Internationalization Updates to RFC 5280

Abstract

The updates to RFC 5280 described in this document 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 is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8399.
Copyright Notice

Copyright (c) 2018 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
(https://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 contain material from IETF Documents or IETF
Contributions published or made publicly available before November
10, 2008. The person(s) controlling the copyright in some of this
material may not have granted the IETF Trust the right to allow
modifications of such material outside the IETF Standards Process.
Without obtaining an adequate license from the person(s) controlling
the copyright in such materials, this document may not be modified
outside the IETF Standards Process, and derivative works of it may
not be created outside the IETF Standards Process, except to format
it for publication as an RFC or to translate it into languages other
than English.

Table of Contents

1. Introduction .................................................... 3
   1.1. Terminology ............................................. 3
2. Updates to RFC 5280 ........................................ 3
   2.1. Update in the Introduction (Section 1) ................. 4
   2.2. Update in Name Constraints (Section 4.2.1.10) ........ 4
   2.3. Update in IDNs in GeneralName (Section 7.2) .......... 5
   2.4. Update in IDNs in Distinguished Names (Section 7.3) ... 6
   2.5. Update in Internationalized Electronic Mail
        Addresses (Section 7.5) ................................ 6
3. Security Considerations ....................................... 7
4. IANA Considerations .......................................... 8
5. References .................................................... 8
   5.1. Normative References .................................. 8
   5.2. Informative References ................................ 9
Acknowledgements .................................................. 9
Author’s Address .................................................. 9
1. Introduction

This document updates 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 of RFC 5280 [RFC5280] 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 a U-label to an A-label is described in [RFC5891].

The GeneralName structure supports many different name forms, including otherName for extensibility. RFC 8398 [RFC8398] specifies the SmtpUTF8Mailbox for internationalized email addresses, which includes IDNs with U-labels.


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 to RFC 5280

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 the Introduction (Section 1)

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 Name Constraints (Section 4.2.1.10)

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 [RFC8398] 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".
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 IDNs in GeneralName (Section 7.2)

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

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 IDNs, 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.

2.4. Update in IDNs in Distinguished Names (Section 7.3)

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.

2.5. Update in Internationalized Electronic Mail Addresses (Section 7.5)

This update aligns with IDNA2008 and RFC 8398 [RFC8398]. 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 RFC 8398 [RFC8398].

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 characters, conforming implementations MUST place the internationalized email address in the SmtpUTF8Mailbox within the otherName choice of GeneralName as specified in Section 3 of RFC 8398 [RFC8398]. 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 RFC 8398 [RFC8398].

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

This document has no IANA actions.

5. References

5.1. Normative References


5.2. Informative References


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.

Author’s Address

Russ Housley
Vigil Security, LLC
918 Spring Knoll Drive
Herndon, VA 20170
United States of America

Email: housley@vigilsec.com