LAMPS
Internet-Draft
Intended status: Standards Track
Expires: June 12, 2017

A. Melnikov, Ed.
Isode Ltd
W. Chuang, Ed.
Google, Inc.

December 9, 2016

Internationalized Email Addresses in X.509 certificates
draft-ietf-lamps-eai-addresses-03

Abstract

This document defines a new name form for inclusion in the otherName field of an X.509 Subject Alternative Name and Issuer Alternate Name extension that allows a certificate subject to be associated with an Internationalized Email Address.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on June 12, 2017.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 2
2. Conventions Used in This Document 2
3. Name Definitions 2
4. Matching of Internationalized Email Addresses in X.509 certificates 3
5. Name constraints in path validation 4
6. Deployment Considerations 6
7. Security Considerations 6
8. IANA Considerations 6
9. References 6
9.1. Normative References 6
9.2. Informative References 7
Appendix A. ASN.1 Module 8
Appendix B. Example of smtpUtf8Name 9
Appendix C. Acknowledgements 9
Authors' Addresses 9

1. Introduction

[RFC5280] defines rfc822Name subjectAltName choice for representing [RFC5322] email addresses. This form is restricted to a subset of US-ASCII characters and thus can't be used to represent Internationalized Email addresses [RFC6531]. To facilitate use of these Internationalized Email addresses with X.509 certificates, this document specifies a new name form in otherName so that subjectAltName and issuerAltName can carry them.

2. Conventions Used in This Document

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 [RFC2119].

The formal syntax use the Augmented Backus-Naur Form (ABNF) [RFC5234] notation.

3. Name Definitions

The GeneralName structure is defined in [RFC5280], and supports many different names forms including otherName for extensibility. This section specifies the smtpUtf8Name name form of otherName, so that Internationalized Email addresses can appear in the subjectAltName of a certificate, the issuerAltName of a certificate, or anywhere else that GeneralName is used.

id-on-smtpUtf8Name OBJECT IDENTIFIER ::= { id-on 9 }

```
smtpUtf8Name ::= UTF8String (SIZE (1..MAX))
```

When the subjectAltName (or issuerAltName) extension contains an Internationalized Email address, the address MUST be stored in the smtpUtf8Name name form of otherName. The format of smtpUtf8Name is defined as the ABNF rule smtputf8Mailbox. smtputf8Mailbox is a modified version of the Internationalized Mailbox which is defined in Section 3.3 of [RFC6531] which is itself derived from SMTP Mailbox from Section 4.1.2 of [RFC5321]. [RFC6531] defines the following ABNF rules for Mailbox whose parts are modified for internationalization: <Local-part>, <Dot-string>, <Quoted-string>, <QcontentSMTP>, <Domain>, and <Atom>. In particular, <Local-part> was updated to also support UTF8-non-ascii. UTF8-non-ascii is described by Section 3.1 of [RFC6532]. Also, sub-domain is extended to support U-label, as defined in [RFC5890]

This document further refines Internationalized [RFC6531] Mailbox ABNF rules and calls this smtputf8Mailbox. In smtputf8Mailbox, sub-domain that encode non-ascii characters SHALL use U-label Unicode native character labels and MUST NOT use A-label [RFC5890]. This restriction prevents having to determine which label encoding A- or U-label is present in the Domain. As per Section 2.3.2.1 of [RFC5890], U-label use UTF-8 [RFC3629] with Normalization Form C and other properties specified there. In smtputf8Mailbox, sub-domain that encode solely ASCII character labels SHALL use NR-LDH restrictions as specified by section 2.3.1 of [RFC5890]. Note that a smtputf8Mailbox has no phrase (such as a common name) before it, has no comment (text surrounded in parentheses) after it, and is not surrounded by "<" and ">".

In the context of building name constraint as needed by [RFC5280], the smtputf8Mailbox rules are modified to allow partial productions to allow for additional forms required by Section 5. Name constraints may specify a complete email address, host name, or domain. This means that the local-part may be missing, and domain partially specified.

smtpUtf8Name is encoded as UTF8String. The UTF8String encoding MUST NOT contain a Byte-Order-Mark (BOM) [RFC3629] to aid consistency across implementations particularly for comparison.

