

EMAILCORE WG

Online San Francisco 2021

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)

Administrivia

- This Meetecho session is being recorded
- Meetecho:
 - <https://meetings.conf.meetecho.com/ietf111/?group=emailcore&short=&item=1>
- Jabber room (discussions/back channel):
 - emailcore@jabber.ietf.org
- Shared note taking:
 - <https://codimd.ietf.org/notes-ietf-111-emailcore>
- Note taker?

Agenda

- Agenda bashing, administrivia, note well (chairs) - 5 mins
- #7 (Better definition for trace header fields) - both 5321bis and 5322bis are affected <<https://trac.ietf.org/trac/emailcore/ticket/7>>
- #20 (G.7.13. Possible SEND, SAML, SOML Loose End) <<https://trac.ietf.org/trac/emailcore/ticket/20>>
- #14 (G.7.8. Review different size limits) <<https://trac.ietf.org/trac/emailcore/ticket/14>>
- #42 (G.12. Extension Keywords Starting in 'X-') <<https://trac.ietf.org/trac/emailcore/ticket/42>>
- #30 (Erratum 4055: Description of SPF and DKIM is wrong) <<https://trac.ietf.org/trac/emailcore/ticket/30>>
- #19 (G.7.6. Requirements for domain name and/or IP address in EHLO) 5321bis EHLO argument requirements (domain name, domain name validity, IP address) <<https://trac.ietf.org/trac/emailcore/ticket/19>>
 - Note interaction with #1 (G.1. IP address literals in EHLO) and #9 (G.7.3. Definition of domain name in Section 2.3.5))
- #50 (Use of top level domains in SMTP) <<https://trac.ietf.org/trac/emailcore/ticket/50>>

RFC 5322/5321

Better definition for trace header fields
- problem statement

<https://trac.ietf.org/trac/emailcore/ticket/7>

- Various documents define trace header fields which can be added during SMTP relay and/or final delivery. RFC 5322 defines ABNF (and list 2 header fields) in Section 3.6.7 ("Trace Fields"). Other RFCs added other trace header fields, e.g. Authentication-Results (RFC 7601) and more esoteric SIO-Label-History (RFC 7444).
- Also, neither RFC 8098 nor RFC 3461 say that Original-Recipient is a trace header field.

RFC 5322

Better definition for trace header fields (1 of 3)

<https://trac.ietf.org/trac/emailcore/ticket/7>

•Syntax currently in 3.6.7:

.trace = [return]
• 1*received

•Proposal on list:

.trace = [return]
• 1*(received / optional-field)

•Possible (but not pretty) suggestion, if “lone Return-Path” is to be allowed:

.trace = return /
• ([return]
• 1*(received / optional-field))

RFC 5322

Better definition for trace header fields (2 of 3)

<https://trac.ietf.org/trac/emailcore/ticket/7>

•Proposed rfc5322bis Section 3.6.7 text regarding syntax seems OK **except for “lone Return-Path:”**

•OLD:

•The trace fields are a group of header fields consisting of an optional "Return-Path:" field, and one or more "Received:" fields. The "Return-Path:" header field contains a pair of angle brackets that enclose an optional addr-spec. The "Received:" field contains a (possibly empty) list of tokens followed by a semicolon and a date- time specification. Each token must be a word, angle-addr, addr- spec, or a domain. Further restrictions are applied to the syntax of the trace fields by specifications that provide for their use, such as [I-D.klensin-rfc5321bis].

•NEW:

•The trace fields are a group of header fields consisting of an optional "Return-Path:" field, and one or more "Received:" fields or other fields (indicated by "optional-field" below) that are defined by other specifications as belonging within the trace fields grouping. The "Return-Path:"...

RFC 5322

Better definition for trace header fields (3 of 3)

<https://trac.ietf.org/trac/emailcore/ticket/7>

•Syntax currently in 3.6:

```
•fields      = *(trace
•              *optional-field /
•              *(resent-date /
•              resent-from /
•              [...other resent-*]
•              resent-msg-id))
•              *(orig-date /
•              from /
•              sender /
• [truncated for brevity]
```

RFC 5321

Better definition for trace header fields

<https://trac.ietf.org/trac/emailcore/ticket/7>

Strawman proposal for changes to rfc5321bis (part 1):

Add a new section that introduces Trace header fields. Possibly change 4.4 to be that section and move definition of the Received header field into a subsection of 4.4 (e.g. 4.4.1). I found the following text in RFC 822, which seems like a good definition:

Trace information is used to provide an audit trail of message handling. In addition, it indicates a route back to the sender of the message.

