Groupe de travail Réseau
**Request for Comments : 4013**
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

K. Zeilenga
OpenLDAP Foundation
février 2005

# SASLprep : Profil Stringprep pour les noms d'utilisateur et les mots de passe

**Statut du présent mémoire**
Le présent document spécifie un protocole de normalisation Internet pour la communauté Internet, et appelle à la discussion et à des suggestions en vue de son amélioration. Prière de se rapporter à l'édition en cours des "Internet Official Protocol Standards" (normes officielles du protocole Internet) (STD 1) pour connaître l'état de la normalisation et le statut du présent protocole. La distribution du présent mémo n'est soumise à aucune restriction.



**Résumé**
Le présent document décrit comment préparer les chaînes Unicode qui représentent les noms d'utilisateur et les mots de passe pour leur comparaison. Le document définit le profil "SASLprep" de l'algorithme "stringprep" à utiliser à la fois pour les noms d'utilisateur et les mots de passe. Ce profil est destiné à être utilisé par les mécanismes d'authentification simple et couche de sécurité (SASL, *Simple Authentication and Security Layer*) (tels que PLAIN, CRAM-MD5, et DIGEST-MD5), ainsi que par d'autres protocoles qui échangent de simples noms d'utilisateur et/ou des mots de passe.

## 1. Introduction

L'utilisation de noms d'utilisateurs et de mots de passe simples pour l'authentification et l'autorisation a envahie l'Internet. Pour accroître la probabilité que l'entrée et la comparaison du nom d'utilisateur et du mot de passe fonctionnent de façon qui ait du sens pour les utilisateurs normaux tout autour du globe, le présent document définit des règles pour préparer la comparaison des noms d'utilisateurs et mots de passe internationalisés. Par souci de simplicité et pour faciliter la mise en œuvre, un seul algorithme est défini à la fois pour les noms d'utilisateur et les mots de passe.

L'algorithme suppose que toutes les chaînes ne comportent que des caractères tirés du jeu de caractères [Unicode].

Le présent document définit le profil "SASLprep" de l'algorithme "stringprep" [StringPrep].

Le profil est conçu pour être utilisé dans les mécanismes d'authentification simple et couche de sécurité (SASL, *Simple Authentication and Security Layer*),tels que [PLAIN], [CRAM-MD5], et [DIGEST-MD5]. Il peut être applicable lorsque des noms d'utilisateur et des mots de passe simples sont utilisés. Ce profil n'est pas destiné à être utilisé dans la préparation de chaînes d'identité qui ne sont pas de simples noms d'utilisateur (par exemple, des adresses de messagerie électronique, des noms de domaines, des noms distinctifs), ou lorsque les chaînes d'identité ou les mots de passe ne sont pas des données de caractères, ou exigent un traitement différent (par exemple, un changement de casse).

Le présent document n'altère pas la spécification technique de protocoles existants. Toute spécification qui souhaite utiliser l'algorithme décrit dans le présent document doit incorporer explicitement le présent document et fournir des détails précis sur l'endroit et la façon dont cet algorithme est utilisé par les mises en œuvre de cette spécification.

## 2. Profil SASLprep

La présente section définit le profil "SASLprep" de l'algorithme "stringprep" [StringPrep]. Ce profil est destiné à être utilisé dans la préparation des chaînes qui représentent des noms d'utilisateurs et mots de passe simples.

Le présent profil utilise Unicode 3.2 [Unicode].

Dans le présent document, les noms de caractères utilisent la notation pour les codets et les noms tirée de la norme Unicode [Unicode]. Par exemple, la lettre "a" peut être représentée soit par <U+0061> soit par <LATIN SMALL LETTER A>. Dans les listes des transpositions et des caractères interdits, le "U+" est laissé de côté pour faciliter la lecture des listes. Les

commentaires sur les gammes de caractères sont indiqués entre des crochets rectangulaires (comme "[CONTROL CHARACTERS]") et ne viennent pas de la norme.

Note : Un glossaire des termes utilisés dans Unicode se trouve dans [Glossary]. On trouve des informations sur le modèle Unicode de codage de caractère dans [CharModel].

### 2.1 Transposition

Le présent profil spécifie :

- les caractères d'espace non-ASCII [StringPrep, C.1.2] qui peuvent être transposés en SPACE (U+0020), et
- les caractères "communément transposés en rien du tout" [StringPrep, B.1] qui peuvent être transposés en rien.

### 2.2 Normalisation

Le présent profil spécifie l'utilisation de la forme KC de normalisation Unicode, telle que décrite à la Section 4 de [StringPrep].

### 2.3 Sorties interdites

Ce profil spécifie les caractères suivants comme entrée interdite :
- Caractères d'espace non-ASCII [StringPrep, C.1.2]
- Caractères de contrôle ASCII [StringPrep, C.2.1]
- Caractères de contrôle non-ASCII [StringPrep, C.2.2]
- Caractères d'utilisation privée [StringPrep, C.3]
- Codets qui ne sont pas des caractères [StringPrep, C.4]
- Codets de substitution [StringPrep, C.5]
- Caractères inappropriés pour le texte en clair [StringPrep, C.6]
- Caractères inappropriés pour la représentation canonique [StringPrep, C.7]
- Caractères de changement des propriétés d'affichage ou déconseillés [StringPrep, C.8]
- Caractères d'étiquetage [StringPrep, C.9]

### 2.4 Caractères bidirectionnels

Ce profil spécifie la vérification des chaînes bidirectionnelles comme décrit dans [StringPrep, Section 6].

