Workgroup: EMAILCORE
Internet-Draft: draft-ietf-emailcore-as-05
Published: 23 May 2022
Intended Status: Standards Track
Expires: 24 November 2022
Authors: J.C. Klensin, Ed. K. Murchison, Ed. E. Sam, Ed.
Fastmail

Applicability Statement for IETF Core Email Protocols

Abstract

Electronic mail is one of the oldest Internet applications that is still in very active use. While the basic protocols and formats for mail transport and message formats have evolved slowly over the years, events and thinking in more recent years have supplemented those core protocols with additional features and suggestions for their use. This Applicability Statement describes the relationship among many of those protocols and provides guidance and makes recommendations for the use of features of the core protocols.

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 24 November 2022.

Table of Contents

1. Introduction

In its current form, this draft is a placeholder and beginning of an outline for the Applicability Statement that has been discussed as a complement for proposed revisions of the base protocol specifications for SMTP [RFC5321] (being revised as [I-D.ietf-emailcore-rfc5321bis]) and Internet Message Format [RFC5322] (being revised as [I-D.ietf-emailcore-rfc5322bis]). Among other things, it is expected to capture topics that a potential WG concludes are important but that should not become part of those core documents.

As discussed in [RFC2026],

> "An Applicability Statement specifies how, and under what circumstances, one or more TSs may be applied to support a particular Internet capability."

That form of a standards track document is appropriate because one of the roles of such a document is to explain the relationship among technical specifications, describe how they are used together, and make statements about what is "required, recommended, or elective".

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 [RFC2119] and [RFC8174].

2. Applicability of Some SMTP Provisions

Over the years since RFC 5321 was published in October 2008, usage of SMTP has evolved, machines and network speeds have increased, and the frequency with which SMTP senders and receivers have to be prepared to deal with systems that are disconnected from the Internet for long periods or that require many hops to reach has decreased. During the same period, the IETF has become much more sensitive to privacy and security issues and the need to be more resistant or robust against spam and other attacks. In addition SMTP (and Message Format) extensions have been introduced that are expected to evolve the Internet's mail system to better accommodate environments in which Basic Latin Script is not the norm.

This section describes adjustments that may be appropriate for SMTP under various circumstances and discusses the applicability of other protocols that represent newer work or that are intended to deal with relatively newer issues.

2.1. Handling of the Domain Argument to the EHLO Command

If the Domain argument to the EHLO command does not have an address record in the DNS that matches the IP address of the client, the SMTP server may refuse any mail from the client as part of established anti-abuse practice. Operational experience has demonstrated that the lack of a matching address record for the the domain name argument is at best an indication of a poorly-configured MTA, and at worst that of an abusive host.

2.2. Use of Address Literals

The address-literal ABNF non-terminal is used in various places in [I-D.ietf-emailcore-rfc5321bis] grammar however, for SMTP connections over the public internet, an address-literal as the argument to EHLO

command or the Domain part of the Mailbox argument to the MAIL FROM command is quite likely to result in the message being rejected as a matter of policy at many sites, since they are deemed to be signs of at best a misconfigured server, and at worst either a compromised host or a server that's intentionally configured to hide its identity.

2.3. Use of Addresses in Top-Level Domains

While addresses in top-level domains (TLDs) are syntactically valid, mail to these addresses has never worked reliably. A handful of country code TLDs have top level MX records but they have never been widely used nor well supported. In 2013 [RFC7085] found 18 TLDs with MX records, which dropped to 17 in 2021 despite many new TLDs having been added.

Mail sent to addresses with single label domains has typically expected the address to be an abbreviation to be completed by a search list, so mail to bob@sales would be completed to bob@sales.example.com. This shortcut has led to unfortunate consequnces; in one famous case, in 1991 when the .CS domain was added to the root, mail in computer science departments started to fail as mail to bob@cs was now treated as mail to Czechoslovakia. Hence, for reliable service, mail SHOULD NOT use addreses that contain single label domains.

2.4. Use of SMTP Extensions

As SMTP has evolved over the years, several extensions have become ubiquitous. As a result, the following extensions MUST be supported by SMTP senders and receivers:

- 8-bit MIME [RFC6152]
- Deliver Status Notifications [RFC3461]

Similarly, the following extensions SHOULD be supported by SMTP senders and receivers:

- Command Pipelining [RFC2920]
- Internationalized Email [RFC6531]

Furthermore, while Enhanced Mail System Status Codes ([RFC3463], [RFC5248]) are widely supported, they are not ubiquitous. Nevertheless, they have been found to be useful to SMTP senders in determining the exact reason for a transmission failure in a machine-readable, language-independent manner, thus allowing them to present more detailed and language-specific error messages to users. Given the usefulness of these enhanced codes, SMTP receivers are

RECOMMENDED to implement the SMTP Service Extension for Returning Enhanced Error Codes [RFC2034] utilizing the codes registered in [RFC5248].

