SMTP Require TLS Option
draft-ietf-uta-smtp-require-tls-09

Abstract

   The SMTP STARTTLS option, used in negotiating transport-level
   encryption of SMTP connections, is not as useful from a security
   standpoint as it might be because of its opportunistic nature;
   message delivery is, by default, prioritized over security. This
   document describes an SMTP service extension, REQUIRETLS, and message
   header field, TLS-Required. If the REQUIRETLS option or TLS-Required
   message header field is used when sending a message, it asserts a
   request on the part of the message sender to override the default
   negotiation of TLS, either by requiring that TLS be negotiated when
   the message is relayed, or by requesting that recipient-side policy
   mechanisms such as MTA-STS and DANE be ignored when relaying a
   message for which security is unimportant.

Status of This Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF). Note that other groups may also distribute
   working documents as Internet-Drafts. The list of current Internet-
   Drafts is at https://datatracker.ietf.org/drafts/current/.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time. It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   This Internet-Draft will expire on February 3, 2020.

Copyright Notice

Table of Contents

1. Introduction

   The SMTP [RFC5321] STARTTLS service extension [RFC3207] provides a
   means by which an SMTP server and client can establish a Transport
   Layer Security (TLS) protected session for the transmission of email
   messages. By default, TLS is used only upon mutual agreement
   (successful negotiation) of STARTTLS between the client and server;
   if this is not possible, the message is sent without transport
   encryption. Furthermore, it is common practice for the client to
   negotiate TLS even if the SMTP server's certificate is invalid.

   Policy mechanisms such as DANE [RFC7672] and MTA-STS [RFC8461] may
   impose requirements for the use of TLS for email destined for some
   domains. However, such policies do not allow the sender to specify
   which messages are more sensitive and require transport-level
   encryption, and which ones are less sensitive and ought to be relayed
   even if TLS cannot be negotiated successfully.

   The default opportunistic nature of SMTP TLS enables several "on the
   wire" attacks on SMTP security between MTAs. These include passive
   eavesdropping on connections for which TLS is not used, interference
   in the SMTP protocol to prevent TLS from being negotiated (presumably
   accompanied by eavesdropping), and insertion of a man-in-the-middle
   attacker exploiting the lack of server authentication by the client.
   Attacks are described in more detail in the Security Considerations
   section of this document.

   REQUIRETLS consists of two mechanisms: an SMTP service extension and
   a message header field. The service extension is used to specify
   that a given message sent during a particular session MUST be sent
   over a TLS-protected session with specified security characteristics.
   It also requires that the SMTP server advertise that it supports
   REQUIRETLS, in effect promising that it will honor the requirement to
   enforce TLS transmission and REQUIRETLS support for onward
   transmission of those messages.

   The TLS-Required message header field is used to convey a request to
   ignore recipient-side policy mechanisms such as MTA-STS and DANE,
   thereby prioritizing delivery over ability to negotiate TLS. Unlike
   the service extension, the TLS-Required header field allows the
   message to transit through one or more MTAs that do not support
   REQUIRETLS.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and
"OPTIONAL" in this document are to be interpreted as described in BCP
14 [RFC2119] [RFC8174] when, and only when, they appear in all
capitals, as shown here.

The formal syntax uses the Augmented Backus-Naur Form (ABNF)
[RFC5234] including the core rules defined in Appendix B of that
document.

2. The REQUIRETLS Service Extension

1. The textual name of the extension is "Require TLS".

2. The EHLO keyword value associated with this extension is
    "REQUIRETLS".

3. No additional SMTP verbs are defined by this extension.

4. One optional parameter ("REQUIRETLS") is added to the MAIL FROM
    command by this extension. No value is associated with this
    parameter.

5. The maximum length of a MAIL FROM command line is increased by 11
    octets by the possible addition of a space and the REQUIRETLS
    keyword.

6. One new SMTP status code is defined by this extension to convey
    an error condition resulting from failure of the client to send
    to a server not also supporting the REQUIRETLS extension.

7. The REQUIRETLS extension is valid for message relay [RFC5321],
    submission [RFC6409], and the Local Mail Transfer Protocol (LMTP)
    [RFC2033]

8. The ABNF syntax for the MAIL FROM parameter is as follows:

    requiretls-param = "REQUIRETLS"
                    ; where requiretls-param is an instance of an
                    ; esmtp-param used in Mail-parameters in
                    ; RFC 5321 Section 4.1.2. There is no esmtp-value
                    ; associated with requiretls-param.

