

EMAILCORE WG

IETF 121

November 2024

Dublin

Chairs:

Alexey Melnikov <alexey.melnikov@isode.com>

Todd Herr <todd.herr@valimail.com>

Note Well

- This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.
- As a reminder:
 - By participating in the IETF, you agree to follow IETF processes and policies.
 - If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
 - As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
 - Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
 - As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (<https://www.ietf.org/contact/ombudsteam/>) if you have questions or concerns about this.

Note Well

(continued)

- Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:
 - BCP 9 (Internet Standards Process)
 - BCP 25 (Working Group processes)
 - BCP 25 (Anti-Harassment Procedures)
 - BCP 54 (Code of Conduct)
 - BCP 78 (Copyright)
 - BCP 79 (Patents, Participation)
 - <https://www.ietf.org/privacy-policy/> (Privacy Policy)

IETF Code Of Conduct Guidelines RFC 7154

- Treat colleagues with respect
- Speak slowly and limit the use of slang
- Dispute ideas by using reasoned argument
- Use best engineering judgment
- Find the best solution for the whole Internet
- Contribute to the ongoing work of the group and the IETF

Administrivia

- This session is being recorded
- Meetecho:
 - <https://meetings.conf.meetecho.com/ietf121/?session=33554>
- Shared note taking:
 - <https://notes.ietf.org/notes-ietf-121-emailcore>
- ***Note taker?***

Agenda

- Agenda bashing, administrivia, note well (chairs) - 5 mins
- Goals: review SecDir and DnsDir feedback on **rfc5321bis**
 - ***<https://github.com/ietf-wg-emailcore/emailcore/issues/>***
- Review A/S tickets, if time permits
- Note that we have two 1 hour session: on Thursday and on Friday

WG Status

- draft-ietf-emailcore-rfc5322bis is done
- draft-ietf-emailcore-rfc5321bis-33 is post IETF LC. Some possibly substantial comments from SecDir and DnsDir reviewers.
- draft-ietf-emailcore-as-12 had some updates after Vancouver IETF. Some issues brought up in SecDir/DnsDir might affect this document as well.

RFC 5321

"required destination mailbox" in description of RCPT TO is unclear

Difficulty: easy

<https://github.com/ietf-wg-emailcore/emailcore/issues/106>

Donald Eastlake wrote: Section 4.1.1.3, 2nd paragraph: I think the word "required" should be deleted here as superfluous. It also reads a bit oddly.

Current text:

The forward-path consists of the required destination mailbox.

Explanation: I read "required destination mailbox" as "not allowed to be empty, like empty return path in MAIL FROM".

Suggestion: no change.

RFC 5321

What is needed to get "Internet Standard" removed from RFC 821 when
5321bis is published

Difficulty: easy

<https://github.com/ietf-wg-emailcore/emailcore/issues/115>

John Klensin: This has been discussed in several messages on-list.
One option is to explicitly impose that as a requirement and/or a note
to the RFC Editor in 5321bis itself. Another is to handle it as an
administrative procedure, if necessarily tuning or clarifying an existing
one. See email, and comments in Section 1.2 of rfc5321bis-32

**Suggestion: punt to our responsible AD to create a management
item to sort this out.**

RFC 5321

Clarify where and how CNAME DNS RR can be used and any limitations

Difficulty: moderate

<https://github.com/ietf-wg-emailcore/emailcore/issues/121>

Ted Lemon wrote: Section 5.1 doesn't say what to do with chained CNAMEs.

After some mailing list discussion Ted proposed the following:

OLD:

Any other response, specifically including a value that will return a CNAME record when queried, lies outside the scope of this Standard. The prohibition on labels in the data that resolve to CNAMEs is discussed in more detail in RFC 2181, Section 10.3 [33].

NEW:

An MX record with a CNAME as its target is a misconfiguration, as explained in RFC2181, Section 1.3 [33]. However, implementations SHOULD still process CNAME responses when received, since a significant number of servers on the internet are configured with MX records pointing to CNAMEs.

RFC 5321

Unclear text in the last paragraph of Section 2.3.5

Difficulty: moderate

<https://github.com/ietf-wg-emailcore/emailcore/issues/98>

Donald Eastlake wrote: The first sentence of this paragraph is of questionable grammar and, in any case, extremely hard to parse.

OLD:

When domain names are used in SMTP, and unless further restricted in this document, names that can be resolved to MX RRs or address (i.e., A or AAAA) RRs (as discussed in Section 5) are permitted, as are CNAME RRs whose targets can be resolved, in turn, to MX or address RRs.