3. Applicability of Message Format Provisions

This section describes adjustments to the Internet Message Format that may be appropriate under various circumstances.

3.1. Use of Empty Quoted Strings

The quoted-string ABNF non-terminal is used in various places in rfc5322bis grammar. While it allows for empty quoted string, such construct is going to cause interoperability issues when used in certain header fields. In particular, use of empty quoted strings is NOT RECOMMENDED in "received-token" (a component of a Received header field), "keywords" (a component of a Keywords header field) and "local-part" (left hand side of email addresses). Use of empty quoted strings is in particular problematic in the "local-part". For example, all of the following email addresses are non interoperable:

""".bar@example.com

foo.""@example.net

""@example.com

Use of empty quoted strings is fine in "display-name".

4. MIME and Its Implications

When the work leading to the original version of the MIME specification was completed in 1992 [RFC1341], the intention was that it be kept separate from the specification for basic mail headers in RFC 822 [RFC0822]. That plan was carried forward into RFC 822's successors, [RFC2822] and [RFC5322] and the successors of that original MIME specification including [RFC2045]. The decision to do so was different from the one made for SMTP, for which the core specification was changed to allow for the extension mechanism [RFC1425] which was then incorporated into RFC 5321 and its predecessor [RFC2821].

Various uses of MIME have become nearly ubiquitous in contemporary email while others may have fallen into disuse or been repurposed from the intent of their original design.

It may be appropriate to make some clear statements about the applicability of MIME and its features.

5. Confidentiality and Authentication with SMTP

SMTP is specified without embedded mechanisms for authentication or confidentiality; its traffic is therefore "in the clear". Years of operational experience have shown that such transmission exposes the message to easy compromise, including wiretapping and spoofing. To mitigate these risks, operation of SMTP has evolved over the years so that it is used with the benefit of Transport Layer Security (TLS) [RFC8446] to provide both confidentiality and authentication in the transmission of messages. This section discusses those topics and their most common uses.

It is important that the reader understand what is meant by the terms "Authentication" and "Confidentiality", and for that we will borrow directly from RFC8446.

* Authentication is the process of establishing the identity of one or more of the endpoints of a communication channel. TLS only requires authentication of the server side of the communication channel; authentication of the client side is optional.

* The term "confidentiality" describes a state where the data (i.e., the message) is transmitted in a way that it is only visible to the endpoints of a communication channel.

It is not uncommon for implementers to use the term "encryption" to mean "confidentiality", but this is not quite correct. Rather, encryption using TLS is the current method by which confidentiality is achieved with SMTP, but that does not mean that future methods might not be developed.

Note: With typical email use of TLS, authentication only is performed for the target receiving server and is not done for the sending client. That is, it serves to validate that the connection has been made to the intended server, but does not validate who initiated it.

5.1. Optional Confidentiality

The most common implementation of message confidentiality is what's known as "opportunistic TLS", which is frequently referred to as "opportunistic encryption". With this method, a receiving server announces in its greeting that it is capable of supporting TLS encryption through the presence of the "STARTTLS" keyword. The sending client then attempts to negotiate an encrypted connection, and if successful, transmits the message in encrypted form; if negotiation fails, the client falls back to sending the message in clear text.

Opportunistic TLS is confidentiality without authentication, because no effort is made to authenticate the receiving server, and it is

optional confidentiality due to the ability to fall back to transmission in the clear if a secure connection cannot be established. That said, most modern implementations of SMTP support this method, especially at the largest mailbox providers, and so the vast majority of email traffic is encrypted during its time transiting from the client to the server.

Note: While TLS provides protection while the message is in transit, there is no guarantee that the message will be stored in encrypted fashion at its destination. In fact, storage in plain text should be expected!

5.2. Required Confidentiality, with Receiving Server Authentication

Two protocols exist that move message confidentiality from optional to required (with conditions as noted below) - MTA-STS [RFC8461] and DANE for SMTP [RFC7672]. While they differ in their implementation details, receiving servers relying on either protocol are stating that they only accept mail if the transmission can be encrypted with TLS, and a failure to negotiate a secure connection MUST result in the sending client refusing to transmit the message. Support for both protocols is increasing, but is not yet mandatory.

These two protocols differ from Opportunistic TLS in that they require receiving server authentication and there is no fallback to sending in the clear if negotiation of an encrypted connection fails.

Note: Both protocols mentioned in this section rely not only on the receiving server but also the sending client supporting the protocol intended to be used. If the sending client does not implement or understand the protocol requested by the receiving server, the sending client will use Opportunistic TLS or clear-text to transmit the message.

