INTERNET-DRAFT
Internet Engineering Task Force
Intended Status: Proposed Standard
Updates: RFC 5280 (once approved)
Expires: 5 July 2017

R. Housley
Vigil Security

5 January 2017

Internationalization Updates to RFC 5280
draft-housley-rfc5280-i18n-update-00

Abstract

These updates to RFC 5280 provide clarity on the handling of Internationalized Domain Names (IDNs) and 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

These updates to the Introduction and Section 7 of RFC 5280 [RFC5280] provide clarity on the handling of Internationalized Domain Names (IDNs) and Internationalized Email Addresses in X.509 Certificates.

IDNs are converted to punycode. The punycode form is carried in certificate, and the punycode form is used to compare two IDNs.

The conversion to punycode is defined in Section 4 of RFC 3490 [RFC3490]. In addition, Section 7.2 of RFC 5280 [RFC5280] provides some guidance about the flags used in that process. That guidance is not changed by this update.

Note that Internationalized Domain Names in Applications specification published in 2008 (IDNA2008) [RFC5891][RFC5892] also refer to RFC 3490 for the conversion to punycode.

Internationalized Email Addresses that contain non-ASCII characters in the local-part of the address follow the conventions recently specified by the IETF LAMPS working group.

1.1. Terminology

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 RFC 2119 [RFC2119].

2. Updates

This section provides updates to several paragraphs in the Introduction and Section 7 of RFC 5280 [RFC5280]. For clarity, the original text and the replacement text are shown.

2.1. Update in Section 1, Introduction

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 [RFC3490], [RFC3987], [RFC4518], [RFC5890], and [RFC5891].

2.2. Update in Section 7.2, IDNs in GeneralName

OLD

> IA5String is limited to the set of ASCII characters. To accommodate internationalized domain names in the current structure, conforming implementations MUST convert internationalized domain names to the ASCII Compatible Encoding (ACE) format as specified in Section 4 of RFC 3490 before storage in the dNSName field. Specifically, conforming implementations MUST perform the conversion operation specified in Section 4 of RFC 3490, with the following clarifications:
>
> ...

Implementations should convert IDNs to Unicode before display. Specifically, conforming implementations should perform the conversion operation specified in Section 4 of RFC 3490, with the following clarifications:

NEW

IA5String is limited to the set of ASCII characters. To accommodate internationalized domain names in the current structure, conforming implementations MUST convert IDNs [RFC5890][RFC5891] to the ASCII Compatible Encoding (ACE) format as specified in Section 4 of [RFC3490] before placement in the dNSName field. Specifically,

conforming implementations MUST perform the conversion operation specified in Section 4 of [RFC3490], with the following clarifications:

...

Implementations should convert IDNs to Unicode before display. Specifically, conforming implementations should perform the conversion operation specified in Section 4 of [RFC3490], with the following clarifications:

2.3. Update in Section 7.3, IDNs in Distinguished Names

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 perform the "ToASCII" label conversion specified in Section 4.1 of [RFC3490]. The label SHALL be considered a "stored string". That is, the AllowUnassigned flag SHALL NOT be set.

2.4. Update in Section 7.5, Internationalized Electronic Mail Addresses

OLD

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; GeneralName includes the rfc822Name choice, which is defined as type IA5String. To accommodate email addresses with internationalized domain names using the current structure, conforming implementations MUST convert the addresses into an ASCII representation.

Where the host-part (the Domain of the Mailbox) contains an internationalized name, the domain name MUST be converted from an IDN to the ASCII Compatible Encoding (ACE) format as specified in Section 7.2.

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 should perform the

conversion of the host-part of the Mailbox as described in Section 7.2.

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 the domain name into an ASCII representation using the ASCII Compatible Encoding (ACE) format as specified in Section 7.2.

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 should perform the conversion of the host-part of the Mailbox as described in Section 7.2.

7.5.2. Local-part Contains Non-ASCII Characters

When the local-part contains non-ASCII character, conforming implementations MUST be placed in the SmtpUtf8Name 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 4 of [ID.lamps-eai-addresses].

Implementations should convert the local-part and the host-part of internationalized email addresses placed in these extensions to Unicode before display.

3. Security Considerations

The security considerations in RFC 5280 [RFC5280] are not changed by this update.

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", December 2016, <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>.

[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>.

[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>.

[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>.

6. Informative References

[RFC3639] St. Johns, M., Ed., Huston, G., Ed., and IAB, "Considerations on the use of a Service Identifier in Packet Headers", RFC 3639, DOI 10.17487/RFC3639, October 2003, <http://www.rfc-editor.org/info/rfc3639>.

Acknowledgements

Thanks to John Klensin for confirming many of the details in this update.

Thanks to Alexey Melnikov for the encouragement to write this update.

Authors' Address

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

EMail: housley@vigilsec.com