Assuming I have parsed it correctly, how about:

NEW:

Unless further restricted in this document, domain names used in SMTP are names that can be resolved to MX or address (A or AAAA) RRs (see also Section 5), or to CNAME RRs that can be resolved to an MX or address RR.

RFC 5321

Additional security considerations: STARTTLS, DKIM, etc

Difficulty: moderate

<https://github.com/ietf-wg-emailcore/emailcore/issues/113> (More explanation of the advantages of transport and encryption between SMTP systems)

<https://github.com/ietf-wg-emailcore/emailcore/issues/109> (STARTTLS discussion in, or pointer from, rfc5321bis security considerations)

<https://github.com/ietf-wg-emailcore/emailcore/issues/110> (References to DKIM, etc)

<https://github.com/ietf-wg-emailcore/emailcore/issues/112> (Expand the comment in the 5321bis introduction about the A/S to contain more detail?)

A/S already talks about most of these.

Possible solutions to these issues:

1. Move the text from A/S to rfc5321bis
2. Normative reference from rfc5321bis to A/S
3. Use the text in #112. Keep the reference as informative, but submit A/S and rfc5321bis to IESG at the same time

Or some combinations of the above?

I think we need guidance from our AD/IESG.

Time Limit this discussion to 10 minutes, unless making lots of progress.

RFC 5321

Should we further deprecate TURN or document it more?

Difficulty: moderate

<https://github.com/ietf-wg-emailcore/emailcore/issues/108>

Should we further deprecate or prohibit TURN, or explain conditions under which it might be appropriate and be safely used?

Current text in Appendix E.1 (under Deprecated features):

This command, described in RFC 821, raises important security issues since, in the absence of strong authentication of the host requesting that the client and server switch roles, it can easily be used to divert mail from its correct destination. Its use is deprecated; SMTP systems ***SHOULD NOT use it unless*** the **server can authenticate** the client.

Alexey: suggestion to change "**SHOULD NOT**" to "**MUST NOT**", because the "use it unless" part of the last sentence already allows implementations when needed. This also avoids writing any further security considerations about TURN!

RFC 5321

What is Section 7.1 about? Authenticity only?

Difficulty: slightly more difficult

<https://github.com/ietf-wg-emailcore/emailcore/issues/111>

John Klensin: Donald Eastlake pointed out, and others noticed and pointed out during the Last Call discussion, that this section is really entirely about authentication and not other security issues. His suggestion is to change the first sentence to "The authenticity of SMTP mail is not secure...". A more drastic fix would be to make the authenticity focus more explicit and/or to add a separate subsection discussing encryption issues.

Up to the WG.

Because of the hop by hop problem, if we adopt his text, we may want to retain (and explain further if necessary), "inherently".

RFC 5321

Clarify text in Section 2.3.12

Difficulty: easy

<https://github.com/ietf-wg-emailcore/emailcore/issues/99>

Donald Eastlake wrote: Section 2.3.12, first sentence: Appears to have missing text and/or have grammatical errors and is hard to parse.

Original text:

This document distinguishes between an "SMTP session" (interchangeable with "mail session") and starting when a connection is made between client and server and a "mail transaction", which is started and terminated by particular commands.

New:

This document distinguishes between an "SMTP session" and a "mail transaction". An SMTP session, often called a "mail session", starts when a connection is made between client and server, ending when that connection is terminated. A "mail transaction" is started and terminated by particular commands, most often MAIL and RSET or QUIT (the latter also instructs the server to close the SMTP session).

Just checking that this change is acceptable to the WG.

RFC 5321

Prohibition on MAIL FROM during transaction is unclear in Section 4.1.4

Difficulty: easy

<https://github.com/ietf-wg-emailcore/emailcore/issues/101>

Donald Eastlake wrote: Donald Eastlake wrote:

Section 4.1.4, page 49, 3rd paragraph: This "MAIL MUST NOT be sent" text seems confusing at a minimum. To most readers MAIL is "being sent" with every RCPT command, with the DATA command, and with every new line of mail content. Please re-word it so it's something about "initiating" the sending of mail or the like.

Suggested replacement:

The MAIL command MUST NOT be sent if a mail transaction is already open ...

Just checking that this change is acceptable to the WG.

RFC 5321

Section 3.5.2: Name of section should include EXPN

Difficulty: easy

<https://github.com/ietf-wg-emailcore/emailcore/issues/104>

The name of the section is "VRFY Normal Response", but it also talks about EXPN.

Should this be "VRFY **and EXPN** Normal Response" or similar?

