Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 22, 2016

A. Melnikov, Ed.
Isode Ltd

May 21, 2016

Internationalized Email Addresses in X.509 certificates
draft-melnikov-spasm-eai-addresses-00.txt

Abstract

This document defines a new name form for inclusion in the otherName field of an X.509 Subject Alternative 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 22, 2016.

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. IANA Considerations 3
6. Security Considerations 3
7. References 3
7.1. Normative References 3
7.2. Informative References 4
Appendix A. Acknowledgements 4
Author's Address 4

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].

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

This section defines the eaiName name as a form of otherName from the GeneralName structure in SubjectAltName defined in [RFC5280].

```
id-on-eaiAddr OBJECT IDENTIFIER ::= { id-on XXX }

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

When the subjectAltName extension contains an Internationalized Email address, the address MUST be stored in the eaiName name form of otherName. The format of an eaiName is a <eaiMailbox> as defined below. A eaiMailbox has the form "uLocal-part@uDomain". Note that a eaiMailbox 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 ">".

eaiMailbox = uLocal-part "@" uDomain

uLocal-part and uDomain are defined in [RFC6531]. [[CREF1: Alexey: uLocal-part and uDomain are no longer in RFC 6531, so we need to write explicit rules]]

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

The <uLocal-part> part of an Internationalized email address is in UTF-8 and need to be compared octet for octet.

The <uDomain> can contain either IDN domain or an ASCII Compatible Encoding (ACE) format. When comparing two <uDomain>s both MUST be converted to the ACE form as described in section 7.2 of [RFC5280].

5. IANA Considerations

[[CREF2: Just need a new OID.]]

6. Security Considerations

[[CREF3: TBD]]

7. References

7.1. 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>.

[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>.

7.2. 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. Acknowledgements

Thank you to Magnus Nystrom for motivating this document.

Author's Address

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

Email: Alexey.Melnikov@isode.com