INTERNET-DRAFT
Internet Engineering Task Force
Intended Status: Proposed Standard
Updates: 5280 (once approved)
Expires: 12 April 2018

R. Housley
Vigil Security

12 October 2017

Internationalization Updates to RFC 5280
draft-ietf-lamps-rfc5280-i18n-update-04

Abstract

These updates to RFC 5280 provide alignment with the 2008 specification for Internationalized Domain Names (IDNs) and add support for Internationalized Email Addresses in X.509 Certificates.

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Copyright and License Notice

1. Introduction

This document updates RFC 5280 [RFC5280]. The Introduction in Section 1, the Name Constraints certificate extension discussion in Section 4.2.1.10, and the Processing Rules for Internationalized Names in Section 7 are updated to provide alignment with the 2008 specification for Internationalized Domain Names (IDNs) and add support for Internationalized Email Addresses in X.509 Certificates.

An IDN in Unicode (native character) form contains at least one U-label [RFC5890]. With one exception, IDNs are carried in certificates in ACE-encoded form. That is, all U-labels within an IDN are converted to A-labels. Conversion of an U-label to an A-label is described in [RFC5891].

The GeneralName structure supports many different names forms, including otherName for extensibility. [ID.lamps-eai-addresses] specifies the SmtpUTF8Mailbox for Internationalized Email addresses, which include IDNs with U-labels.

Note that Internationalized Domain Names in Applications specifications published in 2003 (IDNA2003) [RFC3490] and 2008 (IDNA2008) [RFC5890] both refer to the Punycode Algorithm for conversion [RFC3492].

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Updates

This section provides updates to several paragraphs of RFC 5280 [RFC5280]. For clarity, if the entire section is not replaced, then the original text and the replacement text are shown.

2.1. Update in Section 1, Introduction

This update provides references for IDNA2008.

OLD

* Enhanced support for internationalized names is specified in Section 7, with rules for encoding and comparing Internationalized Domain Names, Internationalized Resource Identifiers (IRIs), and distinguished names. These rules are aligned with comparison rules established in current RFCs, including [RFC3490], [RFC3987], and [RFC4518].

NEW

* Enhanced support for internationalized names is specified in Section 7, with rules for encoding and comparing Internationalized Domain Names, Internationalized Resource Identifiers (IRIs), and distinguished names. These rules are aligned with comparison rules established in current RFCs, including [RFC3987], [RFC4518], [RFC5890], and [RFC5891].

2.2. Update in Section 4.2.1.10, Name Constraints

This update removes the ability to include constraints for a particular mailbox. This capability was not used, and removing it allows name constraints to apply to email addresses in rfc822Name and SmtpUTF8Mailbox [ID.lamps-eai-addresses] within otherName.

OLD

A name constraint for Internet mail addresses MAY specify a particular mailbox, all addresses at a particular host, or all mailboxes in a domain. To indicate a particular mailbox, the

constraint is the complete mail address. For example, "root@example.com" indicates the root mailbox on the host "example.com". To indicate all Internet mail addresses on a particular host, the constraint is specified as the host name. For example, the constraint "example.com" is satisfied by any mail address at the host "example.com". To specify any address within a domain, the constraint is specified with a leading period (as with URIs). For example, ".example.com" indicates all the Internet mail addresses in the domain "example.com", but not Internet mail addresses on the host "example.com".

NEW

A name constraint for Internet mail addresses MAY specify all addresses at a particular host or all mailboxes in a domain. To indicate all Internet mail addresses on a particular host, the constraint is specified as the host name. For example, the constraint "example.com" is satisfied by any mail address at the host "example.com". To specify any address within a domain, the constraint is specified with a leading period (as with URIs). For example, ".example.com" indicates all the Internet mail addresses in the domain "example.com", but not Internet mail addresses on the host "example.com".

2.3. Update in Section 7.2, IDNs in GeneralName

This update aligns with IDNA2008. Since all of Section 7.2 is replaced, the OLD text is not provided.

NEW

Internationalized Domain Names (IDNs) may be included in certificates and CRLs in the subjectAltName and issuerAltName extensions, name constraints extension, authority information access extension, subject information access extension, CRL distribution points extension, and issuing distribution point extension. Each of these extensions uses the GeneralName type; one choice in GeneralName is the dNSName field, which is defined as type IA5String.

IA5String is limited to the set of ASCII characters. To accommodate internationalized domain names U-labels are converted to A-labels. The A-label is the encoding of the U-label according to the Punycode algorithm [RFC3492] with the ACE prefix "xn--" added at the beginning of the string.

When comparing DNS names for equality, conforming implementations MUST perform a case-insensitive exact match on the entire DNS name. When evaluating name constraints, conforming implementations MUST

perform a case-insensitive exact match on a label-by-label basis. As noted in Section 4.2.1.10, any DNS name that may be constructed by adding labels to the left-hand side of the domain name given as the constraint is considered to fall within the indicated subtree.

Implementations SHOULD convert IDNs to Unicode before display. Specifically, conforming implementations convert A-labels to U-labels for display.

Implementation consideration: There are increased memory requirements for IDNs. An IDN ACE label will begin with the four additional characters "xn--", and an IDN can require as many as five ASCII characters to specify a single international character.

2.3. Update in Section 7.3, IDNs in Distinguished Names

This update aligns with IDNA2008.