2.3.10. Originator, Delivery, Relay, and Gateway Systems

A "relay" SMTP

system (usually referred to just as a "relay") receives mail from an SMTP client and transmits it, without modification to the message data other than adding trace information, to another SMTP server for further relaying or for delivery.

Add a reference to the new 4.4. after "trace information".

RFC 5321

Better definition for trace header fields

<https://trac.ietf.org/trac/emailcore/ticket/7>

Strawman proposal for changes to rfc5321bis (part 2):

3.6.3. Message Submission Servers as Relays

As discussed in Section 6.4, a relay SMTP has no need to inspect or act upon the header section or body of the message data and **MUST NOT** do so except to add its own "Received:" header field (Section 4.4)

Add "**and possibly other trace header fields**" at the end of the above line.

and, optionally, to attempt to detect looping in the mail system (see Section 6.3).

7.6. Information Disclosure in Trace Fields

In some circumstances, such as when mail originates from within a LAN whose hosts are not directly on the public Internet, trace ("**Received**") header fields produced in conformance with this

Change '("Received")' to '(**e.g. "Received"**)'

specification may disclose host names and similar information that would not normally be available.

RFC 5321

G.7.13. Possible SEND, SAML, SOML Loose End

<https://trac.ietf.org/trac/emailcore/ticket/20>

Ned Freed wrote:

Clients SHOULD NOT provide SEND, SAML, or SOML as services. **Servers MAY implement them. If they are implemented by servers,** the implementation model specified in RFC 821 MUST be used and the command names MUST be published in the response to the EHLO command.

This last paragraph omits the possibility of them being implemented but not enabled. I also don't see any point to saying that servers MAY implement them. How about:

Clients SHOULD NOT provide SEND, SAML, or SOML as services. **If a server implements them,** the implementation model specified in RFC 821 MUST be used and **the names of any commands that are enabled** MUST be published in the response to the EHLO command.

Alessandro's version (with a small tweak from Alexey) to replace the first sentence of the new text:

Clients SHOULD NOT **use** SEND, SAML, or SOML **commands**.

RFC 5321

G.7.8. Review different size limits

<https://trac.ietf.org/trac/emailcore/ticket/14>

4.5.3.1.1. Local-part: **<=64** octets

4.5.3.1.2. Domain: **<=255** octets

4.5.3.1.3. Path: **<=256** octets (including the punctuation and element separators).

4.5.3.1.4. Command Line: **<=512** octets (including the command name and CRLF), unless extended by an extension.

4.5.3.1.5. Reply Line: **<=512** octets (including reply code and CRLF). Multiline responses extend that.

4.5.3.1.6. Text Line: **<=1000** octets (including CRLF)

4.5.3.1.7. Message Content: **>= 64Kb**

4.5.3.1.8. Recipient Buffer: **>=100** recipients

Given the controversy on the SMTP mailing list between 20191123 and now about maximum lengths, is the above adequate or is further tuning of the limit text below needed?

Also:

G.7.19. Minimum Lengths and Quantities

Are the minimum lengths and quantities specified in Section 4.5.3 still appropriate or do they need adjusting? (See CREF at the beginning of that section.) Also note potential interaction with the proposed LIMITS SMTP extension ([draft-freed-smtp-limits](#)) which may make this question OBE.

RFC 5321

G.12. Extension Keywords Starting in 'X'

<https://trac.ietf.org/trac/emailcore/ticket/42>

General feeling on the mailing list that any restrictions on extensions that start with 'X' should be removed.

Strawman proposal:

Change #1:

2nd paragraph of Section 8 ("IANA Considerations"):

OLD:

- o The first, "Simple Mail Transfer Protocol (SMTP) Service Extensions" [49], consists of SMTP service extensions with the associated keywords, and, as needed, parameters and verbs. ~~As specified in Section 2.2.2, no entry may be made in this registry that starts in an "X".~~ Entries may be made only for service extensions (and associated keywords, parameters, or verbs) that are defined in Standards-Track or Experimental RFCs specifically approved by the IESG for this purpose.

NEW:

- o The first, "Simple Mail Transfer Protocol (SMTP) Service Extensions" [49], consists of SMTP service extensions with the associated keywords, and, as needed, parameters and verbs. Entries may be made only for service extensions (and associated keywords, parameters, or verbs) that are defined in Standards-Track or Experimental RFCs specifically approved by the IESG for this purpose.

