	Start TLS	PEUT	[Start-TLS]
NO-SOLICITING	Notification de non sollicitation	PEUT	[Msg-Track]
MTRK	Traçage de message	PEUT	[Msg-Track]

Les futures extensions SMTP DEVRAIENT explicitement spécifier si elles sont valides sur le port de présentation.

Certaines extensions SMTP sont particulièrement utiles pour la présentation de message : Codes d'état étendu [SMTP-CODES] DEVRAIT être pris en charge et utilisé conformément à [CODES-EXTENSION]. 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 mémo. 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.

[PIPELINING] DEVRAIT être pris en charge par le MSA.

[SMTP-AUTH] permet au MSA de valider l'autorité et de déterminer l'identité de l'utilisateur présentateur et DOIT être accepté par le MSA.

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

8 Modifications de message

Les sites PEUVENT modifier les présentations pour s'assurer de la conformité aux normes et à la politique du site. La présente section décrit un certain nombre de telles 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 de [SMTP-MTA] et de [MESSAGE-FORMAT].

8.1 Ajout du 'Sender'

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 présenté, s'il n'en a pas, ou corriger le champ 'Date' s'il ne se conforme pas à la syntaxe de [MESSAGE-FORMAT].

8.3 Ajout de 'Message-ID'

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 [MESSAGE-FORMAT]). 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 Signer le message

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

8.6 Chiffrer le 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 doit 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 présentation à la couche transport, ou en utilisant un mécanisme [SMTP-AUTH] qui fournisse l'intégrité de session.

8.7 Résoudre les alias

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

NOTE : Résoudre inconditionnellement les alias peut 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 'criard.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. Par contre, 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 [SMTP-MTA] sur la modification des parties locales.

9 Considérations pour la sécurité

La séparation de la présentation 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 à 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 la messagerie d'un site.

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

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

L'enregistrement pour le port 587 a été mis à jour pour se référer au présent mémo plutôt qu'à la RFC 2476.

11 Remerciements

Nathaniel Borenstein et Barry Leiba ont été les artisans du développement de cette mise à jour de la RFC 2476.

Le mémo original (RFC 2476) avait été développé en partie sur la base des commentaires et des discussions qui avaient eu lieu sur la liste de diffusion de IETF-Submit. L'aide de ceux qui ont pris le temps de relire ce document et faire des suggestions a été appréciée, en particulier de la part de Dave Crocker, Ned Freed, Keith Moore, John Myers, et Chris Newman.

Des remerciements particuliers à Harald Alvestrand, qui est à l'origine de ces efforts.

12 Références normatives

[ESMTP] J. Klensin, N. Freed, M. Rose, E. Stefferud et D. Crocker, "Extensions de service SMTP", STD 10, RFC 1869, novembre 1995.

[KEYWORDS] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigences", BCP 14, RFC 2119, mars 1997.

[SMTP-MTA] J. Postel, "Protocole simple de transfert de messagerie", STD 10, RFC 821, août 1982.

Partridge, C., "L'acheminement de messagerie et le système de domaines", STD 10, RFC 974, janvier 1986.

Braden, R., "Exigences pour les hôtes Internet - Application et prise en charge", STD 3, RFC 1123, octobre 1989.

Klensin, J., "Protocole simple de transfert de messagerie", RFC 2821, avril 2001.

13 Références informatives

[521REPLY] A. Durand et F. Dupont, "Le code de réponse SMTP 521", RFC 1846, septembre 1995.

[8BITMIME] J. Klensin, N. Freed, M. Rose, E. Stefferud et D. Crocker, "Extension de service SMTP pour le transport MIME sur 8 bits", RFC 1652, juillet 1994.

[CHECKPOINT] D. Crocker, N. Freed et A. Cargille, "Extension de service SMTP pour point de vérification/redémarrage", RFC 1845, septembre 1995.

[CHUNKING] G. Vaudreuil, "Extension de service SMTP pour la transmission de grands messages MIME binaires", RFC 3030, décembre 2000.

[CODES-EXTENSION] N. Freed, "Extension de service SMTP pour le retour de codes d'erreur améliorés", RFC 2034, octobre 1996.

[DSN] K. Moore, "Extension de service du protocole simple de transfert de messagerie (SMTP) pour les notifications d'état de livraison", RFC 3461, janvier 2003.

[ETRN] J. De Winter, "Extension de service SMTP pour le début de file d'attente distante de message", RFC 1985, août 1996.

[IMAP4] M. Crispin, "Protocole d'accès de message Internet - version 4 révision 1", RFC 3501, mars 2003.

[IPSEC] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", RFC 2401, novembre 1998.

[MESSAGE-FORMAT] D. Crocker, "Norme pour le format des messages textuels ARPA Internet", STD 11, RFC 822, août 1982.

Braden, R., "Exigences pour les hôtes Internet - Application et prise en charge", STD 3, RFC 1123, octobre 1989.

Resnick, P., "Format des messages Internet", RFC 2822, avril 2001.

[Msg-Track] E. Allman et T. Hansen, "Extension de service SMTP pour le traçage de message", RFC 3885, septembre 2004.

[PIPELINING] N. Freed, "Extension de service SMTP pour l'intubage de commande", STD 60, RFC 2920, septembre 2000.

[POP3] J. Myers et M. Rose, "Protocole Post Office - version 3", STD 53, RFC 1939, mai 1996.

[SIZE] J. Klensin, N. Freed et K. Moore, "Extension de service SMTP pour la déclaration de taille de message", STD 10, RFC 1870, novembre 1995.

[SMTP-AUTH] J. Myers, "Extension de service SMTP pour l'authentification", RFC 2554, mars 1999.

[SMTP-CODES] G. Vaudreuil, "Code d'état améliorés du système de messagerie", RFC 3463, janvier 2003.

[Start-TLS] P. Hoffman, "Extension de service SMTP pour SMTP sécurisé sur la sécurité de couche Transport", RFC 3207, février 2002.

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
mél : john+ietf@jck.com

Déclaration de copyright

Copyright (C) Le Internet Society (2006).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à www.rfc-editor.org, et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations y contenues sont fournies sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourrait être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ou pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à <http://www.ietf.org/ipr>.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres

droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'activité de soutien administratif de l'IETF (IASA, *Administrative Support Activity*).