OLD

Domain Names may also be represented as distinguished names using domain components in the subject field, the issuer field, the subjectAltName extension, or the issuerAltName extension. As with the dNSName in the GeneralName type, the value of this attribute is defined as an IA5String. Each domainComponent attribute represents a single label. To represent a label from an IDN in the distinguished name, the implementation MUST perform the "ToASCII" label conversion specified in Section 4.1 of RFC 3490. The label SHALL be considered a "stored string". That is, the AllowUnassigned flag SHALL NOT be set.

NEW

Domain Names may also be represented as distinguished names using domain components in the subject field, the issuer field, the subjectAltName extension, or the issuerAltName extension. As with the dNSName in the GeneralName type, the value of this attribute is defined as an IA5String. Each domainComponent attribute represents a single label. To represent a label from an IDN in the distinguished name, the implementation MUST convert all U-labels to A-labels.

2.4. Update in Section 7.5, Internationalized Electronic Mail Addresses

This update aligns with IDNA2008 and [ID.lamps-eai-addresses]. Since all of Section 7.5 is replaced, the OLD text is not provided.

NEW

Electronic Mail addresses may be included in certificates and CRLs in the subjectAltName and issuerAltName extensions, name constraints extension, authority information access extension, subject information access extension, issuing distribution point extension, or CRL distribution points extension. Each of these extensions uses the GeneralName construct. If the email address includes an IDN but the local-part of the email address can be represented in ASCII, then the email address is placed in the rfc822Name choice of GeneralName, which is defined as type IA5String. If the local-part of the internationalized email address cannot be represented in ASCII, then the internationalized email address is placed in the otherName choice of GeneralName using the conventions in [ID.lamps-eai-addresses].

7.5.1. Local-part Contains Only ASCII Characters

Where the host-part contains an IDN, conforming implementations MUST convert all U-labels to A-labels.

Two email addresses are considered to match if:

1) the local-part of each name is an exact match, AND

2) the host-part of each name matches using a case-insensitive ASCII comparison.

Implementations SHOULD convert the host-part of internationalized email addresses specified in these extensions to Unicode before display. Specifically, conforming implementations convert A-labels to U-labels for display.

7.5.2. Local-part Contains Non-ASCII Characters

When the local-part contains non-ASCII character, conforming implementations MUST place the internationalized email address in the SmtpUTF8Mailbox within the otherName choice of GeneralName as specified in Section 3 of [ID.lamps-eai-addresses]. Note that the UTF8 encoding of the internationalized email address MUST NOT contain a Byte-Order-Mark (BOM) [RFC3629] to aid comparison.

The comparison of two internationalized email addresses is specified in Section 5 of [ID.lamps-eai-addresses].

Implementations SHOULD convert the host-part of internationalized email addresses specified in these extensions to Unicode before display. Specifically, conforming implementations convert A-labels to U-labels for display.

3. Security Considerations

Conforming CAs SHOULD ensure that IDNs are valid. This can be done by validating all code points according to IDNA2008 [RFC5892]. Failure to use valid A-labels and valid U-labels may yield a domain name that cannot be correctly represented in the Domain Name System (DNS). In addition, the CA/Browser Forum offers some guidance regarding internal server names in certificates [CABF].

4. IANA Considerations

No IANA registries are changed by this update.

5. Normative References

[ID.lamps-eai-addresses] Melnikov, A. (Ed.) and W. Chuang (Ed.), "Internationalized Email Addresses in X.509 certificates", September 2017, <http://www.ietf.org/id/draft-ietf-lamps-eai-addresses>, work-in-progress.

[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>.

[RFC3492] Costello, A., "Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)", RFC 3492, DOI 10.17487/RFC3492, March 2003, <http://www.rfc-editor.org/info/rfc3492>.

[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>.

[RFC3987] Duerst, M. and M. Suignard, "Internationalized Resource Identifiers (IRIs)", RFC 3987, DOI 10.17487/RFC3987, January 2005, <http://www.rfc-editor.org/info/rfc3987>.

[RFC4518] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP): Internationalized String Preparation", RFC 4518, DOI 10.17487/RFC4518, June 2006, <http://www.rfc-editor.org/info/rfc4518>.

[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>.

[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>.

[RFC5892] Faltstrom, P., Ed., "The Unicode Code Points and Internationalized Domain Names for Applications (IDNA)", RFC 5892, DOI 10.17487/RFC5892, August 2010, <http://www.rfc-editor.org/info/rfc5892>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017. <http://www.rfc-editor.org/info/rfc8174>.

6. Informative References

[CABF] CA/Browser Forum, "Internal Server Names and IP Address Requirements for SSL", Version 1.0, June 2012, <https://cabforum.org/internal-names/>

[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>.

Acknowledgements

Thanks to Alexey Melnikov for the encouragement to write this update. Thanks to John Klensin and Patrik Falstrom for confirming many of the details in this update. Thanks to Ben Campbell, Wei Chuang, Spencer Dawkins, Phillip Hallam-Baker, Warren Kumari, Alexey Melnikov, Adam Roach, Tim Ruehsen, and Sean Turner for their careful review and comments.

Authors' Address

Russ Housley
Vigil Security, LLC
918 Spring Knoll Drive
Herndon, VA 20170
USA

EMail: housley@vigilsec.com