In order to specify REQUIRETLS treatment for a given message, the
REQUIRETLS option is specified on the MAIL FROM command when that
message is transmitted. This option MUST only be specified in the

context of an SMTP session meeting the security requirements of
REQUIRETLS:

o The session itself MUST employ TLS transmission.

o If the SMTP server to which the message is being transmitted is
   identified through an MX record lookup, its name MUST be validated
   via a DNSSEC signature on the recipient domain's MX record, or the
   MX hostname MUST be validated by an MTA-STS policy as described in
   Section 4.1 of RFC 8461 [RFC8461]. DNSSEC is defined in RFC 4033
   [RFC4033], RFC 4034 [RFC4034], and RFC 4035 [RFC4035].

o The certificate presented by the SMTP server MUST either verify
   successfully in a trust chain leading to a certificate trusted by
   the SMTP client or it MUST verify successfully using DANE as
   specified in RFC 7672 [RFC7672]. For trust chains, the choice of
   trusted (root) certificates is at the discretion of the SMTP
   client.

o Following the negotiation of STARTTLS, the SMTP server MUST
   advertise in the subsequent EHLO response that it supports
   REQUIRETLS.

3. The TLS-Required Header Field

One new message header field [RFC5322], TLS-Required, is defined by
this specification. It is used for messages for which the originator
requests that recipient TLS policy (including MTA-STS [RFC8461] and
DANE [RFC7672]) be ignored. This might be done, for example, to
report a misconfigured mail server, such as an expired TLS
certificate.

The TLS-Required header field has a single REQUIRED parameter:

o No - The SMTP client SHOULD attempt to send the message regardless
   of its ability to negotiate STARTTLS with the SMTP server,
   ignoring policy-based mechanisms (including MTA-STS and DANE), if
   any, asserted by the recipient domain. Nevertheless, the client
   SHOULD negotiate STARTTLS with the server if available.

More than one instance of the TLS-Required header field MUST NOT
appear in a given message.

The ABNF syntax for the TLS-Required header field is as follows:

```
       requiretls-field = "TLS-Required:" [FWS] "No" CRLF
               ; where requiretls-field in an instance of an
               ; optional-field defined in RFC 5322 Section
               ; 3.6.8.
       FWS = <as defined in RFC 5322>
       CRLF = <as defined in RFC 5322>
```

4. REQUIRETLS Semantics

4.1. REQUIRETLS Receipt Requirements

Upon receipt of the REQUIRETLS option on a MAIL FROM command during
the receipt of a message, an SMTP server MUST tag that message as
needing REQUIRETLS handling.

Upon receipt of a message not specifying the REQUIRETLS option on its
MAIL FROM command but containing the TLS-Required header field in its
message header, an SMTP server implementing this specification MUST
tag that message with the option specified in the TLS-Required header
field. If the REQUIRETLS MAIL FROM parameter is specified, the TLS-
Required header field MUST be ignored but MAY be included in onward
relay of the message.

The manner in which the above tagging takes place is implementation-
dependent. If the message is being locally aliased and redistributed
to multiple addresses, all instances of the message MUST be tagged in
the same manner.

4.2. REQUIRETLS Sender Requirements

4.2.1. Sending with TLS Required

When sending a message tagged as requiring TLS for which the MAIL
FROM return-path is not empty (an empty MAIL FROM return-path
indicating a bounce message), the sending (client) MTA MUST:

1. Look up the SMTP server to which the message is to be sent as
    described in [RFC5321] Section 5.1.

2. If the server lookup is accomplished via the recipient domain's
    MX record (the usual case) and is not accompanied by a valid
    DNSSEC signature, the client MUST also validate the SMTP server
    name using MTA-STS as described in RFC 8461 [RFC8461]
    Section 4.1.

3. Open an SMTP session with the peer SMTP server using the EHLO
    verb.

4. Establish a TLS-protected SMTP session with its peer SMTP server
    and authenticate the server's certificate as specified in
    [RFC6125] or [RFC7672] as applicable. The hostname from the MX
    record lookup (or the domain name in the absence of an MX record
    where an A record is used directly) MUST match the DNS-ID or CN-
    ID of the certificate presented by the server.

5. Ensure that the response to the subsequent EHLO following
    establishment of the TLS protection advertises the REQUIRETLS
    capability.

The SMTP client SHOULD follow the recommendations in [RFC7525] or its
successor with respect to negotiation of the TLS session.

