

LAMPS
Internet-Draft
Intended status: Standards Track
Expires: November 19, 2017

A. Melnikov, Ed.
Isode Ltd
W. Chuang, Ed.
Google, Inc.
May 18, 2017

**Internationalized Email Addresses in X.509 certificates
draft-ietf-lamps-eai-addresses-10**

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 November 19, 2017.

Copyright Notice

Copyright (c) 2017 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.	IDNA2008	4
5.	Matching of Internationalized Email Addresses in X.509 certificates	4
6.	Name constraints in path validation	5
7.	Security Considerations	7
8.	IANA Considerations	7
9.	References	8
9.1.	Normative References	8
9.2.	Informative References	9
Appendix A.	ASN.1 Module	9
Appendix B.	Example of Smtputf8Name	10
Appendix C.	Acknowledgements	11
	Authors' Addresses	11

[1.](#) Introduction

[RFC5280] defines rfc822Name subjectAltName choice for representing [RFC5321] 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. In addition this document calls for all email address domain in X.509 certificates to conform to IDNA2008 [RFC5890].

[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 was defined in [Section 3.3 of \[RFC6531\]](#) which was 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 was described by [Section 3.1 of \[RFC6532\]](#). Also, sub-domain was 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 ASCII character labels SHALL use NR-LDH restrictions as specified by [section 2.3.1 of \[RFC5890\]](#) and SHALL be restricted to lower case letters. One suggested approach to apply these sub-domains restriction is to restrict sub-domain so that labels not start with two letters followed by two hyphen-minus characters. Consistent with the treatment of rfc822Name in [\[RFC5280\]](#), SmtpUTF8Name is an envelope <Mailbox> and 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 ">".

Due to operational reasons described shortly and name constraint compatibility reasons described in its section, SmtpUTF8Name subjectAltName MUST only be used when the local part of the email address contains UTF-8. When the local-part is ASCII, rfc822Name subjectAltName MUST be used 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 SmtpUTF8Name supports U-label whereas rfc822Name supports A-label.

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. IDNA2008

To facilitate comparison between email addresses, all email address domain in X.509 certificates MUST conform to IDNA2008 [RFC5890] (and excludes any "mappings" mentioned in that document). Otherwise non-conforming email address domains introduces the possibility of conversion errors between alternate forms. This applies to Smtputf8Mailbox and rfc822Name in subjectAltName, issuerAltName and anywhere else that GeneralName is used.

5. 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 is straightforward with no setup work needed. They are considered equivalent if there is an exact octet-for-octet match. Comparison with other email address forms such as Internationalized email address or rfc822Name requires additional setup steps. 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 \[RFC3629\]](#). For ASCII NR-LDH labels, upper case letters are converted to lower case letters. In setup for Smtputf8Mailbox, the email address local-part MUST conform to the requirements of [RFC6530] and [RFC6531], including being a string in UTF-8 form. In particular, the local-part MUST NOT be transformed in any way, such as by doing case folding or normalization of any kind. The <Local-part> part of an Internationalized email address is already in UTF-8. For

rfc822Name the local-part, which is IA5String (ASCII), trivially maps to UTF-8 without change. Once setup is complete, they are again compared octet-for-octet.

To summarize non-normatively, the comparison steps including setup are:

1. If the domain contains A-labels, transform them to U-label.
2. If the domain contains ASCII NR-LDH labels, lowercase them.
3. Ensure local-part is UTF-8.
4. Compare strings octet-for-octet for equivalence.

This specification expressly does not define any wildcards characters and Smtputf8Name comparison implementations MUST NOT interpret any character as wildcards. Instead, to specify multiple email addresses through Smtputf8Name, the certificate SHOULD use multiple subjectAltNames or issuerAltNames to explicitly carry those email addresses.

