

Groupe de Travail Réseau
Request For Comments : 1864
 RFC rendue obsolète : 1544
 Catégorie : Projet de norme

J. Myers, Carnegie Mellon
 M. Rose, Dover Beach Consulting, Inc.
 octobre 1995
 Traduction Xclaude Brière de L'Isle

Champ d'en-tête Contenu-MD5

Statut de ce 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.

Résumé

Le présent mémoire spécifie un champ d'en-tête facultatif, Contenu-MD5, à utiliser avec les messages qui se conforment à MIME.

Table des matières

1. Introduction.....	1
2. Génération du champ Contenu-MD5.....	1
3. Traitement du champ Contenu-MD5.....	2
4. Considérations pour la sécurité.....	2
5. Remerciements.....	2
6. Références.....	2
7. Adresse des auteurs.....	2

1. Introduction

En dépit de tous les mécanismes fournis par MIME [RFC1521] qui tentent de protéger les données contre les dommages au cours du transport de la messagerie électronique, il est toujours souhaitable d'avoir un mécanisme pour vérifier que les données, une fois décodées, sont intactes. Pour cette raison, le présent mémoire définit l'utilisation d'un champ d'en-tête facultatif, Contenu-MD5, qui peut être utilisé comme vérification de l'intégrité d'un message (*MIC message integrity check*) pour vérifier que les données décodées sont les mêmes données qui ont été initialement envoyées. L'en-tête Contenu-MD5 peut aussi être placé dans les en-têtes encapsulés d'un objet de type message/corps externe, à utiliser pour vérifier que les données restituées et décodées sont les mêmes données qui étaient initialement référencées.

MD5 est un algorithme pour calculer un "résumé" de 128 bits de données de longueur arbitraire, avec un fort degré de confiance que toute altération des données sera reflétée par une altération du résumé. L'algorithme MD5 lui-même est défini dans la [RFC1321]. Le présent mémoire spécifie comment l'algorithme peut être utilisé comme vérification d'intégrité pour la messagerie MIME.

2. Génération du champ Contenu-MD5

Le champ Contenu-MD5 est généré seulement par un agent d'utilisateur d'origine. Il est expressément interdit aux relais et passerelles de message de générer un champ Contenu-MD5.

L'utilisation du champ Contenu-MD5 est entièrement facultative ; son utilisation est recommandée chaque fois que l'intégrité des données est désirée, mais que les services de messagerie à confidentialité améliorée [RFC1421] ne sont pas disponibles. (Consulter la section 4 pour des précisions.) Le champ Contenu-MD5 ne peut être ajouté qu'à des entités MIME de nature "feuille", c'est-à-dire que le champ Contenu-MD5 peut être utilisé avec tout type de contenu autre que multiparties ou message/rfc822.

Pour générer la valeur du champ Contenu-MD5, l'algorithme MD5 est calculé sur la forme canonique de l'objet de l'entité MIME. En particulier, cela signifie que l'expéditeur applique l'algorithme MD5 sur les données immédiatement

après la conversion à la forme canonique, avant d'appliquer aucun codage de transfert de contenu, et que le receveur applique aussi l'algorithme MD5 sur la forme canonique, après avoir défait tout codage de transfert de contenu. Pour les données textuelles, cela signifie que l'algorithme MD5 doit être calculé sur les données dans lesquelles s'applique la forme canonique pour les nouvelles lignes, c'est-à-dire, dans lesquelles chaque nouvelle ligne est représentée par une paire CR-LF. Le modèle de codage canonique de MIME est décrit à l'Appendice G de la [RFC1521].

Le résultat de l'algorithme MD5 est un résumé de 128 bits. Vu dans l'ordre des octets du réseau (ordre gros boutien) cela donne une séquence de 16 octets de données binaires. Ces 16 octets sont alors codés conformément à l'algorithme base64 afin d'obtenir la valeur qui est placée dans le champ Contenu-MD5. Donc, si l'application de l'algorithme MD5 sur les données brutes d'une entité MIME résulte en un résumé qui a la valeur (improbable) de "Vérification d'intégrité!", alors cet en-tête d'entité MIME pourrait contenir le champ :

Contenu-MD5: Q2hlY2sgSW50ZWdyaXR5IQ==

Finalement, comme exposé à l'Appendice B de la [RFC1521], les données textuelles sont régulièrement altérées dans la livraison normale de messagerie. Comme l'ajout ou la suppression d'espaces blanches en queue va résulter en un résumé différent, les algorithmes quoted-printable ou base64 devraient être employés comme codage de transfert de contenu lorsque le champ Contenu-MD5 est utilisé.

3. Traitement du champ Contenu-MD5

Si le champ Contenu-MD5 est présent, un agent d'utilisateur receveur peut choisir de l'utiliser pour vérifier que le contenu d'une entité MIME n'a pas été modifié durant le transport. Il est expressément interdit aux relais et passerelles de message de modifier leur traitement en fonction de la présence du champ Contenu-MD5. Cependant, une passerelle de message est autorisée à retirer le champ Contenu-MD5 si l'entité MIME correspondante est traduite dans un type de contenu différent.

4. Considérations pour la sécurité

Le présent document spécifie un service d'intégrité des données qui protège les données contre une modification accidentelle lors du transit de l'expéditeur au receveur. Un service sûr de protection de l'intégrité des données, tel que celui fourni par la messagerie à confidentialité améliorée de la [RFC1421], est prévu pour protéger les données de toute modification.

5. Remerciements

Le présent mémoire se fonde presque entièrement sur le texte écrit à l'origine par Nathaniel Borenstein de Bellcore. Quelques améliorations ont de plus été suggérées par Keith Moore de l'Université du Tennessee, Knoxville.

6. Références

[RFC1521] N. Borenstein et N. Freed, "MIME (Extensions [multi-usage de messagerie Internet](#)) Partie 1 : Mécanismes pour spécifier et décrire le format des corps de message Internet", septembre 1993. (*Rendue obsolète par les RFC 2045 à 2049*)

[RFC1321] R. Rivest, "Algorithme de [résumé de message MD5](#)", avril 1992. (*Information*)

[RFC1421] J. Linn, "Amélioration de la confidentialité pour la messagerie électronique Internet : Partie I : Chiffrement de message et procédures d'authentification", février 1993. (*Historique*)

7. Adresse des auteurs

John G. Myers
Carnegie Mellon University
mél : jgm+@cmu.edu

Marshall T. Rose
Dover Beach Consulting, Inc.
mél : mrose@dbc.mtview.ca.us