If any of the above steps fail, the client MUST issue a QUIT to the
server and repeat steps 2-5 with each host on the recipient domain's
list of MX hosts in an attempt to find a mail path that meets the
sender's requirements. The client MAY send other, unprotected,
messages to that server if it has any prior to issuing the QUIT. If
there are no more MX hosts, the client MUST NOT transmit the message
to the domain.

Following such a failure, the SMTP client MUST send a non-delivery
notification to the reverse-path of the failed message as described
in section 3.6 of [RFC5321]. The following status codes [RFC5248]
SHOULD be used:

o REQUIRETLS not supported by server: 5.7.YYY REQUIRETLS needed

o Unable to establish TLS-protected SMTP session: 5.7.10 Encryption
   needed

Refer to Section 5 for further requirements regarding non-delivery
messages.

If all REQUIRETLS requirements have been met, transmit the message,
issuing the REQUIRETLS option on the MAIL FROM command with the
required option(s), if any.

4.2.2. Sending with TLS Optional

Messages tagged TLS-Required: No are handled as follows. When
sending such a message, the sending (client) MTA MUST:

o Look up the SMTP server to which the message is to be sent as
   described in [RFC5321] Section 5.1.

o Open an SMTP session with the peer SMTP server using the EHLO
   verb. Attempt to negotiate STARTTLS if possible, and follow any
   policy published by the recipient domain, but do not fail if this
   is unsuccessful.

Some SMTP servers may be configured to require STARTTLS connections
as a matter of policy and not accept messages in the absence of
STARTTLS. A non-delivery notification MUST be returned to the sender
if message relay fails due to an inability to negotiate STARTTLS when
required by the server.

Since messages tagged with TLS-Required: No will sometimes be sent to
SMTP servers not supporting REQUIRETLS, that option will not be
uniformly observed by all SMTP relay hops.

4.3. REQUIRETLS Submission

An MUA or other agent making the initial introduction of a message
has the option to decide whether to require TLS. If TLS is to be
required, it MUST do so by negotiating STARTTLS and REQUIRETLS and
include the REQUIRETLS option on the MAIL FROM command, as is done
for message relay.

When TLS is not to be required, the sender MUST include the TLS-
Required header field in the message. SMTP servers implementing this
specification MUST interpret this header field as described in
Section 4.1.

In either case, the decision whether to specify REQUIRETLS MAY be
done based on a user interface selection or based on a ruleset or
other policy. The manner in which the decision to require TLS is
made is implementation-dependent and is beyond the scope of this
specification.

4.4. Delivery of REQUIRETLS messages

Messages are usually retrieved by end users using protocols other
than SMTP such as IMAP [RFC3501], POP [RFC1939], or web mail systems.
Mail delivery agents supporting the REQUIRETLS SMTP option SHOULD
observe the guidelines in [RFC8314].

5. Non-delivery message handling

Non-delivery ("bounce") messages usually contain important metadata
about the message to which they refer, including the original message
header. They therefore MUST be protected in the same manner as the
original message. All non-delivery messages resulting from messages
with the REQUIRETLS SMTP option, whether resulting from a REQUIRETLS

error or some other, MUST also specify the REQUIRETLS SMTP option
unless redacted as described below.

The path from the origination of an error bounce message back to the
MAIL FROM address may not share the same REQUIRETLS support as the
forward path. Therefore, users requiring TLS are advised to make
sure that they are capable of receiving mail using REQUIRETLS as
well. Otherwise, such non-delivery messages will be lost.

If a REQUIRETLS message is bounced, the server MUST behave as if
RET=HDRS was present as described in [RFC3461]. If both RET=FULL and
REQUIRETLS are present, the RET=FULL MUST be disregarded. The SMTP
client for a REQUIRETLS bounce message uses an empty MAIL FROM
return-path as required by [RFC5321]. When the MAIL FROM return-path
is empty, the REQUIRETLS parameter SHOULD NOT cause a bounce message
to be discarded even if the next-hop relay does not advertise
REQUIRETLS.

Senders of messages requiring TLS are advised to consider the
possibility that bounce messages will be lost as a result of
REQUIRETLS return path failure, and that some information could be
leaked if a bounce message is not able to be transmitted with
REQUIRETLS.

