EMAILCORE WG

IETF 123 – July 2025

A/S Status

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

Resolved and Closed since IETF 122

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

Changes since IETF 122

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

Sections 6.2, 6.3:

- Changed all instances of “optional confidentiality” to “opportunistic confidentiality”
- Changed all instances of “required confidentiality” to “enforced confidentiality”

Changes since IETF 122

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

Added the following:

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 [RFC3365], BCP200 [RFC1984]), and therefore that message transmission over SMTP is subject to both. To mitigate these risks, opportunistic confidentiality is now widely implemented and used in Internet email, and some deployment and use of enforced confidentiality is also now seen. Therefore, confidentiality (for example, the STARTTLS extension) MUST be implemented by SMTP servers in order to at least provide over-the-wire confidentiality during an individual SMTP exchange. That said, there are many legacy implementations of SMTP that are still in widespread use in both private and Internet-connected networks, and most receiving servers implementations will be expected to be capable of receiving such messages. Therefore, SMTP servers MUST be configurable to allow for receiving messages without confidentiality between servers in order to maximize interoperation.

Changes since IETF 122

#138 – Description of DKIM:

Old text:

DKIM [RFC6376] provides a method to detect forged sender addresses in an email (spoofing).

New text:

DKIM [RFC6376] permits a person, role, or organization to claim some responsibility for an email message by associating a domain name [RFC1034] with the message, which they are authorized to use.

Changes since IETF 122

Clarification of hop-by-hop vs end-to-end confidentiality:

Additional text in “6.2 Opportunistic Confidentiality”:

Note that 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! Also, in a situation where a message traverses multiple hops through multiple SMTP servers, each intermediate server will have access to the plain text of the message. The only way to completely assure confidentiality so that no one server has access to the contents of a message is to use message-level confidentiality as described in Section 6.4.

Changes since IETF 122

Clarification of hop-by-hop vs end-to-end confidentiality:

Additional text in “6.3 Enforced Confidentiality”:

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.

However, as noted in Section 6.2, both SMTP servers will most likely have access to the plain text of the message, as will all SMTP servers where multiple hops are involved. Again, only message-level confidentiality described in Section 6.4 will prevent that lack of confidentiality.

Open Issues

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

  Per IETF 120, John Klensin to propose text.

Open Issues

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

Proposed new text at end of “6.2 Opportunistic Confidentiality”:

Note that opportunistic TLS via the STARTTLS [RFC3207] extension is vulnerable to man-in-the-middle attacks. Enforced confidentiality (Section 6.3) can be used to mitigate these attacks.

Open Issues

- #135 – Confidentiality and authentication

Rob Sayre's suggested edit:

Opportunistic TLS is ~~confidentiality without authentication, because no effort is made to authenticate the receiving server, and it is opportunistic~~ optional confidentiality due to the ability to fall back to transmission in the clear if a secure connection cannot be established.
Opportunistic TLS is often configured to provide confidentiality without authentication, where no effort is made to authenticate the receiving server [RFC 3207, Section 4.1].
~~That said, m~~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.

Open Issues

- #137 – Recommended email address syntax for web forms

Existing text:

Email addresses are frequently used as input in HyperText Markup Language (HTML) forms but the allowed grammar of these email addresses is more restrictive than the grammar for a 'Mailbox' in Section 4.1.2 of [I-D.ietf-emailcore-rfc5321bis] (the lack of quoted strings and limited characters allowed in domains). As of the time this document was written, non-ASCII characters (as discussed in Section 4.2 above) were also not permitted. Implementations that intend to accept email addresses in HTML forms are encouraged to consult the valid email address grammar in Section 4.10.5.1.5 of [HTML].

Additionally, the following general guidance is provided:

- Few mail systems allow leading, trailing, or consecutive unquoted dots ('.') in the local-part of email addresses even though the HTML grammar referenced above currently allows them. Consequently, implementations are discouraged from accepting such addresses.

Open Issues

- #137 – Recommended email address syntax for web forms

Proposed new text:

Email addresses are frequently used as input in HyperText Markup Language (HTML) forms but the allowed grammar of these email addresses (see Section 4.10.5.1.5 of [HTML]) is not compatible with the grammar for a 'Mailbox' in Section 4.1.2 of [I-D.ietf-emailcore-rfc5321bis]. Specifically, the HTML form grammar:

- Does not supported quoted strings.
- Only allows a limited set of characters in domains.
- Allows leading, trailing, or consecutive unquoted dots ('.') in the local-part of email addresses.
- As of the time this document was written, non-ASCII characters (as discussed in Section 4.2 above) were also not permitted.

Consequently, implementations that intend to accept email addresses in HTML forms are encouraged to allow at least the following, more restricted 'Mailbox' grammar:

Limited-Mailbox = Dot-string "@" Domain

Additionally, the following general guidance is provided:

- Implementations are discouraged from accepting addresses having leading, trailing, or consecutive unquoted dots ('.') in the local-part, as few mail systems support them.