

Security Working Group
Internet-Draft
Expires: August 7, 2016

L. Baudoin
W. Chuang
N. Lidzborski
Google, Inc.
February 4, 2016

**Internationalized Electronic Mail Addresses in [RFC5280](#) / X.509
Certificates
draft-lbaudoin-iemax-02**

Abstract

Specifies support for email address internationalization in [RFC5280](#) / X.509 certificates. This defines an encoding for Unicode email local-part characters in certificate Subject Alternative Names and Issuer Alternative rfc822Names. The encoding is backwards compatible with existing practices with rfc822Name.

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 August 7, 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.

This document may not be modified, and derivative works of it may not be created, and it may not be published except as an Internet-Draft.

Table of Contents

1.	Background	2
2.	Proposal	2
3.	References	3
	Authors' Addresses	4

[1.](#) Background

Internationalization of email addresses has significant precedence. Email addresses and their parts are specified in [\[RFC5322\]](#). Internationalization of domain names was specified in [\[RFC3490\]](#) and more recently in [\[RFC5890\]](#) via puny-coding of the unicode domain name labels. Email address as certificate Subject Alternative Name (SAN) and Issuer Alternative Name (IAN) rfc822Name support this internationalization of domain names as described in [section 7.5 of \[RFC5280\]](#). In [\[RFC6532\]](#), email headers as specified in [\[RFC5321\]](#) and [\[RFC5322\]](#) was refined to support UTF-8 unicode representation which implies support for Unicode email addresses but [RFC5280](#) was not updated to take Unicode email local-part into account.

[2.](#) Proposal

This draft proposes an encoding for internationalized email addresses with Unicode local-part. This encoding is a further refinement of email addresses in [RFC5280](#) SAN and IAN rfc822Name thus allowing existing PKI practices using email addresses to continue. To support the Unicode local-part, this draft proposes a base64 encoding for the local-part string with an identifier character to distinguish this encoding. That is the encoded string starts with an escape character ':' to identify that the local-part is Unicode and that the successive characters contain the base64 encoded local-part until the '@' character is seen. The escape colon character is a character intentionally chosen such that it is supported by IA5String but not possible in a compliant ASCII [RFC5322](#) email addresses. The local-part of the email address then consists of Unicode UTF-8 name that must be websafe base64url encoded as specified in [\[RFC4648\]](#). Support for internationalized domain names in the certificates is already specified in [RFC5280](#), and this draft does not change that interpretation for the email domain. Similarly the email address must follow existing Mailbox name practices specified in [RFC5280 section 4.2.1.6](#) that there must be no common name, no comment, nor

"<" or ">" present. A compliant reader of the encoded email address would strip the escape ':' and decode the base64 local-part to UTF-8.

One potential issue for an encoded internationalized SAN or IAN email address is its impact on [RFC5280](#) naming constraints particularly between a draft compliant certificate and a non compliant implementation. This encoding will not impact name matching in this scenario as mismatching local-part names and constraints will always match test negatively. The local-parts should only match if the implementation is compliant with this draft. Because the draft does not change internationalized domain name behavior, both the compliant and non-compliant implementation can test domain name constraints in the expected way.

3. References

- [RFC3490] Faltstrom, P., Hoffman, P., and A. Costello, "Internationalizing Domain Names in Applications (IDNA)", [RFC 3490](#), DOI 10.17487/RFC3490, March 2003, <<http://www.rfc-editor.org/info/rfc3490>>.
- [RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", [RFC 4648](#), DOI 10.17487/RFC4648, October 2006, <<http://www.rfc-editor.org/info/rfc4648>>.
- [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>>.
- [RFC5322] Resnick, P., Ed., "Internet Message Format", [RFC 5322](#), DOI 10.17487/RFC5322, October 2008, <<http://www.rfc-editor.org/info/rfc5322>>.
- [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>>.
- [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>>.

Authors' Addresses

Laetitia Baudoin
Google, Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043
US

Email: lbaudoin@google.com

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

Email: weihaw@google.com

Nicolas Lidzborski
Google, Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043
US

Email: nlidz@google.com