6. Reorigination considerations

In a number of situations, a mediator [RFC5598] originates a new
message as a result of an incoming message. These situations
include, but are not limited to, mailing lists (including
administrative traffic such as message approval requests), Sieve
[RFC5228], "vacation" responders, and other filters to which incoming
messages may be piped. These newly originated messages may
essentially be copies of the incoming message, such as with a
forwarding service or a mailing list expander. In other cases, such
as with a vacation message or a delivery notification, they will be
different but might contain parts of the original message or other
information for which the original message sender wants to influence
the requirement to use TLS transmission.

Mediators that reoriginate messages should apply REQUIRETLS
requirements in incoming messages (both requiring TLS transmission
and requesting that TLS not be required) to the reoriginated messages
to the extent feasible. A limitation to this might be that for a
message requiring TLS, redistribution to multiple addresses while
retaining the TLS requirement could result in the message not being
delivered to some of the intended recipients.

   User-side mediators (such as use of Sieve rules on a user agent)
   typically do not have access to the SMTP details, and therefore may
   not be aware of the REQUIRETLS requirement on a delivered message.
   Recipients that expect sensitive traffic should avoid the use of
   user-side mediators. Alternatively, if operationally feasible (such
   as when forwarding to a specific, known address), they should apply
   REQUIRETLS to all reoriginated messages that do not contain the "TLS-
   Required: No" header field.

7. IANA Considerations

   If published as an RFC, this draft requests the addition of the
   following keyword to the SMTP Service Extensions Registry
   [MailParams]:

   Textual name: Require TLS
   EHLO keyword value: REQUIRETLS
   Syntax and parameters: (no parameters)
   Additional SMTP verbs: none
   MAIL and RCPT parameters: REQUIRETLS parameter on MAIL
   Behavior: Use of the REQUIRETLS parameter on the
                               MAIL verb causes that message to require
                               the use of TLS and tagging with
                               REQUIRETLS for all onward relay.
   Command length increment: 11 characters

   If published as an RFC, this draft requests the addition of an entry
   to the Simple Mail Transfer Protocol (SMTP) Enhanced Status Codes
   Registry [SMTPStatusCodes]:

   Code: 5.7.YYY
   Sample Text: REQUIRETLS support required
   Associated basic status code: 550
   Description: This indicates that the message was not
                               able to be forwarded because it was
                               received with a REQUIRETLS requirement
                               and none of the SMTP servers to which
                               the message should be forwarded provide
                               this support.
   Reference: (this document)
   Submitter: J. Fenton
   Change controller: IESG

   If published as an RFC, this draft requests the addition of an entry
   to the Permanent Message Header Field Names Registry
   [PermMessageHeaderFields]:

       Header field name: TLS-Required
       Applicable protocol: mail
       Status: standard
       Author/change controller: IETF
       Specification document: (this document)

       This section is to be updated for publication by the RFC Editor.

8. Security Considerations

   The purpose of REQUIRETLS is to give the originator of a message
   control over the security of email they send, either by conveying an
   expectation that it will be transmitted in an encrypted form "over
   the wire" or explicitly that transport encryption is not required if
   it cannot be successfully negotiated.

   The following considerations apply to the REQUIRETLS service
   extension but not the TLS-Required header field, since messages
   specifying the header field are less concerned with transport
   security.

8.1. Passive attacks

   REQUIRETLS is generally effective against passive attackers who are
   merely trying to eavesdrop on an SMTP exchange between an SMTP client
   and server. This assumes, of course, the cryptographic integrity of
   the TLS connection being used.

8.2. Active attacks

   Active attacks against TLS encrypted SMTP connections can take many
   forms. One such attack is to interfere in the negotiation by
   changing the STARTTLS command to something illegal such as XXXXXXXX.
   This causes TLS negotiation to fail and messages to be sent in the
   clear, where they can be intercepted. REQUIRETLS detects the failure
   of STARTTLS and declines to send the message rather than send it
   insecurely.

   A second form of attack is a man-in-the-middle attack where the
   attacker terminates the TLS connection rather than the intended SMTP
   server. This is possible when, as is commonly the case, the SMTP
   client either does not verify the server's certificate or establishes
   the connection even when the verification fails. REQUIRETLS requires
   successful certificate validation before sending the message.

   Another active attack involves the spoofing of DNS MX records of the
   recipient domain. An attacker having this capability could
   potentially cause the message to be redirected to a mail server under

the attacker's own control, which would presumably have a valid
certificate. REQUIRETLS requires that the recipient domain's MX
record lookup be validated either using DNSSEC or via a published
MTA-STS policy that specifies the acceptable SMTP server hostname(s)
for the recipient domain.

