

RFC 4282 : The Network Access Identifier

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 3 janvier 2006. Dernière mise à jour le 4 janvier 2006

Date de publication du RFC : Décembre 2005

<https://www.bortzmeyer.org/4282.html>

Autrefois, chaque FAI avait sa propre base d'utilisateurs et tous ses équipements réseaux savaient comment interroger cette base. Aujourd'hui, il est de plus en plus fréquent qu'on doive s'authentifier auprès d'un autre FAI que le sien, parce qu'il sous-traite à un vrai opérateur, parce que son réseau de collecte est différent de son épine dorsale, parce qu'on est en déplacement et qu'on bénéficie d'accords de roaming avec un autre FAI... Le "*network access identifier*", décrit dans ce RFC, permet à l'abonné d'avoir une identité unique, que les équipements réseaux du FAI du moment sauront auprès de qui vérifier. (Le NAI a depuis été sérieusement réformé dans le RFC 7542¹.)

Le NAI est de la forme `user@sub.realm.example`. Il ressemble syntaxiquement à une adresse de courrier électronique mais n'en est **pas** une (les règles de syntaxe ne sont même pas exactement identiques, voir la section 2.5 du RFC). La partie droite, le domaine d'authentification ("*realm*"), ressemble à un nom de domaine mais ne l'est pas forcément même si c'est conseillé par le RFC (mon NAI actuel est `bortzmeyer@net2.nerim.nerim`).

C'est ce NAI qu'on configure dans son client réseau, par exemple dans les fichiers du répertoire `/etc/ppp` sur une machine Unix.

Lorsque le premier équipement réseau du trajet (le RFC le nomme NAS pour "*Network Access Server*") reçoit le NAI, il sait, d'après la partie droite, à qui il doit demander d'authentifier l'utilisateur indiqué en partie gauche. Par exemple, si mon NAI est `jean.durand@gold.iap.example`, il sait qu'il doit authentifier `jean.durand` auprès des serveurs (par exemple Radius, RFC 2865) de `gold.iap.example`.

Notons que, pour faciliter ce routage vers le bon serveur d'authentification, le RFC prévoit une syntaxe (facultative) avec routage explicite (section 2.7), en utilisant le point d'exclamation. Ainsi, `myserver.example.org!` est un NAI légal, qui demande que l'authentification passe d'abord par `gold.iap.example`, qui devra ensuite rediriger vers `myserver.example.org`.

Notre RFC est une mise à jour du précédent RFC sur les NAI, le RFC 2486. Le principal changement est l'addition de l'internationalisation, qui permet désormais des NAI comme `stéphane@immeuble.cité.fr`. La partie gauche sera traitée par un profil de l'algorithme "*stringprep*", décrit dans le RFC 4013, la partie droite sera encodée en IDN, `immeuble.xn--cit-dma.fr`. Le RFC 7542, qui a remplacé notre RFC, a sérieusement changé le modèle d'internationalisation (en supprimant Punycode).

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc7542.txt>