                E-mail Authentication for Internationalized Mail
                        draft-ietf-dmarc-eaiauth-00

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

Copyright Notice

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.

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 UTF-8 characters in the local
   parts of mailbox names, which were historically only 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] and [RFC8174].

   The term IDN, for Internationalized Domain Name, refers to a doman
   name containing either U-labels or A-labels.

   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 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
   argument MUST be represented as an A-label. An IDN 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. (Note that unlike U-labels, there is
   no way to rewrite non-ASCII local parts into ASCII.)

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 2.11 of [RFC6376] defines dkim-quoted-printable. Its
definition is modified in internationalized messages so that non-
ASCII UTF-8 characters need not be quoted. The ABNF for dkim-safe-
char in internationalized messages is replaced by the following:

```
dkim-safe-char        =  %x21-3A / %x3C / %x3E-7E / %x80-FF
                      ; '!' - ':', '<', '>' - '~', non-ASCII
```

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 SHOULD be represented as U-labels but MAY be A-labels. This
provides improved consistency with other headers. The set of
allowable characters in the local-part of an i= tag is extended as
described in [RFC6532]. 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 sections 6.3 and 7.1, 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 still have to be conventional addresses, not
internationalized addresses.

7. IANA Considerations

   This document makes no request of IANA.

8. 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.

9. 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>.

   [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>.

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

Appendix A. Change history

   00 First WG version

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