INTERNET-DRAFT   Editor: Kurt D. Zeilenga
Intended Category: Standards Track   OpenLDAP Foundation
Expires in six months   24 February 2003

            SASLprep: Stringprep profile for user names and passwords
                    <draft-ietf-sasl-saslprep-00.txt>

Status of Memo

  This document is an Internet-Draft and is in full conformance with all
  provisions of Section 10 of RFC2026.

  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>.

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

---

INTERNET-DRAFT   draft-ietf-sasl-saslprep-00.txt   24 February 2003

   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
   likelyhood that user name and password input and comparsion 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 user names and passwords are used. This profile is not
   intended to be used for arbitrary text.

1.1. Conventions

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
   document are to be interpreted as described in BCP 14 [RFC2119].

   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. The SASLprep profile

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

2.1. Character Repertoire

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

2.2. Mapping

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

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

2.3. Normalization

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

2.4. Prohibited Output

   This profile specifies the following characters:

     - Non-ASCII space characters [StringPrep, C.1.2],
     - ASCII control charcters [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.

2.5. Bidirectional characters

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

2.6. Unassigned Code Points

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

3. IANA Considerations

This document details the "SASLprep" profile of [StringPrep] protocol. Upon Standards Action, it 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 User Name profile.

5. Acknowledgement

    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.

6. Normative References

[Keywords]   S. Bradner, "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14 (also RFC 2119), March 1997.

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

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

7. Informative References

    [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/).

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

    [CharModel] Unicode Technical Report;17, Character Encoding Model.
                <http://www.unicode.org/unicode/reports/tr17/>.

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

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

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

8. Editor's Address

   Kurt Zeilenga
   OpenLDAP Foundation

   Email: kurt@OpenLDAP.org