5.3. Message-Level Authentication

Protocols exist to allow for authentication of different identities associated with an email message - SPF [RFC7208] and DKIM [RFC6376]. A third protocol, DMARC [RFC7489], relies on SPF and DKIM to allow for validation of the domain in the visible From header, and a fourth, ARC [RFC8617], provides a way for each hop to record results of authentication checks performed at that hop.

All of these are outside the scope of this document, as they are outside the scope of SMTP. They deal with validating the authorized usage of one or more domains in an email message, and not with establishing the identity of the receiving server.

5.4. SMTP Authentication

SMTP Authentication [RFC4954], which is often abbreviated as SMTP AUTH, is an extension to SMTP. While its name might suggest that it would be within scope for this section of the Applicability Statement, nothing could be further from the truth.

SMTP AUTH defines a method for a client to identify itself to a Message Submission Agent (MSA) when presenting a message for transmission, usually using port 587 rather than the traditional port 25. The most common implementation of SMTP AUTH is for a person to present a username and password to their mailbox provider's outbound SMTP server when configuring their MUA for sending mail.

5.5. Message-Level Confidentiality

Protocols such as S/MIME [RFC8551] and OpenPGP [RFC4880] exist to allow for message confidentiality outside of the operation of SMTP. That is to say, using these protocols results in encryption of the message prior to its being submitted to the SMTP communications channel, and decryption of the message is the responsibility of the message recipient. There are numerous implementations of these protocols, too many to list here. As they operate fully independent of SMTP, they are out of scope for this document.

6. Acknowledgments

The Emailcore group arose out of discussions on the ietf-smtp group over changes and additions that should be made to the core email protocols. It was agreed upon that it was time to create a working group that would fix many potential errors and opportunities for misunderstandings within the RFCs.

7. IANA Considerations

This memo includes no requests to or actions for IANA. The IANA registries associated with the protocol specifications it references are specified in their respective documents.

8. Security Considerations

All drafts are required to have a security considerations section and this one eventually will.

... To be supplied ...

9. References

9.1. Normative References

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, DOI 10.17487/RFC2026, October 1996, <https://www.rfc-editor.org/info/rfc2026>.

[RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, DOI 10.17487/RFC2045, November 1996, <https://www.rfc-editor.org/info/rfc2045>.

[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>.

[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>.

9.2. Informative References

[I-D.ietf-emailcore-rfc5321bis] Klensin, J. C., "Simple Mail Transfer Protocol", Work in Progress, Internet-Draft, draft-ietf-emailcore-rfc5321bis-10, 7 March 2022, <https://www.ietf.org/archive/id/draft-ietf-emailcore-rfc5321bis-10.txt>.

[I-D.ietf-emailcore-rfc5322bis] Resnick, P. W., "Internet Message Format", Work in Progress, Internet-Draft, draft-ietf-emailcore-rfc5322bis-03, 4 April 2022, <https://www.ietf.org/archive/id/draft-ietf-emailcore-rfc5322bis-03.txt>.

[RFC0822] Crocker, D., "STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES", STD 11, RFC 822, DOI 10.17487/RFC0822, August 1982, <https://www.rfc-editor.org/info/rfc822>.

[RFC1341] Borenstein, N. and N. Freed, "MIME (Multipurpose Internet Mail Extensions): Mechanisms for Specifying and Describing the Format of Internet Message Bodies", RFC 1341, DOI 10.17487/RFC1341, June 1992, <https://www.rfc-editor.org/info/rfc1341>.

[RFC1425] Klensin, J., Freed, N., Ed., Rose, M., Stefferud, E., and D. Crocker, "SMTP Service Extensions", February 1993, <https://www.rfc-editor.org/info/rfc1425>.

[RFC2034] Freed, N., "SMTP Service Extension for Returning Enhanced Error Codes", RFC 2034, DOI 10.17487/RFC2034, October 1996, <https://www.rfc-editor.org/info/rfc2034>.

[RFC2821] Klensin, J., Ed., "Simple Mail Transfer Protocol", RFC 2821, DOI 10.17487/RFC2821, April 2001, <https://www.rfc-editor.org/info/rfc2821>.

[RFC2822] Resnick, P., Ed., "Internet Message Format", RFC 2822, DOI 10.17487/RFC2822, April 2001, <https://www.rfc-editor.org/info/rfc2822>.

[RFC2920] Freed, N., "SMTP Service Extension for Command Pipelining", STD 60, RFC 2920, DOI 10.17487/RFC2920, September 2000, <https://www.rfc-editor.org/info/rfc2920>.

