Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 11, 2018

J. Levine
Taughannock Networks

February 7, 2018

E-mail Authentication for Internationalized Mail
draft-levine-appsarea-eaiauth-03

Abstract

SPF, DKIM, and DMARC enable a domain owner to publish e-mail authentication and policy information in the DNS. In internationalized e-mail, domain names can occur both as U-labels and A-labels. The Authentication-Results header reports the result of authentication checks made with SPF, DKIM, DMARC, and other schemes. This specification clarifies when to use which form of domain names when using SPF, DKIM, and DMARC and when creating Authentication-Results headers.

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 https://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 11, 2018.

Table of Contents

1. Introduction

SPF, DKIM, and DMARC enable a domain owner to publish e-mail authentication and policy information in the DNS. SPF primarily publishes information about what host addresses are authorized to send mail for a domain. DKIM places cryptographic signatures on e-mail messages, with the validation keys published in the DNS. DMARC publishes policy information related to the domain in the From: header of e-mail messages.

In conventional e-mail, all domain names are ASCII in all contexts so there is no question about the representation of the domain names. All internationalized domain names are represented as A-labels [RFC5890] in unencoded message bodies, in SMTP sessions, and in the DNS. Internationalized mail [RFC6530] allows U-labels in SMTP sessions [RFC6531] and in message headers [RFC6532].

Every U-label is equivalent to an A-label, so in principle the choice of label format should not cause any ambiguities. But in practice, consistent use of label formats will make it more likely that mail senders' and receivers' code interoperates.

Internationalized mail also allows arbitrary UTF-8 strings in the local parts of mailbox names, which were historically arbitrary ASCII.

2. Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" when written in upper case in in this document are to be interpreted as described in [RFC2119].

The term IDN, for Internationalized Domain Name, refers to either a U-label or an A-label.

Since DMARC is not currently a standards track protocol, this specification offers advice rather than requirements for DMARC.

3. General principles

In headers in EAI mail messages, domain names that were restricted to ASCII can now be U-labels, and mailbox local parts can be arbitrary UTF-8. Header names and other text intended primarily to be interpreted by computers rather than read by people remains ASCII.

Strings stored in DNS records remain ASCII since there is no way to tell whether a client retrieving a DNS record expects an EAI or an ASCII result. When a domain name found in a mail header includes U-labels, those labels are translated to A-labels before being looked up in the DNS, as described in [RFC5891].

4. SPF and internationalized mail

SPF [RFC7208] uses two identities from the SMTP session, the host name in the EHLO command, and the domain in the address in the MAIL FROM command. Since the EHLO command precedes the server response that tells whether the server supports the SMTPUTF8 extension, an IDN domain name argument MUST be represented as an A-label. An IDN domain name in MAIL FROM can be either U-labels or an A-labels.

All U-labels MUST be converted to A-labels before being used for an SPF validation. This includes both the original DNS lookup, described in Section 3 of [RFC7208] and the macro expansion of domain-spec described in section 7. Section 4.3 of [RFC7208] states that all IDNs in an SPF DNS record MUST be A-labels; this rule is unchanged since any SPF record can be used to authorize either EAI or conventional mail.

SPF macros %s and %l expand the local-part of the sender's mailbox. If the local-part contains non-ASCII characters, terms that include %s or %l do not match anything.

5. DKIM and internationalized mail

DKIM [RFC6376] specifies a message header that contains a cryptographic message signature and a DNS record that contains the validation key.

Section 3.5 of [RFC6376] states that IDNs in the d=, i=, and s= tags of a DKIM-Signature header MUST be encoded as A-labels. This rule is relaxed only for headers in internationalized messages [RFC6532] so IDNs MAY be represented either as A-labels or U-labels. This provides improved consistency with other headers, particularly since the local-part of the i= tag is likely to be UTF-8 rather than ASCII. When computing or verifying the hash in a DKIM signature as described in section 3.7, the hash MUST use the domain name in the format it occurs in the header.