4. Matching of Internationalized Email Addresses in X.509 certificates

In equivalence comparison with smtpUtf8Name, there may be some setup work to enable the comparison i.e. processing of the smtpUtf8Name content or the email address that is being compared against. The process for setup for comparing with smtpUtf8Name is split into domain steps and local-part steps. The comparison form for local-

part always is UTF-8. The comparison form for domain depends on context. While some contexts such as certificate path validation in [RFC5280] specify transforming domain to A-label, this document RECOMMENDS transforming to UTF-8 U-label instead. This reduces the likelihood of errors by reducing conversions as more implementations natively support U-label domains.

Comparison of two smtpUtf8Name can be straightforward. No setup work is needed and it can be an octet for octet comparison. For other email address forms such as Internationalized email address or rfc822Name, the comparison requires additional setup to convert the format for comparison. Domain setup is particularly important for forms that may contain A- or U-label such as International email address, or A-label only forms such as rfc822Name. This document specifies the process to transform the domain to U-label. (To convert the domain to A-label, follow the process specified in section 7.5 and 7.2 in [RFC5280]) The first step is to detect A-label by using section 5.1 of [RFC5891]. Next if necessary, transform the A-label to U-label Unicode as specified in section 5.2 of [RFC5891]. Finally if necessary convert the Unicode to UTF-8 as specified in section 3 of [RFC3629]. In setup for smtputf8Mailbox, the email address local-part MUST be converted to UTF-8 if it is not already. The <Local-part> part of an Internationalized email address is already in UTF-8. For the rfc822Name local-part is IA5String (ASCII), and conversion to UTF-8 is trivial since ASCII octets maps to UTF-8 without change. Once the setup is completed, comparison is an octet for octet comparison.

This specification expressly does not define any wildcards characters and smtpUtf8Name comparison implementations MUST NOT interpret any character as wildcards. Instead, to specify multiple specifying multiple email addresses through smtpUtf8Name, the certificate should use multiple subjectAltNames or issuerAltNames to explicitly carry those email addresses.

5. Name constraints in path validation

This section defines use of smtpUtf8Name name for name constraints. The format for smtpUtf8Name in name constraints is identical to the use in subjectAltName as specified in Section 3 with the extension as noted there for partial productions.

Constraint comparison on complete email address with smtpUtf8Name name uses the matching procedure defined by Section 4. As with rfc822Name name constraints as specified in Section 4.2.1.10 of [RFC5280], smtpUtf8Name name can specify a particular mailbox, all addresses at a host, or all mailboxes in a domain by specifying the complete email address, a host name, or a domain.

Name constraint comparisons in the context [RFC5280] is specified with smtpUtf8Name name are only done on the subjectAltName (and issuerAltName) smtpUtf8Name name, and says nothing more about constraints on other email address forms such as rfc822Name. Consequently it may be necessary to include other name constraints such as rfc822Name in addition to smtpUtf8Name to constrain all potential email addresses. For example a domain with both ascii and non-ascii local-part email addresses may require both rfc822Name and smtpUtf8Name name constraints. This can be illustrated in the following non-normative diagram Figure 1 which shows a name constraint set in the intermediate CA certificate, which then applies to the children entity certificates. Note that a constraint on rfc822Name does not apply to smtpUtf8Name and vice versa.



Figure 1

6. Deployment Considerations

For email addresses whose local-part is ASCII it may be more reasonable to continue using rfc822Name instead of smtpUtf8Name. The use of rfc822Name rather than smtputf8Name is currently more likely to be supported. Also use of smtpUtf8Name incurs higher byte representation overhead due to encoding with otherName and the additional OID needed. This may be offset if domain requires non-ASCII characters as smptUtf8Name supports U-label whereas rfc822Name supports A-label. This document RECOMMENDS using smtpUtf8Name when local-part contains non-ASCII characters, and otherwise rfc822Name.

7. Security Considerations

Use for smtpUtf8Name for certificate subjectAltName (and issuerAltName) will incur many of the same security considerations of Section 8 in [RFC5280] but further complicated by permitting non-ASCII characters in the email address local-part. As mentioned in Section 4.4 of [RFC5890] and in Section 4 of [RFC6532] Unicode introduces the risk for visually similar characters which can be exploited to deceive the recipient. The former document references some means to mitigate against these attacks.

8. IANA Considerations

This document makes use of object identifiers for the smtpUtf8Name defined in Section Section 3 and the ASN.1 module identifier defined in Section Appendix A. IANA is kindly requested to make the following assignments for:

The LAMPS-EaiAddresses-2016 ASN.1 module in the "SMI Security for PKIX Module Identifier" registry (1.3.6.1.5.5.7.0).

The smtpUtf8Name otherName in the "PKIX Other Name Forms" registry (1.3.6.1.5.5.7.8).