[RFC3461] Moore, K., "Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)", RFC 3461, DOI 10.17487/RFC3461, January 2003, <https://www.rfc-editor.org/info/rfc3461>.

[RFC3463] Vaudreuil, G., "Enhanced Mail System Status Codes", RFC 3463, DOI 10.17487/RFC3463, January 2003, <https://www.rfc-editor.org/info/rfc3463>.

[RFC4880] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format", RFC 4880, DOI 10.17487/RFC4880, November 2007, <https://www.rfc-editor.org/info/rfc4880>.

[RFC4954] Siemborski, R., Ed. and A. Melnikov, Ed., "SMTP Service Extension for Authentication", RFC 4954, DOI 10.17487/RFC4954, July 2007, <https://www.rfc-editor.org/info/rfc4954>.

[RFC5248] Hansen, T. and J. Klensin, "A Registry for SMTP Enhanced Mail System Status Codes", BCP 138, RFC 5248, DOI 10.17487/RFC5248, June 2008, <https://www.rfc-editor.org/info/rfc5248>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <https://www.rfc-editor.org/info/rfc5321>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <https://www.rfc-editor.org/info/rfc5322>.

[RFC6152] Klensin, J., Freed, N., Rose, M., and D. Crocker, Ed., "SMTP Service Extension for 8-bit MIME Transport", STD 71, RFC 6152, DOI 10.17487/RFC6152, March 2011, <https://www.rfc-editor.org/info/rfc6152>.

[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>.

[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>.

[RFC7085] Levine, J. and P. Hoffman, "Top-Level Domains That Are Already Dotless", RFC 7085, DOI 10.17487/RFC7085, December 2013, <https://www.rfc-editor.org/info/rfc7085>.

[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>.

[RFC7672] Dukhovni, V. and W. Hardaker, "SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)", RFC 7672, DOI 10.17487/RFC7672, October 2015, <https://www.rfc-editor.org/info/rfc7672>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC8461] Margolis, D., Risher, M., Ramakrishnan, B., Brotman, A., and J. Jones, "SMTP MTA Strict Transport Security (MTA-STS)", RFC 8461, DOI 10.17487/RFC8461, September 2018, <https://www.rfc-editor.org/info/rfc8461>.

[RFC8551] Schaad, J., Ramsdell, B., and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification", RFC 8551, DOI 10.17487/RFC8551, April 2019, <https://www.rfc-editor.org/info/rfc8551>.

[RFC8617] Andersen, K., Long, B., Ed., Blank, S., Ed., and M. Kucherawy, Ed., "The Authenticated Received Chain (ARC) Protocol", RFC 8617, DOI 10.17487/RFC8617, July 2019, <https://www.rfc-editor.org/info/rfc8617>.

Appendix A. Change Log

RFC Editor: Please remove this appendix before publication.

A.1. Changes from draft-klensin-email-core-as-00 (2020-03-30) to draft-ietf-emailcore-as-00

*Change of filename, metadata, and date to reflect transition to WG document for new emailcore WG. No other substantive changes

A.2. Changes from draft-ietf-emailcore-as-00 (2020-10-06) to -01

*Added co-authors (list is in alphabetical order for the present).

*Updated references to 5321bis and 5322bis.

*Added note at top, "This version is provided as a document management convenience to update the author list and make an un-expired version available to the WG. There are no substantive changes from the prior version", which should be removed for version -02.

A.3. Changes from draft-ietf-emailcore-as-01 (2021-04-09) to -02

*Added new editors and also added some issues the emailcore group will be dealing with.

*Added reference to RFC 6648.

A.4. Changes from draft-ietf-emailcore-as-02 (2021-08-06) to -03

*Moved discussion of address-literals (issue #1) and domain names in EHLO (issue #19) under SMTP Provisions section

*Moved discussion of empty quoted-strings under Message Format Provisions section

*Added text on use of addresses in TLDs (issue #50)

*Marked all authors as editors.

*Miscellaneous editorial changes.

A.5. Changes from draft-ietf-emailcore-as-03 (2022-01-31) to -04

*Added requirements for SMTP extensions (issue #40).

A.6. Changes from draft-ietf-emailcore-as-04 (2022-05-21) to -05

*Added text addressing use ofx enhanced status codes.

*Added text addressing confidentiality and authentication (issue #54).

Authors' Addresses

John C Klensin (editor)
1770 Massachusetts Ave, Ste 322
Cambridge, MA 02140
United States of America

Phone: +1 617 245 1457
Email: john-ietf@jck.com

Kenneth Murchison (editor)
Fastmail US LLC
1429 Walnut Street - Suite 1201
Philadelphia, PA 19102
United States of America

Email: murch@fastmailteam.com

E Sam (editor)

Email: winshell64@gmail.com