

RFC 5337 : Internationalized Delivery Status and Disposition Notifications

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 7 Septembre 2008

Date de publication du RFC : Septembre 2008

<http://www.bortzmeyer.org/5337.html>

Dans l'ensemble des RFC sur l'internationalisation des adresses de courrier électronique, ce document traite le cas des **accusés de réception** et **avis de non-remise** (DSN pour "*Delivery Status Notification*").

Puisque les RFC 5336¹ et RFC 5335 permettent désormais d'utiliser des adresses de courrier électroniques internationalisées, c'est-à-dire utilisant tout le jeu de caractères Unicode, il faut prévoir le cas où les courriers provoquent l'envoi d'avis de remise ou de non-remise (DSN pour "*Delivery Status Notification*", RFC 3461 et RFC 3464) et d'accusés de réception (MDN, pour "*Message Disposition Notification*", RFC 3798). C'est l'objet de ce RFC, qui met à jour les anciens documents qui limitaient ces accusés et avis au jeu ASCII.

Le format des DSN dans le RFC 3464 parle de « types d'adresse ». Les adresses en UTF-8 du RFC 5335 sont un nouveau type d'adresses. Si le serveur SMTP accepte l'extension UTF8SMTP du RFC 5336 et l'extension DSN du RFC 3461, il doit permettre d'utiliser ce type dans le paramètre ORCPT ("*Original Recipient*", section 4.2 du RFC 3461). Si le serveur n'accepte pas UTF8SMTP, l'adresse à utiliser dans les DSN doit être encodée en 7bits, selon les règles exposées dans cette section 3 (et non pas selon les règles du RFC 5137, paru trop tard). Par exemple, `stphane@bortzmeyer.org` peut s'écrire `st\x{E9}phane@bortzmeyer.org`. (La section 3 détaille plus complètement le traitement des adresses UTF-8.)

Une fois réglé le problème de la représentation des adresses, la section 4 traite les DSN en UTF-8. Les DSN traditionnels étaient composés d'un objet MIME de type `multipart/report` comportant trois objets décrivant le problème (un objet conçu pour être lu par un humain, un `message/delivery-status` et le message originel, `message/rfc822`). Pour le courrier internationalisé, de nouveaux types ont été créés :

¹Pour voir le RFC de numéro NNN, <http://www.ietf.org/rfc/rfcNNN.txt>, par exemple <http://www.ietf.org/rfc/rfc5336.txt>

- `message/global-delivery-status` qui, contrairement à son prédécesseur `message/delivery-status`, accepte l'UTF-8 et permet donc de placer directement les adresses UTF-8, sans encodage en ASCII. En outre, il dispose d'un nouveau champ, "*Localized-Diagnostic*", qui permet de stocker des messages lisibles par un humain. La langue de ces messages est indiquée par une étiquette de langue (RFC 4646).
- `message/global` qui remplace `message/rfc822` (dont le nom, hommage au vieux RFC 822, était de toute façon dépassé). À noter que le terme "*global*" (mondial) utilisé pour noter ce type avait fait l'objet de vives discussions et même d'un vote (<http://www.ietf.org/mail-archive/web/ima/current/msg02077.html>). Cet objet permet de transporter le message original (si on ne transporte que les en-têtes, on utilise `message/global-headers`).

On peut noter que la norme MIME (RFC 2046) interdisait l'usage de l'option `Content-Transfer-Encoding` pour les objets de type `message/*` mais cette règle a été assouplie par le RFC 5335.

La section 5 traite des MDN ("*Message Disposition Notificatin*", RFC 3798). Ils ne sont pas très différents des DSN et ont un format très proche, avec un type MIME `message/global-disposition-notification`.

La section 6 traite des registres IANA. Le type « UTF-8 » est ajouté au registre des types d'adresses (<http://www.iana.org/assignments/mail-parameters>) (section 6.1), et les nouveaux types MIME comme `message/global` sont ajoutés au registre des types MIME (<http://www.iana.org/assignments/media-types/>) (sections 6.3 à 6.5).

Enfin, la section 7 est dédiée aux questions de sécurité. Outre les problèmes de sécurité classiques des DSN et des MDN (non authentifiés, ils permettent de faire croire qu'un message a échoué, alors qu'il a bien été délivré, ou le contraire), le RFC nous prévient que des DSN ou des MDN délibérément incorrects peuvent être envoyés par un attaquant dans l'espoir de profiter d'erreur dans la programmation des analyseurs, par exemple pour déclencher un débordement de tampon. Le risque est plus important s'il y a beaucoup d'encodage, le décodage pouvant faire varier la taille des données.