RFC 5321

G.12. Extension Keywords Starting in 'X'

<https://trac.ietf.org/trac/emailcore/ticket/42>

Change #2:

OLD:

4.1.5. Private-Use Commands

As specified in Section 2.2.2, commands starting in "X" may be used by bilateral agreement between the client (sending) and server (receiving) SMTP agents. An SMTP server that does not recognize such a command is expected to reply with "500 Command not recognized". An extended SMTP server MAY list the feature names associated with these private commands in the response to the EHLO command.

Commands sent or accepted by SMTP systems that do not start with "X" MUST conform to the requirements of Section 2.2.2.

NEW - drop the whole section?

RFC 5321

G.12. Extension Keywords Starting in 'X'

<https://trac.ietf.org/trac/emailcore/ticket/42>

Change #3:

Last 2 paragraphs of Section 2.2.2 ("Definition and Registration of Extensions"):

OLD:

~~In addition, any EHLO keyword value starting with an upper or lower case "X" refers to a local SMTP service extension used exclusively through bilateral agreement. Keywords beginning with "X" MUST NOT be used in a registered service extension. Conversely, keyword values presented in the EHLO response that do not begin with "X" MUST correspond to a Standard, Standards-Track, or IESG-approved Experimental SMTP service extension registered with IANA. A conforming server MUST NOT offer non-"X" prefixed keyword values that are not described in a registered extension.~~

~~Additional verbs and parameter names are bound by the same rules as EHLO keywords; specifically, verbs beginning with "X" are local extensions that may not be registered or standardized. Conversely, verbs not beginning with "X" must always be registered.~~

NEW:

Keyword values presented in the EHLO response **SHOULD** correspond to a IESG approved Standards-Track or Experimental SMTP service extension registered with IANA.

(Note that I changed original MUST to SHOULD, taking into consideration that none of "X" extensions would be registered with IANA.)

Should extensions like **XCLIENT** be registerable in **IESG approved Informational RFCs**?

RFC 5321

Erratum 4055: Description of SPF and DKIM is wrong

<https://trac.ietf.org/trac/emailcore/ticket/30>

Last paragraph of section 3.6.2 in RFC 5321 reads:

This specification does not deal with the verification of return paths for use in delivery notifications. Recent work, such as that on SPF [29] and DKIM [30] [31], has been done to provide ways to ascertain that an address is valid or belongs to the person who actually sent the message. A server MAY attempt to verify the return path before using its address for delivery notifications, but methods of doing so are not defined here nor is any particular method recommended at this time.

Ticket recommends removing bits about SPF and DKIM.

List discussion has landed on the following as a suggestion:

This specification does not deal with the verification of a return path for use in delivery notifications. Verification of the return path is outside the scope of this specification.

Questions:

Is the proposed text acceptable?

Should “for use in delivery notifications” be kept or stricken?

RFC 5321 & A/S

G.7.6. Requirements for domain name and/or IP address in EHLO

<https://trac.ietf.org/trac/emailcore/ticket/19>

Current text in RFC 5321, section 4.1.4, Order of Commands, includes this paragraph:

An SMTP server MAY verify that the domain name argument in the EHLO command actually corresponds to the IP address of the client. However, if the verification fails, the server MUST NOT refuse to accept a message on that basis. Information captured in the verification attempt is for logging and tracing purposes. Note that this prohibition applies to the matching of the parameter to its IP address only; see Section 7.9 for a more extensive discussion of rejecting incoming connections or mail messages.

Proposal to strike the entire paragraph and replace it with:

An SMTP server MAY verify that the domain name argument in the EHLO command has an address record matching the IP address of the client.

Further proposal to add text similar to the following the Applicability Statement:

If the domain name argument in 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 tells us that some types of abusive hosts forge or otherwise fake an EHLO value, and so SMTP operators may choose to refuse traffic based on the EHLO value mismatch.

A/S

Use of top level domains in SMTP

<https://trac.ietf.org/trac/emailcore/ticket/50>

Use of top level domains where FQDN are expected is not necessarily interoperable. See [RFC 7085](#).

Should something be said about this in A/S?

Extra slides, if needed

Suggested scope for the “Core Email Applicability Statement”

- Best practices on use of SMTP, email format/MIME.
- Don't touch POP/IMAP/JMAP or Sieve
 - They IMAP/Sieve and JMAP have their own WGs (EXTRA and JMAP respectively)
- Don't touch SMTP Submission (RFC 6409) this time around
- Reference DMARC/DKIM/SPF?
 - Note that DMARC has its own WG, so not doing any work here