### 2.5 Codets non alloués

Ce profil spécifie le tableau [StringPrep, A.1] comme sa liste de codets non alloués.

## 3. Exemples

Le tableau suivant fournit des exemples de la façon dont diverses données de caractères sont transformées par l'algorithme de préparation de chaîne SASLprep

| n° | Entrée | Sortie | Commentaires |
|---|---|---|---|
| 1 | I<U+00AD>X | IX | SOFT HYPHEN transposé en rien |
| 2 | usager | usager | pas de transformation |
| 3 | USAGER | USAGER | casse préservée, ne correspond pas au n° 2 |
| 4 | <U+00AA> | a | la sortie est NFKC, l'entrée en ISO 8859-1 |
| 5 | <U+2168> | IX | la sortie est NFKC, correspond au n° 1 |
| 6 | <U+0007> | Erreur | caractère interdit |
| 7 | <U+0627> | <U+0031> | Erreur – vérification bidirectionnelle |

## 4. Considérations pour la sécurité

Ce profil est destiné à préparer des chaînes simples de nom d'utilisateur et de mot de passe pour leur comparaison ou leur utilisation dans des fonctions cryptographiques (par exemple, des résumés de message). L'algorithme de préparation a été spécifiquement conçu pour que la sortie soit canonique, et soit bien formée.

Cependant, du fait d'une anomalie [PR29] dans la spécification de la normalisation Unicode, l'équivalence canonique n'est pas garantie pour quelques séquences de caractères choisies. Ces séquences, n'apparaissent cependant pas dans le texte bien formé. La présente spécification a été publiée en dépit de la connaissance de ce problème technique. Il est prévu que la présente spécification sera révisée avant d'autres étapes sur la voie de la normalisation (après que les spécifications [Unicode] et/ou [StringPrep] auront été mises à jour pour régler ce problème).

Il n'est pas destiné à préparer les chaînes d'identité qui ne sont pas de simples noms d'utilisateurs (par exemple, des noms distinctifs, des noms de domaines), et le profil n'est pas destiné à être utilisé pour les simples noms d'utilisateur qui requièrent un traitement différent (tel que le changement de casse). Les protocoles (ou applications de ces protocoles) qui ont des formes d'identité spécifiques de l'application et/ou les algorithmes de comparaison devraient utiliser des mécanismes spécifiquement conçus pour ces formes et algorithmes.

L'application de la préparation de chaîne peut avoir un impact sur la faisabilité des attaques en force et les attaques de dictionnaire. Alors que le nombre de chaînes préparées possible est inférieur au nombre de chaînes Unicode possibles, le nombre de noms et mots de passe utilisables est supérieur si seul ASCII est utilisé. Bien que SASLprep élimine certaines séquences de codets Unicode comme chaînes préparées possibles, cette élimination rend généralement les formes de sortie (canoniques) praticables et interdit les entrées qui n'ont pas de sens.

Les noms d'utilisateur et les mots de passe devraient être protégés contre l'espionnage.

Les considérations pour la sécurité générales de "stringprep" et d'Unicode s'appliquent. Toutes deux sont exposées dans [StringPrep].

## 5. Considérations relatives à l'IANA

Le présent document détaille le profil "SASLprep" du protocole [StringPrep]. Ce profil a été enregistré dans le registre du profil stringprep.

Nom de ce profil : SASLprep
RFC dans laquelle le profil est défini : RFC 4013
Indication de ce que ceci est la plus récente version du profil : Ceci est la première version du profil SASPprep.

## 6. Remerciement

Le présent document emprunte des textes tirés de "Preparation of Internationalized Strings ('stringprep')" et "Nameprep: A Stringprep Profile for Internationalized Domain Names", tous deux de Paul Hoffman et Marc Blanchet. Le présent document est produit par le groupe de travail SASL de l'IETF.

## 7. Références normatives

[StringPrep] P. Hoffman et M. Blanchet, "Préparation des chaînes internationalisées ("stringprep")", RFC 3454, décembre 2002.

[Unicode] The Unicode Consortium, "The Unicode Standard, Version 3.2.0" est défini par "The Unicode Standard, Version 3.0" (Reading, MA, Addison-Wesley, 2000. ISBN 0-201-61633-5), tel qu'amendé par le "Unicode Standard Annex #27: Unicode 3.1" (http://www.unicode.org/reports/tr27/) et par "Unicode Standard Annex #28: Unicode 3.2" (http://www.unicode.org/reports/tr28/).

## 8. Références informatives

[Glossary] The Unicode Consortium, "Unicode Glossary", <http://www.unicode.org/glossary/>.

[CharModel] Whistler, K. and M. Davis, "Unicode Technical Report #17, Character Encoding Model", UTR17, <http://www.unicode.org/unicode/reports/tr17/>, August 2000.

[SASL] A. Melnikov, éd., "Simple Authentication and Security Layer (SASL)", Travail en cours.

[CRAM-MD5] L. Nerenberg, "The CRAM-MD5 SASL Mechanism", Travail en cours.

[DIGEST-MD5] P. Leach, C. Newman et A. Melnikov, "Using Digest Authentication as a SASL Mechanism", Travail en cours.

[PLAIN] Zeilenga, K., Ed., "The Plain SASL Mechanism", Travail en cours.

[PR29] Public Review Issue #29: Normalization Issue", <http://www.unicode.org/review/pr-29.html>, février 2004.

**Adresse de l'auteur**

Kurt D. Zeilenga
OpenLDAP Foundation
mèl : Kurt@OpenLDAP.org

## Déclaration de copyright



**Propriété intellectuelle**



**Remerciement**

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