DKIM key records, described in section 3.6.1, do not contain domain names, so there is no change to their specification.

6. DMARC and internationalized mail

DMARC [RFC7489] defines a policy language that domain owners can specify for the domain of the address in a RFC5322.From header.

Section 6.6.1 specifies, somewhat imprecisely, how IDNs in the RFC5322.From address domain are to be handled. That section is updated to say that all U-labels in the domain are converted to A-labels before further processing. Sections 6.7 and 7.1 are similarly updated to say that all U-labels in domains being handled are converted to A-labels before further processing.

DMARC policy records, described in section 6.3, can contain e-mail addresses in the rua and ruf tags. Since a policy record can be used for both internationalized and conventional mail, those addresses have to be conventional addresses, not internationalized addresses.

7. Authentication-Results and internationalized mail

The Authentication-Results [RFC7601] header reports the results of authentication tests made using a variety of authentication schemes.

In EAI messages, in every place where a domain name may appear in an Authentication-Results header, that domain name MAY be stored as a U-label. In the ABNF descriptions in section 2.2, each domain-name MAY be a U-label, and each local-part MAY be arbitrary UTF-8.

When a domain name is used as an authserv-id described in section 2.5, it MAY be a U-label.

In section 2.7.1, the domain name in the DKIM header.d field MAY be a U-label.

In section 2.7.4, the authentication identity and mailbox MAY include a UTF-8 local-part and U-label domain name.

In S/MIME signature verification [RFC7281] results, the body.smime-identifier parameter MAY include a UTF-8 local-part and U-label domain name.

8. IANA Considerations

This document makes no request of IANA.

9. Security Considerations

E-mail is subject to a vast range of threats and abuses. This document attempts to slightly mitigate some of them but does not, as far as the author knows, add any new ones.

10. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5890] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, DOI 10.17487/RFC5890, August 2010, <https://www.rfc-editor.org/info/rfc5890>.

[RFC5891] Klensin, J., "Internationalized Domain Names in Applications (IDNA): Protocol", RFC 5891, DOI 10.17487/RFC5891, August 2010, <https://www.rfc-editor.org/info/rfc5891>.

[RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011, <https://www.rfc-editor.org/info/rfc6376>.

[RFC6530] Klensin, J. and Y. Ko, "Overview and Framework for Internationalized Email", RFC 6530, DOI 10.17487/RFC6530, February 2012, <https://www.rfc-editor.org/info/rfc6530>.

[RFC6531] Yao, J. and W. Mao, "SMTP Extension for Internationalized Email", RFC 6531, DOI 10.17487/RFC6531, February 2012, <https://www.rfc-editor.org/info/rfc6531>.

[RFC6532] Yang, A., Steele, S., and N. Freed, "Internationalized Email Headers", RFC 6532, DOI 10.17487/RFC6532, February 2012, <https://www.rfc-editor.org/info/rfc6532>.

[RFC7208] Kitterman, S., "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1", RFC 7208, DOI 10.17487/RFC7208, April 2014, <https://www.rfc-editor.org/info/rfc7208>.

[RFC7281] Melnikov, A., "Authentication-Results Registration for S/MIME Signature Verification", RFC 7281, DOI 10.17487/RFC7281, June 2014, <https://www.rfc-editor.org/info/rfc7281>.

[RFC7489] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015, <https://www.rfc-editor.org/info/rfc7489>.

[RFC7601] Kucherawy, M., "Message Header Field for Indicating Message Authentication Status", RFC 7601, DOI 10.17487/RFC7601, August 2015, <https://www.rfc-editor.org/info/rfc7601>.

Appendix A. Change history

02 to 03 SPF local-part macros don't match non-ASCII. Add S/MIME auth results.

Author's Address

John Levine
Taughannock Networks
PO Box 727
Trumansburg, NY 14886

Phone: +1 831 480 2300
Email: standards@taugh.com
URI: http://jl.ly