6. Name constraints in path validation

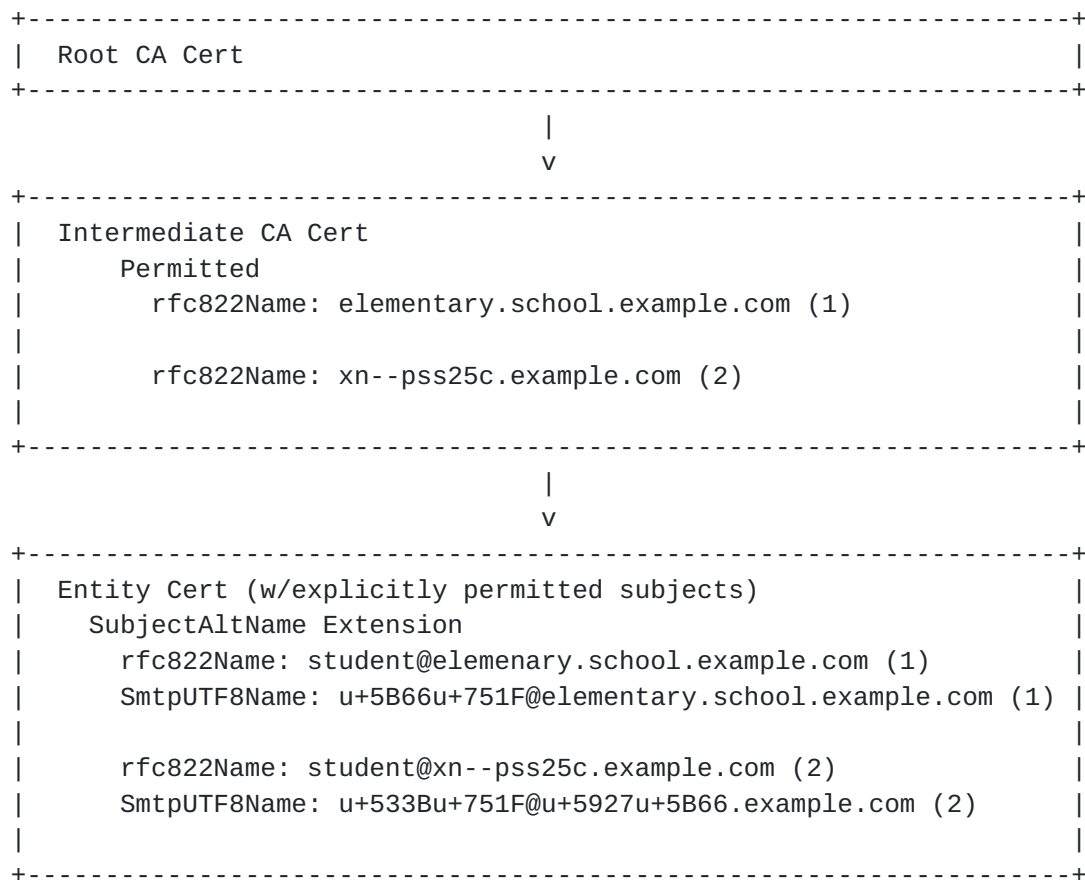
This section updates [RFC5280] name constraints defined in [section 4.2.1.10](#) to work with Smtputf8Name subjectAltName. The following specifies that a Smtputf8Name aware CA use a compatible name constraint representation. Similarly a Smtputf8Name aware path validators MUST be able to apply name constraint comparison to the subject distinguished name and both forms of subject alternative name rfc822Name and Smtputf8Name.

The Smtputf8Name aware email address name constraint form is specified to be rfc822Name motivated by compatibility considerations with legacy systems that already understand that form. This specification modifies [RFC5280] name constraint to only require with MAY that it represents all addresses at a host or all mailboxes in a domain, and require with MAY NOT that it represent a particular mailbox. For context, [\[RFC5280\] Section 4.2.1.10](#) specifies with MAY that name constraint represent 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. The change is due to rfc822Name name constraints inability to represent a specific mailbox with a UTF-8 email local part email address. CA certificate issuers should be aware of this lessened support.

Constraint comparison with Smtputf8Name subjectAltName starts with the setup steps defined by [Section 5](#). The setup applies to the

inputs of the comparison which is one of a subject distinguished name or a rfc822Name or Smtputf8Name subjectAltName, and one of a rfc822Name name constraint. Non-normatively the setup will convert any domain A-label to U-label in the rfc822Name name constraint, and to lower case any domain NR-LDH label in both the name constraint and the subject. After setup, this follows the comparison steps defined in 4.2.1.10 of [\[RFC5280\]](#) with some modifications as follows. The comparison process starts by determining the name constraint representation i.e. email host name or domain part, then comparing the name constraint against the corresponding part in the email address using a byte for byte comparison. This document suggests that name constraint comparison with subject distinguished name or rfc822Name subjectAltName also follow these setup and comparisons steps as well.

The name constraint requirement with Smtputf8Name subject alternative name is illustrated in the non-normative diagram Figure 1. The first example (1) illustrates a permitted rfc822Name ASCII only hostname name constraint, and the corresponding valid rfc822Name subjectAltName and Smtputf8Name subjectAltName email addresses. The second example (2) illustrates a permitted rfc822Name hostname name constraint with A-label, and the corresponding valid rfc822Name subjectAltName and Smtputf8Name subjectAltName email addresses.



Name constraints with Smtputf8Name and rfc822Name

Figure 1

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 is further complicated by permitting non-ASCII characters in the email address local-part. This complication, as mentioned in [Section 4.4 of \[RFC5890\]](#) and in [Section 4 of \[RFC6532\]](#), is that use of Unicode introduces the risk of visually similar and identical characters which can be exploited to deceive the recipient. The former document references some means to mitigate against these attacks.

8. IANA Considerations

in [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>>.
- [RFC6530] Klensin, J. and Y. Ko, "Overview and Framework for Internationalized Email", [RFC 6530](#), DOI 10.17487/RFC6530, February 2012, <<http://www.rfc-editor.org/info/rfc6530>>.

- [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

- [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>>.

[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. [\[RFC5912\]](#) updates normative documents using older ASN.1 notation.


```

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 "u+8001u+5E2B@example.com".

The hexadecimal 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, Sean Turner, John Levine, and Patrik Falstrom for their feedback. Also special thanks to John Klensin for his valuable input on internationalization, Unicode and ABNF formatting, to Jim Schaad for his help with the ASN.1 example and his helpful feedback, and to Viktor Dukhovni for his help with name constraints.

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 Amphitheater Parkway
Mountain View, CA 94043
US

Email: weihaw@google.com

