INTERNET-DRAFT
Intended Category: Standards Track
Expires in six months

Kurt D. Zeilenga
OpenLDAP Foundation

30 June 2003

SASLprep: Stringprep profile for user names and passwords
<draft-ietf-sasl-saslprep-03.txt>

Status of Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC 2026.

This document is intended to be, after appropriate review and revision, submitted to the RFC Editor as a Standards Track document. Distribution of this memo is unlimited. Technical discussion of this document will take place on the IETF SASL mailing list <ietf-sasl@imc.org>. Please send editorial comments directly to the document editor <Kurt@OpenLDAP.org>.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as ``work in progress.''

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>. The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Copyright (C) The Internet Society (2003). All Rights Reserved.

Please see the Full Copyright section near the end of this document for more information.

Abstract

This document describes how to prepare Unicode strings representing user names and passwords for comparison. The document defines the "SASLprep" "stringprep" profile to be used for both user names and passwords. This profile is intended to be used by Simple Authentication and Security Layer (SASL) mechanisms (such as PLAIN, CRAM-MD5, and DIGEST-MD5) as well as other protocols exchanging user

names and/or passwords.

1. Introduction

The use of simple user names and passwords in authentication and authorization is pervasive on the Internet. To increase the likelihood that user name and password input and comparison work in ways that make sense for typical users throughout the world, this document defines rules for preparing internationalized user names and passwords for comparison. For simplicity and implementation ease, a single algorithm is defined for both user names and passwords.

This document defines the "SASLprep" profile of the "stringprep" protocol [StringPrep].

The profile is designed for use in Simple Authentication and Security Layer ([SASL]) mechanisms such as [PLAIN]. It may be applicable elsewhere simple user names and passwords are used. This profile is not intended to be used for arbitrary text. This profile is also not intended to be used to prepare identity strings which are not simple user names (e.g., e-mail addresses, domain names, distinguished names).

2. The SASLprep profile

This section defines the "SASLprep" profile. This profile is intended to be used to prepare strings representing simple user names and passwords.

This profile uses Unicode 3.2, as defined in [StringPrep, A.1].

Character names in this document use the notation for code points and names from the Unicode Standard [Unicode]. For example, the letter "a" may be represented as either <U+0061> or <LATIN SMALL LETTER A>. In the lists of mappings and the prohibited characters, the "U+" is left off to make the lists easier to read. The comments for character ranges are shown in square brackets (such as "[CONTROL CHARACTERS]") and do not come from the standard.

Note: a glossary of terms used in Unicode can be found in [Glossary]. Information on the Unicode character encoding model can be found in [CharModel].

2.1. Mapping

This profile specifies:
- non-ASCII space characters [StringPrep, C.1.2] be mapped to SPACE (U+0020), and

- the "commonly mapped to nothing" characters [StringPrep, B.1] be mapped to nothing.

2.2. Normalization

This profile specifies using Unicode normalization form KC, as described in Section 4 of [StringPrep].

2.3. Prohibited Output

This profile specifies the following characters:

- Non-ASCII space characters [StringPrep, C.1.2],
- ASCII control characters [StringPrep, C.2.1],
- Non-ASCII control characters [StringPrep, C.2.2],
- Private Use [StringPrep, C.3],
- Non-character code points [StringPrep, C.4],
- Surrogate code points [StringPrep, C.5],
- Inappropriate for plain text [StringPrep, C.6],
- Inappropriate for canonical representation [StringPrep, C.7],
- Change display properties or are deprecated [StringPrep, C.8], and
- Tagging characters [StringPrep, C.9].

are prohibited output.

2.4. Bidirectional characters

This profile specifies checking bidirectional strings as described in [StringPrep, Section 6].

2.5. Unassigned Code Points

This profile specifies [StringPrep, A.1] table as its list of unassigned code points.

3. Security Considerations

This profile is intended to used to prepare simple user names and

passwords for comparison. It is not intended to be used for to prepare identities which are not simple user names (e.g., distinguished names and domain names). Nor is the profile intended to be used for simple user names which require different handling. Protocols (or applications of those protocols) which have application-specific identity forms and/or comparison algorithms should use mechanisms specifically designed for these forms and algorithms.

User names and passwords should be protected from eavesdropping.

General "stringprep" and Unicode security considerations apply. Both are discussed in [StringPrep].

4. IANA Considerations

This document details the "SASLprep" profile of [StringPrep] protocol. Upon Standards Action the profile should be registered in the stringprep profile registry.

> Name of this profile: SASLprep
> RFC in which the profile is defined: This RFC
> Indicator whether or not this is the newest version of the profile: This is the first version of the SASPprep profile.

5. Acknowledgment

This document borrows text from "Preparation of Internationalized Strings ('stringprep')" and "Nameprep: A Stringprep Profile for Internationalized Domain Names", both by Paul Hoffman and Marc Blanchet.

This document is a product of the IETF SASL WG.

6. Normative References

[StringPrep] Hoffman P. and M. Blanchet, "Preparation of Internationalized Strings ('stringprep')", RFC 3454, December 2002.

[SASL] Myers, J., "Simple Authentication and Security Layer (SASL)", draft-myers-saslrev-xx.txt, a work in progress.

[Unicode] The Unicode Consortium, "The Unicode Standard, Version 3.2.0" is defined by "The Unicode Standard, Version 3.0"

(Reading, MA, Addison-Wesley, 2000. ISBN 0-201-61633-5), as amended by the "Unicode Standard Annex #27: Unicode 3.1" (http://www.unicode.org/reports/tr27/) and by the "Unicode Standard Annex #28: Unicode 3.2" (http://www.unicode.org/reports/tr28/).

7. Informative References

[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.

[CRAM-MD5] Nerenberg, L., "The CRAM-MD5 SASL Mechanism", draft-nerenberg-sasl-crammd5-xx.txt, a work in progress.

[DIGEST-MD5] Leach, P., C. Newman, and A. Melnikov, "Using Digest Authentication as a SASL Mechanism", draft-ietf-sasl-rfc2831bis-xx.txt, a work in progress.

[PLAIN] Zeilenga, K., "The Plain SASL Mechanism", draft-ietf-sasl-plain-xx.txt, a work in progress.

8. Editor's Address

Kurt Zeilenga
OpenLDAP Foundation

Email: kurt@OpenLDAP.org

Intellectual Property Rights

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to

obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implmentation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.