EMAILCORE WG

IETF 122 – March 2025

A/S Status

Editors:
John Klensin <john-ietf@jck.com>
Ken Murchison <murch@fastmail.com

Resolved and Closed since IETF 121

- #40 – Recommended SMTP Extensions
- #78 – Advice against using URL %-encoding on non ASCII email addresses to create ASCII version of them
- #79 – Add Internationalization Considerations section
- #84 – Add text about handling of Trace Header Fields by MUAs
- #85 – Add text to A/S about what mail agents should do/not do with Received header fields

Resolved and Closed since IETF 121

- #93 – “7.3 VRFY, EXPN, and Security” should point to SMTP AUTH RFC

- #96 – Popular misuse of multipart/alternative relative to its original purpose

- #112 – Expand the comment in the 5321bis introduction about the A/S to contain more detail?

- #127 – STARTTLS needs a reference to RFC 3207

Changes since IETF 121

#94 – Use of Quoted Strings:

In particular, use of empty quoted strings is discouraged in "received-token" (a component of a Received header field) and ~~"keywords" (a component of a Keywords header field)~~ "local-part" (left hand side of email addresses). For example, all of the following email header fields are non-interoperable:

Received: from node.example by x.y.test "" foo; 21 Nov 1997 10:01:22 -0600

~~Keywords: foo, "", bar~~

From: "".bar@example.com

To: foo.""@example.net"

Cc: "@example.com

Use of empty quoted strings is fine in "display-name". For example, the following email header field is interoperable:

To: "" <test@example.com>

Changes since IETF 121

#110 – References to DKIM, etc:
#132 – Mention that OpenPGP and S/MIME can be used for providing message authenticity, not just confidentiality
#133 – Mention that draft-ietf-lamps-header-protection as providing header authenticity and confidentiality with OpenPGP & S/MIME

Existing text:

6.4. 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.

Changes since IETF 121

#110, #132, #133

New text:

6.4. Message-Level Authentication

Protocols exist to allow for authentication of different identities associated with an email message:

- SPF [RFC7208] provides a method to ensure that the sending mail server is authorized to originate mail from the sender's domain.
- DKIM [RFC6376] provides a method to detect forged sender addresses in an email (spoofing).
- DMARC [RFC7489] relies on SPF and DKIM to allow for validation of the domain in the visible From header.

Changes since IETF 121

#110, #132, #133

New text cont'd:

- ARC [RFC8617] provides a method for each hop to record results of authentication checks performed at that hop.

- S/MIME [RFC8551] and OpenPGP [RFC9580], along with Header Protection for Cryptographically Protected E-mail [I-D.ietf-lamps-header-protection], allow for emails to be digitally signed, thereby providing a method to verify that an email was actually sent by the entity claiming to be the sender.

Changes since IETF 121

Per interim-2025-emailcore-02:

3.2. Use of Received Header Fields

3.2.1. Generation

Email addresses are commonly classified as Personally Identifiable Information (PII). Improper application of the FOR clause in Received header fields can result in disclosure of PII. As such, the FOR clause ~~MUST~~ SHOULD NOT be generated if the message copy is associated with multiple recipients from multiple SMTP RCPT commands.

Other Open Issues

- #92 – CNAME handling in “5.1. Locating the Target Host”

  Per IETF 120, John Klensin to propose text.

Other Open Issues

- #113 – More explanation of the advantages of transport and encryption between SMTP systems

Pete's suggested changes:

6.2 ~~Optional~~ Opportunistic Confidentiality

6.3 ~~Required~~ Enforced Confidentiality, with Receiving Server Authentication

And change all instances of "optional" to "opportunistic" and "required" to "enforced"

Other Open Issues

- #113 – More explanation of the advantages of transport and encryption between SMTP systems

Pete's suggested addition:

6.7 Confidentiality Requirements

The vast majority of email sent on the Internet at present does not use message-level confidentiality. It has been recognized that Internet traffic is exposed to both active attack and passive monitoring (see [BCP61], [BCP200]), and therefore that message transmission over SMTP is subject to both. To mitigate these risks, opportunistic TLS is now widely implemented and used in Internet email, and some deployment and use of MTA-STS and DANE for SMTP are also now seen. Therefore, the STARTTLS extension MUST be implemented by SMTP servers in order to allow users to maintain as much confidentiality as possible. That said, there are many legacy implementations of SMTP that are still in widespread use in both private and Internet-connected networks that do not implement STARTTLS and will not be updated to do so, and most receiving server implementations will be expected to be capable of receiving such messages. Therefore, SMTP servers MUST be configurable to allow for the STARTTLS extension not to be used in order to maximize interoperation.

Other Open Issues

- #134 – clarify that MTA-STS fixes an active attack in STARTTLS

Rob Sayre says:

The document should state that MTA-STS [RFC8461] addresses a fairly serious vulnerability in STARTTLS [RFC3207], where an active attacker can downgrade or intercept the SMTP session (a brief version of the introduction in RFC8461). This problem is noted in RFC3207, but the document should mention that MTA-STS addresses it.

Other Open Issues

- #135 – confidentiality and authentication

Rob Sayre says:

The document says "Opportunistic TLS is confidentiality without authentication". I'm a little confused here. Shouldn't it always at least authenticate the server if the TLS handshake works? Maybe I'm just misreading this part.
Maybe it has some different kind of "authentication" in mind? It's confusing, because the introduction to TLS 1.3 says TLS provides Authentication, Confidentiality, and Integrity.