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, DOI 10.17487/RFC3629, November 2003, <http://www.rfc-editor.org/info/rfc3629>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <http://www.rfc-editor.org/info/rfc5234>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <http://www.rfc-editor.org/info/rfc5280>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <http://www.rfc-editor.org/info/rfc5321>.

[RFC5890] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, DOI 10.17487/RFC5890, August 2010, <http://www.rfc-editor.org/info/rfc5890>.

[RFC5891] Klensin, J., "Internationalized Domain Names in Applications (IDNA): Protocol", RFC 5891, DOI 10.17487/RFC5891, August 2010, <http://www.rfc-editor.org/info/rfc5891>.

[RFC5912] Hoffman, P. and J. Schaad, "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)", RFC 5912, DOI 10.17487/RFC5912, June 2010, <http://www.rfc-editor.org/info/rfc5912>.

[RFC6531] Yao, J. and W. Mao, "SMTP Extension for Internationalized Email", RFC 6531, DOI 10.17487/RFC6531, February 2012, <http://www.rfc-editor.org/info/rfc6531>.

[RFC6532] Yang, A., Steele, S., and N. Freed, "Internationalized Email Headers", RFC 6532, DOI 10.17487/RFC6532, February 2012, <http://www.rfc-editor.org/info/rfc6532>.

9.2. Informative References

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <http://www.rfc-editor.org/info/rfc5322>.

Appendix A. ASN.1 Module

The following ASN.1 module normatively specifies the smtpUtf8Name structure. This specification uses the ASN.1 definitions from [RFC5912] with the 2002 ASN.1 notation used in that document.

```
LAMPS-EaiAddresses-2016
  { iso(1) identified-organization(3) dod(6)
    internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
    id-mod-lamps-eai-addresses-2016(TBD) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS
  OTHER-NAME
  FROM PKIX1Implicit-2009
    { iso(1) identified-organization(3) dod(6) internet(1) security(5)
    mechanisms(5) pkix(7) id-mod(0) id-mod-pkix1-implicit-02(59) }

  id-pkix
  FROM PKIX1Explicit-2009
    { iso(1) identified-organization(3) dod(6) internet(1) security(5)
    mechanisms(5) pkix(7) id-mod(0) id-mod-pkix1-explicit-02(51) }

--
-- otherName carries additional name types for subjectAltName, issuerAltName,
-- and other uses of GeneralNames.
--

  id-on OBJECT IDENTIFIER ::= { id-pkix 8 }

  SmtpUtf8OtherNames OTHER-NAME ::= { on-smtpUtf8Name, ... }

  on-smtpUtf8Name OTHER-NAME ::= {
      smtpUtf8Name IDENTIFIED BY id-on-smtpUtf8Name
  }

  id-on-smtpUtf8Name OBJECT IDENTIFIER ::= { id-on 9 }

  SmtpUtf8Name ::= UTF8String (SIZE (1..MAX))

END
```

Figure 2

Appendix B. Example of smtpUtf8Name

This non-normative example demonstrates using smtpUtf8Name as an otherName in GeneralName to encode the email address "\u8001\u5E2B@example.com".

The hexidecimal DER encoding of the email address is:
A022060A 2B060105 05070012 0809A014 0C12E880 81E5B8AB 40657861 6D706C65 2E636F6D

The text decoding is:

```
0  34: [0] {
  2  10:   OBJECT IDENTIFIER '1 3 6 1 5 5 7 0 18 8 9'
 14  20:   [0] {
 16  18:     UTF8String '..@example.com'
       :     }
       :   }
```

Figure 3

The example was encoded on the OSS Nokalva ASN.1 Playground and the above text decoding is an output of Peter Gutmann's "dumpasn1" program.

Appendix C. Acknowledgements

Thank you to Magnus Nystrom for motivating this document. Thanks to Russ Housley, Nicolas Lidzborski, Laetitia Baudoin, Ryan Sleevi, Sean Leonard, and Sean Turner for their feedback. Also special thanks to John Klensin for his valuable input on internationalization, Unicode and ABNF formatting, and to Jim Schaad for his help with the ASN.1 example and his helpful feedback.

Authors' Addresses

Alexey Melnikov (editor)
Isode Ltd
14 Castle Mews
Hampton, Middlesex TW12 2NP
UK

Email: Alexey.Melnikov@isode.com

Weihaw Chuang (editor)
Google, Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043
US

Email: weihaw@google.com