8.3. Bad Actor MTAs

A bad-actor MTA along the message transmission path could
misrepresent its support of REQUIRETLS and/or actively strip
REQUIRETLS tags from messages it handles. However, since
intermediate MTAs are already trusted with the cleartext of messages
they handle, and are not part of the threat model for transport-layer
security, they are also not part of the threat model for REQUIRETLS.

It should be reemphasized that since SMTP TLS is a transport-layer
security protocol, messages sent using REQUIRETLS are not encrypted
end-to-end and are visible to MTAs that are part of the message
delivery path. Messages containing sensitive information that MTAs
should not have access to MUST be sent using end-to-end content
encryption such as OpenPGP [RFC4880] or S/MIME [RFC8551].

8.4. Policy Conflicts

In some cases, the use of the TLS-Required header field may conflict
with a recipient domain policy expressed through the DANE [RFC7672]
or MTA-STS [RFC8461] protocols. Although these protocols encourage
the use of TLS transport by advertising availability of TLS, the use
of "TLS-Required: No" header field represents an explicit decision on
the part of the sender not to require the use of TLS, such as to
overcome a configuration error. The recipient domain has the
ultimate ability to require TLS by not accepting messages when
STARTTLS has not been negotiated; otherwise, "TLS-Required: No" is
effectively directing the client MTA to behave as if it does not
support DANE nor MTA-STS.

9. Acknowledgements

The author would like to acknowledge many helpful suggestions on the
ietf-smtp and uta mailing lists, in particular those of Viktor
Dukhovni, Chris Newman, Tony Finch, Jeremy Harris, Arvel Hathcock,
John Klensin, Barry Leiba, John Levine, Rolf Sonneveld, and Per
Thorsheim.

[10](). Revision History

To be removed by RFC Editor upon publication as an RFC.

[10.1](). Changes since -08 Draft

Additional changes in response to IESG review:

o Unify wording describing TLS-Required in [Appendix A.2]().

o Add specifics on verification of mail server hostnames with certificates.

o Wording tweak in 4.3 to emphasize optional nature of REQUIRETLS.

o Update S/MIME reference from [RFC 5751]() to 8551

[10.2](). Changes since -07 Draft

Changes in response to IESG review and IETF Last Call comments:

o Change associated status code for 5.7.YYY from 530 to 550.

o Correct textual name of extension in IANA Considerations for consistency with the rest of the document.

o Remove special handling of bounce messages in [Section 4.1]().

o Change name of header field from RequireTLS to TLS-Required and make capitalization of parameter consistent.

o Remove mention of transforming RET=FULL to RET=HDRS on relay in [Section 5]().

o Replace [Section 6]() dealing with mailing lists with a more general section on reorigination by mediators.

o Add security considerations section on policy conflicts.

[10.3](). Changes since -06 Draft

Various changes in response to AD review:

o Reference [RFC 7525]() for TLS negotiation recommendations.

o Make reference to requested 5.7.YYY error code consistent.

o Clarify applicability to LMTP and submission.

o Provide ABNF for syntax of SMTP option and header field and
   examples in Appendix A.

o Correct use of normative language in Section 5.

o Clarify case where REQUIRETLS option is used on bounce messages.

o Improve Security Requirements wording to be inclusive of both SMTP
   option and header field.

10.4. Changes since -05 Draft

Corrected IANA Permanent Message Header Fields Registry request.

10.5. Changes since -04 Draft

Require validation of SMTP server hostname via DNSSEC or MTA-STS
policy when TLS is required.

10.6. Changes since -03 Draft

Working Group Last Call changes, including:

o Correct reference for SMTP DANE

o Clarify that RequireTLS: NO applies to both MTA-STS and DANE
   policies

o Correct newly-defined status codes

o Update MTA-STS references to RFC

10.7. Changes since -02 Draft

o More complete documentation for IANA registration requests.

o Changed bounce handling to use RET parameters of [RFC3461], along
   with slightly more liberal transmission of bounces even if
   REQUIRETLS can't be negotiated.

10.8. Changes since -01 Draft

o Converted DEEP references to RFC 8314.

o Removed REQUIRETLS options: CHAIN, DANE, and DNSSEC.

o Editorial corrections, notably making the header field name
   consistent (RequireTLS rather than Require-TLS).