RFC 5321

SHOULD requirement on accepting trailing spaces in commands in section
4.1.1

Difficulty: easy

<https://github.com/ietf-wg-emailcore/emailcore/issues/105>

Donald Eastlake wrote: Section 4.1.1: Suggest removing the parenthesis around the parenthetical. It seems like a fine top-level sentence and a reader might wonder why it is in parenthesis. For example, they might somehow think that it weakens the "SHOULD".

Current text:

The SMTP commands define the mail transfer or the mail system function requested by the user. SMTP commands are character strings terminated by . The commands themselves are alphabetic characters terminated by if parameters follow and otherwise. (**In the interest of improved interoperability, SMTP receivers SHOULD tolerate trailing white space before the terminating.**) The syntax of the local part of a mailbox MUST conform to receiver site conventions and the syntax specified in Section 4.1.2.

Suggestion: no change.

RFC 5321

Functional Groups in Section 4.2.2 are unclear
Difficulty: slightly more difficult

<https://github.com/ietf-wg-emailcore/emailcore/issues/102>

Donald Eastlake wrote: Section 4.2.2: OK, but what are these "Functional Groups"? Some sort of subheadings (not necessarily part of the hierarchical numbering) are needed.

The latest version restored formatting so that grouping is visible.

John Klensin: As of his 2024-10-27 message at <<https://mailarchive.ietf.org/arch/msg/last-call/1qEIdmIXiDGhLkFnvEwppEZMfCs>>, Donald still believes that we should add subheadings. Not clear to me what those would be even if the WG agreed.

Suggestion: no further change.

RFC 5321

In rfc5321bis, adding "(or HELO)" in more places

Difficulty: slightly more difficult

<https://github.com/ietf-wg-emailcore/emailcore/issues/116>

Donald Eastlake pointed out: 'Seems simple enough to me. There are ~83 occurrences of EHLO in the document. There are plenty of places where it is clear that EHLO is mentioned in relation to extensions, so HELO is irrelevant. And there are a number of places where "EHLO (or HELO)" is already used. For the remaining sections where EHLO is mentioned, I suggest replacing the first and only the first occurrence of "EHLO" in each of the following numbered sections with "EHLO (or HELO)":

3.3, 4.1.1.5, 4.1.4, 4.2.4.2, 4.4.1 and 4.4.5

Not 4.2, 4.2.4.1 (and 4.4.5 instead of 4.4.3) as in the ticket

In particular, this clarifies that HELO also resets the current transaction, like EHLO.

RFC 5321

Why is the requirement not to append extra info at the end of EHLO is only a SHOULD NOT?

Difficulty: slightly more difficult

<https://github.com/ietf-wg-emailcore/emailcore/issues/107>

(From Ted Lemon): Paragraph 2 of Section 4.1.1.1 says:

RFC 2821, and some earlier informal practices, encouraged following the literal by information that would help to identify the client system. That convention was not widely supported, and many SMTP servers considered it an error. In the interest of interoperability, it is probably wise for servers to be prepared for this string to occur, but SMTP clients **SHOULD NOT** send it.

Suggestion: **SHOULD NOT** ==> **MUST NOT**. Also clarify that this change would make such clients non-conformant.

RFC 5321 (1 of 2)

Do Sections 6.1 and 6.2 of 5321bis require clarification and/or rewriting?

Difficulty: slightly more difficult

<https://github.com/ietf-wg-emailcore/emailcore/issues/114>

Donald Eastlake wrote:

Section 6.1: I do not quite understand saying that something is mandatory/required and then talking about where it is impossible or impractical to do that thing. Section 6.1 says, concerning a host holding an email message, "It MUST NOT lose the message for frivolous reasons, such as because the host later crashes ...". "frivolous" does not seem very well defined for a mandatory implementation requirement. The only examples given later of non-frivolous reasons seem to be spam or "hostile" (infected?) messages. Maybe this should be more like "In so far as practical, messages MUST NOT be accidentally lost. For example, messages and their processing state should be committed to non-volatile storage until responsibility is taken for that message by the next host in the delivery path." or something like that.

RFC 5321 (2 of 2)

Do Sections 6.1 and 6.2 of 5321bis require clarification and/or rewriting?

Difficulty: slightly more difficult

<https://github.com/ietf-wg-emailcore/emailcore/issues/114>

(Continued)

Donald Eastlake suggested:

6.2 could be trivially fixed by simply replacing "requires that messages that can be delivered should be delivered" with "benefits when messages that can be delivered are delivered". I do note that this "requires" statement does not use a capitalized keyword and is softened by the lower case "should". I did not notice any self-contradiction as egregious as this elsewhere in the document.'

