RFC 4013 : SASLprep: Stringprep Profile for User Names and Passwords

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 20 juin 2008

Date de publication du RFC : Février 2005

https://www.bortzmeyer.org/4013.html

Beaucoup de protocoles Internet ont besoin de comparer des **noms**, par exemple pour tester leur égalité avant une authentification de ce nom. Si les noms sont en Unicode, il est préférable de les **normaliser** avant la comparaison, pour que le résultat de celle-ci ne soit pas trop déroutant pour l'utilisateur. C'est le but de SASLprep, normalisé dans ce RFC.

Le RFC sur SASLprep est très court car SASLprep est juste un profil de stringprep (normalisé dans le RFC 3454 [1]). Stringprep était l'algorithme général de normalisation des noms à l'IETF. Il ne spécifiait pas tous les détails de la normalisation effectuée, laissant ceux-ci à des profils comme nameprep (RFC 3491, utilisé dans les IDN) ou bien notre SASLprep. Stringprep ayant depuis été abandonné (cf. RFC 7564), ce RFC 4013 a été remplacé par le nouveau mécanisme du RFC 7613.

SASLprep est conçu pour l'utilisation dans le contexte de l'authentification, notamment pour SASL (RFC 4422). L'idée est de passer les noms et les mots de passe à travers SASLprep avant toute comparaison, pour que le résultat de celle-ci corresponde aux attentes de l'utilisateur (section 1).

Le profil lui-même est décrit dans la section 2. Par exemple, SASLprep utilise la normalisation Unicode NFKC (section 2.2 de notre RFC et section 4 du RFC 3454). Ainsi, comme l'illustre les exemples de la section 3, la chaîne U+2168 ([Caractère Unicode non montré [2]], chiffre romain 9) sera transformée en la chaîne « IX », qui a la même signification. Sans SASLprep, un utilisateur dont le nom comporterait ce caractère Unicode aurait du mal à se loguer ! La section 2 spécifie aussi (section 2.3) les caractères interdits par SASLprep, comme les caractères de contrôle.

On peut tester cet algorithme sur Unix avec la commande idn de la "*GNU libidn*" <http://www.gnu.org/software/libidn/> et son option --profile :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc3454.txt
2. Car trop difficile à faire afficher par LaTeX

```
% echo Café | idn --quiet --stringprep --profile SASLprep
Café

% echo pi2 | idn --quiet --stringprep --profile SASLprep
pi2
```

Dans le premier exemple, on note que SASLprep est sensible à la casse (qui n'a pas été modifiée). Dans le second exemple, l'exposant 2 dans « pi au carré » a été remplacé par un 2 ordinaire, conséquence de la normalisation NFKC. Un hypothétique mot de passe « pi^2 » serait donc équivalent à « pi2 ».

Une mise en œuvre de SASLprep, sous forme d'une bibliothèque utilisable depuis vos programmes, figure dans la "*GNU SASL Library*" <http://www.gnu.org/software/gsasl/>.