

Groupe de travail Réseau
Request for Comments : 3848
Catégorie : En cours de normalisation

C. Newman, Sun Microsystems
juillet 2004
Traduction Claude Brière de L'Isle

Enregistrement des types de transmission ESMTP et LMTP

Statut du présent mémoire

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

Notice de copyright

Copyright (C) The Internet Society (2004).

Résumé

Ceci enregistre sept nouveaux types de transmission de messagerie (ESMTPA, ESMTPS, ESMTPSA, LMTP, LMTPA, LMTPS, LMTPSA) à utiliser avec la clause "with" d'un en-tête Received dans un message Internet.

1. Considérations relatives à l'IANA

Selon les instructions de SMTP [RFC2821], l'IANA tient un registre [IANA] des "types de protocole WITH" à utiliser avec la clause "with" de l'en-tête Received dans un message Internet. Ce registre inclut présentement SMTP [RFC0821], et ESMTP [RFC2821]. La présente spécification met à jour le registre comme suit :

- o Le nouveau mot clé "ESMTPA" indique l'utilisation de ESMTP lorsque l'extension SMTP AUTH [RFC2554] est aussi utilisée et que l'authentification est réalisée avec succès.
- o Le nouveau mot clé "ESMTPS" indique l'utilisation de ESMTP lorsque STARTTLS [RFC3207] est aussi négocié avec succès pour fournir une couche de chiffrement fort de transport.
- o Le nouveau mot clé "ESMTPSA" indique l'utilisation de ESMTP lorsque STARTTLS et SMTP AUTH sont tous deux négociés avec succès (c'est la combinaison de ESMTPS et de ESMTPA).
- o Le nouveau mot clé "LMTP" indique l'utilisation de LMTP [RFC2033].
- o Le nouveau mot clé "LMTPA" indique l'utilisation de LMTP lorsque l'extension SMTP AUTH est aussi utilisée et que l'authentification est réalisée avec succès.
- o Le nouveau mot clé "LMTPS" indique l'utilisation de LMTP lorsque STARTTLS est aussi négocié avec succès pour fournir une couche de chiffrement fort de transport.
- o Le nouveau mot clé "LMTPSA" indique l'utilisation de LMTP lorsque STARTTLS et SMTP AUTH sont tous deux négociés avec succès (c'est la combinaison de LSMTPS et de LSMTPA).
- o Les références des entrées ESMTP et SMTP dans le registre devraient être mises à jour à la plus récente spécification [RFC2821] car les [RFC0821] et [RFC1869] ont toutes deux été rendues obsolètes par la [RFC2821].

2. Expérience de mise en œuvre

Les mots-clés ESMTPA, ESMTPS et ESMTPSA ont été mise en œuvre dans des logiciels de serveur de messagerie électronique en service pendant plusieurs années et aucun problème n'a été rapporté de cette utilisation.

3. Considérations sur la sécurité

L'utilisation de ces mots clés supplémentaires fournit des informations de traçage pour indiquer lorsque divers protocoles de tramage de sécurité de haut niveau sont utilisés pour le transport de bond en bond de messagerie électronique sans exposer les détails des spécificités du mécanisme de sécurité. Ces informations de traçage fournissent un moyen informel de suivre le déploiement de ces mécanismes sur l'Internet et peuvent assister le diagnostic après coup des malversations de messagerie électronique.

Ces mots clés ne sont normalement pas protégés dans le transport ce qui signifie qu'ils peuvent être modifiés par une attaque active. Ils n'indiquent pas non plus les spécificités du mécanisme utilisé, et ne fournissent donc aucune assurance réelle de sécurité. Ils ne devraient pas être utilisés pour le filtrage de messagerie ou pour relayer des décisions sauf dans des environnements très contrôlés. Comme ils sont à la fois cryptiques et cachés dans les en-têtes de traçage utilisés principalement pour diagnostiquer les problèmes de messagerie électronique, on ne s'attend pas à ce qu'ils fassent éprouver à l'utilisateur final un sentiment de sécurité trompeur. Des informations d'un degré de fiabilité plus élevé peuvent être obtenues en corrélant les en-têtes Received avec les journaux d'enregistrement des divers agents de transfert de messagerie par lesquels est passé le message.

Les informations de traçage fournies par ces mots clés et les autres parties de l'en-tête Received procurent un avantage significatif lorsque on fait le diagnostic après coup de tromperies ou problèmes avec la messagerie électronique. Malheureusement, en essayant de cacher les informations sur leurs serveurs internes; certaines personnes vont supprimer les en-têtes Received des informations utiles et vont réduire leur capacité à corriger des violations de la sécurité après coup. Le résultat de ces efforts malencontreux est généralement une diminution de la sécurité globale des systèmes.

4. Références

4.1 Références normatives

[RFC2033] J. Myers; "Protocole de transfert de messagerie locale", octobre 1996. (*Information*)

[RFC2554] J. Myers, "Extension de service [SMTP pour l'authentification](#)", mars 1999. (*Obsolète, voir [RFC4954](#)*) (*P.S.*)

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

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

4.2 Références pour information

[RFC0821] J. Postel, "Protocole simple de [transfert de messagerie](#)", STD 10, août 1982.

[RFC1869] J. Klensin, N. Freed, M. Rose, E. Stefferud, D. Crocker, "Extensions de service à SMTP", novembre 1995. (*Obsolète, voir [RFC5321](#), [STD0010](#)*)

4.3 URI

[IANA] < <http://www.iana.org/assignments/mail-parameters> >

Adresse del'auteur

Chris Newman
Sun Microsystems
1050 Lakes Drive
West Covina, CA 91790
USA

mél : chris.newman@sun.com

Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2004).

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 contenues sont fournis 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 pourraient 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 ; 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 le 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](mailto:ietf-ipr@ietf.org) .

Remerciement

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