RFC 5321 (1 of 2)

Gateway comments, Section 3.7, and Appendix D

Difficulty: slightly more difficult

<https://github.com/ietf-wg-emailcore/emailcore/issues/119>

John Klensin: In his comments (see last part of <<https://mailarchive.ietf.org/arch/msg/last-call/1qEldmIXiDGhLkFnvEwppEZMfCs>>), Donald Eastlake argues quite strongly that the text of Appendix D should be moved into Section 3.7 or at least that the appendix be referenced from 3.7.

3.7. Mail Gatewaying

3.7.1. Header Fields in Gatewaying

3.7.2. Received Lines in Gatewaying

3.7.3. Addresses in Gatewaying

3.7.4. Other Header Fields in Gatewaying

3.7.5. Envelopes in Gatewaying

Appendix D. Other Gateway Issues

RFC 5321 (2 of 2)

Gateway comments, Section 3.7, and Appendix D

Difficulty: slightly more difficult

<https://github.com/ietf-wg-emailcore/emailcore/issues/119>

(Continued)

Appendix D. Other Gateway Issues

In general, gateways between the Internet and other mail systems SHOULD attempt to preserve any layering semantics across the boundaries between the two mail systems involved. Gateway-translation approaches that attempt to take shortcuts by mapping (such as mapping envelope information from one system to the message header section or body of another) have generally proven to be inadequate in important ways. Systems translating between environments that do not support both envelopes and a header section and Internet mail must be written with the understanding that some information loss is almost inevitable.

Alexey: suggestion to move Appendix D as 3.7.6. If we want to keep Appendix D, add a reference to 3.7 there. Also note the move in the change log.

RFC 5321 (1 of 2)

An IANA registry for SMTP reply codes?

Difficulty: slightly more difficult

<https://github.com/ietf-wg-emailcore/emailcore/issues/118>

John Klensin: In his review, Donald Eastlake strongly suggested that, instead of the explanation in Section 4.2, we create an IANA registry for SMTP reply codes. He said, more or less, that the material in that section essentially defines allocation requirements and is therefore improper.

His message at <<https://mailarchive.ietf.org/arch/msg/last-call/1qEldmIXiDGhLkFnvEwppEZMfCs>> contains proposed XML for that registry (among other suggestions).

RFC 5321 (2 of 2)

An IANA registry for SMTP reply codes?

Difficulty: slightly more difficult

<https://github.com/ietf-wg-emailcore/emailcore/issues/118>

(Continued)

John Klensin: As I understand it, we have decided that we don't want any more codes, preferring that people invent new Enhanced Status Codes and use them with the existing base codes. If circumstances arise that require new codes, it should be a big deal, presumably including an update to 5321bis. If we decide to agree with Donald, then in addition to checking and updating his XML (at least one error/ issue is obvious), we need to create a new subsection of Section 7 on IANA considerations and figure out what should be moved there from Section 4.2. We might conceivably also want to add some additional explicit requirements or recommendations for the relevant Standards Track documents (expert review + standards action?).

Suggestion: **do nothing. Can always be done in a separate (future) document. When lack of the Enhanced Status Codes registry became an issue this is exactly what this community did.**

RFC 5321

IANA instructions about sub-registries created by MT-PRIORITY extension need to be clarified

Difficulty: slightly more difficult

<https://github.com/ietf-wg-emailcore/emailcore/issues/103>

John Klensin: Following paragraph requires input from Alexey, revised text, and WG signoff on the result.

Another subregistry question arises with the MT-PRIORITY extension. The authors of RFC 6710 (one of whom is obviously quite handy) should review how that extension is handled, including whether the use of "MT-PRIORITY" in some places as "PRIORITY" in others is confusing. At present, it is listed as a Service Extension, in the Extension Parameters list, and with its own separate registry in the Mail Parameters registry group [60] [57]. At least that registry should be shown as a sub-subregistry of the Service Extensions Registry and/or carefully cross-referenced.

Alexey: I think the only change needed is to rename "SMTP PRIORITY extension Priority Assignment Policy" sub-registry to "SMTP MT-PRIORITY extension Priority Assignment Policy". I also suggest removing this text from the document and handle it directly with IESG/IANA (via a Management Item).

RFC 5321

Inconsistent terminology in Section 4.5.3.2

Difficulty: slightly more difficult

<https://github.com/ietf-wg-emailcore/emailcore/issues/100>

Donald Eastlake wrote: Section 4.5.3.2: It seems confusing that the first paragraph talks about "each buffer of the data transfer" but there is only one mail data buffer at the server for a particular mail message and the subject of 4.5.3.2.5 uses "block" while contents of 4.5.3.2.5 uses "chunk" and "TCP SEND call"s.

Default suggestion "no change", unless somebody wants to volunteer to review the section and suggest some changes?