EMAILCORE WG
March 2023 Interim

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/interim/?short=ee23ecd5-4be3-4309-93cc-cf2ce800f83a
- Shared note taking:
    - https://notes.ietf.org/notes-ietf-interim-2023-emailcore-01-emailcore
- In room participants: please use masks
- ***Note taker***?

Agenda (1 of 3)

- Agenda bashing, administrivia, note well (chairs) - 5 mins

- Tickets for the Message Format and SMTP drafts related to Trace Header Fields:
- #74 Syntax of Received header field need to be clarified ***https://github.com/ietf-wg-emailcore/emailcore/issues/74***
- Should rfc5322bis "generate" grammar allow for non trace header fields between trace and resent block ***https://github.com/ietf-wg-emailcore/emailcore/issues/83***

- #81 IANA registration procedure for Trace Header Fields? ***https://github.com/ietf-wg-emailcore/emailcore/issues/81***

Agenda (2 of 3)

- Tickets for the SMTP draft:

- #75 G.21. Appendix B and Message Submission ***https://github.com/ietf-wg-emailcore/emailcore/issues/75***
- #82 G.24. Describing the "Operational Requirements" Loopholes ***https://github.com/ietf-wg-emailcore/emailcore/issues/82***

Agenda (3 of 3)

- Tickets for the A/S draft:
- #84 Add text about handling of Trace Header Fields by MUAs ***https://github.com/ietf-wg-emailcore/emailcore/issues/84***
- #85 Add text to A/S about what mail agents should do/not do with Received header fields ***https://github.com/ietf-wg-emailcore/emailcore/issues/85***
- #86 Expand on operational meaning of being a trace header field ***https://github.com/ietf-wg-emailcore/emailcore/issues/86***
- #80 G.6. Clarify where the protocol stands with respect to submission and TLS issues ***https://github.com/ietf-wg-emailcore/emailcore/issues/80***

RFC 5322/5321

Better definition for trace header fields - problem statement

https://github.com/ietf-wg-emailcore/emailcore/issues/7

- Various documents define trace header fields which can be added during SMTP submission, 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 5322/5321

Syntax of Received header field need to be clarified

https://github.com/ietf-wg-emailcore/emailcore/issues/74

Need to clarify relationship between Received header field syntax in rfc5322bis and rfc5321bis. Current rfc5322bis text:

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.ietf-emailcore-rfc5321bis].

Suggested addition to the end of the last sentence to clarify:

... defining more specific syntax of the Received header field as used by SMTP.

RFC 5322/5321

Should rfc5322bis "generate" grammar allow for non trace header fields between trace and resent block

https://github.com/ietf-wg-emailcore/emailcore/issues/83

- Syntax in section 3.6 of rfc5322bis-04:

- fields = *(trace
- *__optional-field__ /
- *(resent-date /
- resent-from /
- *[...other resent-*]*
- resent-msg-id))
- *(orig-date /
- from /
- sender /
- [truncated for brevity]

Confirm removal of the top optional-field.

RFC 5321/5322

IANA registration procedure for Trace Header Fields?

https://github.com/ietf-wg-emailcore/emailcore/issues/81

The proposal on the table is to extend **Message Header Field Names** registry with an extra field that includes trace header field information. Possibly just a boolean field ("is trace"?)

Which document should include the IANA registration?

- rfc5322bis?
- A/S
- rfc5321bis

Suggestion to add this to rfc5322bis or A/S, as Trace Header Fields are not SMTP specific.

RFC 5321

G.21. Appendix B and Message Submission

https://github.com/ietf-wg-emailcore/emailcore/issues/75

- John Klensin wrote:

  Appendix B ("Generating SMTP Commands from Internet Message Format Header Fields") was written long ago and does not distinguish very carefully from the case where an MSA is involved from direct MUA-MTA communications. On the other hand, the situation it describes cannot arise with a conforming message submission system. Should it be rewritten and, if so, how much?

Proposal: no change, the current text is Ok as is. It also includes suggestions about BCC handling when generating SMTP transactions from the message header section

RFC 5321

G.24. Describing the "Operational Requirements" Loopholes

https://github.com/ietf-wg-emailcore/emailcore/issues/82

- John Klensin wrote:

The discussion in Section 7.8 ('Local Operational Requirements and Resistance to Attacks') and Section 7.9 ('Scope of Operation of SMTP Servers'), and the pointers to them from Section 6.2 ('Unwanted, Unsolicited, and "Attack" Messages') and elsewhere essentially provide the basis for implementations to deviate, in multiple ways, from the intent of RFC 5321 and 5321bis while claiming conformance. Is the present text what we want? Should it be made more explicit about what is allowed and what isn't (whether either is possible is obviously part of the question)? If we intend to address those issues in the A/S (not just the limits question which is already there), do we want explicit forward pointers to it in the existing sections?

Proposal: no change, the current text is Ok as is?

A/S

Add text to A/S about what mail agents should do/not do with Received header fields

https://github.com/ietf-wg-emailcore/emailcore/issues/85

Suggested addition:

> "Received header fields are not normally useful to the end user, becoming useful only when there are delivery problems with a message or when the message itself is problematic or suspicious for some reason. Their content is also fairly easy to fake should someone desire to do that. Therefore, if anyone or anything receiving a message pays attention to such fields that it did not insert (or otherwise have reason to trust), they should be used with care, whatever information seems to be valuable used as appropriate, but with no assumptions of trust especially when syntax or values occur that are not defined by the specifications [rfc5321bis] [rfc5322bis]."

A/S

Add text about handling of Trace Header Fields by MUAs

https://github.com/ietf-wg-emailcore/emailcore/issues/84

Suggested addition:

> A MUA that uses an existing email message
> as a template for editing with the intention of
> sending it to new set of recipients (this is
> sometimes implemented as "edit as a new message"
> feature) SHOULD strip trace header fields.

A/S

Expand on operational meaning of being a trace header field

https://github.com/ietf-wg-emailcore/emailcore/issues/86

Pete Resnick wrote:

Right now, being a trace field is syntactically to be part of the Return-Path/Received block, and semantically means to be information about this messages movement through the system from submission to delivery. But what is the operational meaning? Is the only operational implication of being a trace field that you delete it in certain circumstances (like edit-as-new, mailing list distribution, etc.), or does it mean something more than that?

If it only means "delete on MUA resend" (or some variant of that), then the registry should probably be labeled that instead of "trace". If it means something more than that, then the A/S should probably have a much richer discussion than text suggested for ticket #84.

A/S

G.6. Clarify where the protocol stands with respect to submission and TLS issues

https://github.com/ietf-wg-emailcore/emailcore/issues/80

1. submission on port 587
2. submission on port 465
3. TLS relay on a port different from 25 (whenever)
4. Recommendations about general use of transport layer (hop by hop) security, particularly encryption including consideration of RFC 8314.

The MTA-to-MTA relay case is already covered by the now closed ticket #54 ("Hop-by-hop Authentication and/or Encryption"), in particular it mentions MTA-STS [RFC8461] and DANE for SMTP [RFC7672].

Section 6.1 has text about TLS protecting messages in transit, but not in storage. So it wouldn’t help against a compromised server. (Might need to clarify the last point)

Do we need to say anything about submission and RFC 8314 ("Cleartext Considered Obsolete: Use of Transport Layer Security (TLS) for Email Submission and Access")?