

Internationalized Electronic Mail Addresses in X.509 Certificates
draft-lbaudoin-iemax-00

Abstract

Specifies support for internationalized email address local parts in X.509 certificates. [RFC6532](#) established support for UTF8 email headers hence internationalized email addresses including the local part. S/MIME email also needs support for UTF8 local part email addresses in X.509 certificates. This draft defines an encoding for UTF-8 characters in X.509 certificates which is backwards compatible with the IA5String encoding used to encode email addresses.

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 April 3, 2016.

Copyright Notice

Copyright (c) 2015 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This document may not be modified, and derivative works of it may not be created, and it may not be published except as an Internet-Draft.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.	Proposal	2
2.	Conversion	3
3.	References	3
	Authors' Addresses	3

[1.](#) Proposal

Internationalization of names in the internet has been an ongoing effort for a little bit over a decade. Internationalization of Domain Names was specified in [RFC3490](#) [[RFC3490](#)] and more recently in [RFC5890](#) [[RFC5890](#)] via puny-coding of the unicode representation of the internationalized name. This domain name internationalization is supported in the current definition of the X.509 certificates [RFC5280](#) [[RFC5280](#)]. In particular X.509 certificates specify email addresses in Subject Alternative Name (SAN) and Issuer Alternative Name (IAN) as IA5String representation and that RFC has instructions on interpreting internationalized domain names in [section 7.5](#). More recently the IETF has focussed their efforts on addresses used in SMTP electronic mail as specified in [RFC5321](#) [[RFC5321](#)] and [RFC5322](#) [[RFC5322](#)]. In [RFC6532](#) [[RFC6532](#)], email headers was specified to support UTF-8 unicode representation which implies support for unicode email addresses.

Internationalized S/MIME email lacks a means to support unicode local parts in X.509 certificates which this draft proposes a solution for. To support the unicode local name part, this draft proposes an encoding for the local part of the unicode name in the X.509 certificate SAN and IAN. That is the encoded string starts with an escape character ':' to indicate to the X.509 certificate parser that the local name is internationalized. Then the content of the unicode UTF-8 name should be base64 encoded and stored in the certificate. The escape colon character is a character intentionally chosen that is supported by IA5String but not possible in a compliant ASCII [RFC5322](#) email addresses. Support for internationalized domain names in the certificates is already specified in [RFC5280](#) [[RFC5280](#)], and this draft does not change that interpretation.

One potential issue for an encoded internationalized SAN or IAN email address is its impact on [RFC5280](#) naming constraints particularly

between say a draft compliant certificate and a non compliant implementation. In such a scenario we believe this encoding will not impact this processing as mismatching local part names and constraints will always test negatively. The local part 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.

2. Conversion

TODO: Conversion process

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>>.
- [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

Weihow 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