10.9. Changes since -00 Draft

   o Created new header field, Require-TLS, for use by "NO" option.

   o Removed "NO" option from SMTP service extension.

   o Recommend DEEP requirements for delivery of messages requiring
      TLS.

   o Assorted copy edits

10.10. Changes since fenton-03 Draft

   o Wording improvements from Rolf Sonneveld review 22 July 2017

   o A few copy edits

   o Conversion from individual to UTA WG draft

10.11. Changes Since -02 Draft

   o Incorporation of "MAY TLS" functionality as REQUIRETLS=NO per
      suggestion on UTA WG mailing list.

   o Additional guidance on bounce messages

10.12. Changes Since -01 Draft

   o Specified retries when multiple MX hosts exist for a given domain.

   o Clarified generation of non-delivery messages

   o Specified requirements for application of REQUIRETLS to mail
      forwarders and mailing lists.

   o Clarified DNSSEC requirements to include MX lookup only.

   o Corrected terminology regarding message retrieval vs. delivery.

   o Changed category to standards track.

10.13. Changes Since -00 Draft

   o Conversion of REQUIRETLS from an SMTP verb to a MAIL FROM
      parameter to better associate REQUIRETLS requirements with
      transmission of individual messages.

   o Addition of an option to require DNSSEC lookup of the remote mail
      server, since this affects the common name of the certificate that
      is presented.

   o Clarified the wording to more clearly state that TLS sessions must
      be established and not simply that STARTTLS is negotiated.

   o Introduced need for minimum encryption standards (key lengths and
      algorithms)

   o Substantially rewritten Security Considerations section

11. References

11.1. Normative References

   [MailParams]
              Internet Assigned Numbers Authority (IANA), "IANA Mail
              Parameters", 2007,
              <http://www.iana.org/assignments/mail-parameters>.

   [PermMessageHeaderFields]
              Internet Assigned Numbers Authority (IANA), "Permanent
              Message Header Field Names Registry", 2004,
              <https://www.iana.org/assignments/message-headers/
              message-headers.xhtml#perm-headers>.

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119,
              DOI 10.17487/RFC2119, March 1997,
              <https://www.rfc-editor.org/info/rfc2119>.

   [RFC3207] Hoffman, P., "SMTP Service Extension for Secure SMTP over
              Transport Layer Security", RFC 3207, DOI 10.17487/RFC3207,
              February 2002, <https://www.rfc-editor.org/info/rfc3207>.

   [RFC3461] Moore, K., "Simple Mail Transfer Protocol (SMTP) Service
              Extension for Delivery Status Notifications (DSNs)",
              RFC 3461, DOI 10.17487/RFC3461, January 2003,
              <https://www.rfc-editor.org/info/rfc3461>.

   [RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S.
              Rose, "DNS Security Introduction and Requirements",
              RFC 4033, DOI 10.17487/RFC4033, March 2005,
              <https://www.rfc-editor.org/info/rfc4033>.

   [RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S.
              Rose, "Resource Records for the DNS Security Extensions",
              RFC 4034, DOI 10.17487/RFC4034, March 2005,
              <https://www.rfc-editor.org/info/rfc4034>.

   [RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S.
              Rose, "Protocol Modifications for the DNS Security
              Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005,
              <https://www.rfc-editor.org/info/rfc4035>.

   [RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax
              Specifications: ABNF", STD 68, RFC 5234,
              DOI 10.17487/RFC5234, January 2008,
              <https://www.rfc-editor.org/info/rfc5234>.

   [RFC5248] Hansen, T. and J. Klensin, "A Registry for SMTP Enhanced
              Mail System Status Codes", BCP 138, RFC 5248,
              DOI 10.17487/RFC5248, June 2008,
              <https://www.rfc-editor.org/info/rfc5248>.

   [RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321,
              DOI 10.17487/RFC5321, October 2008,
              <https://www.rfc-editor.org/info/rfc5321>.

   [RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322,
              DOI 10.17487/RFC5322, October 2008,
              <https://www.rfc-editor.org/info/rfc5322>.

   [RFC6125] Saint-Andre, P. and J. Hodges, "Representation and
              Verification of Domain-Based Application Service Identity
              within Internet Public Key Infrastructure Using X.509
              (PKIX) Certificates in the Context of Transport Layer
              Security (TLS)", RFC 6125, DOI 10.17487/RFC6125, March
              2011, <https://www.rfc-editor.org/info/rfc6125>.

   [RFC7525] Sheffer, Y., Holz, R., and P. Saint-Andre,
              "Recommendations for Secure Use of Transport Layer
              Security (TLS) and Datagram Transport Layer Security
              (DTLS)", BCP 195, RFC 7525, DOI 10.17487/RFC7525, May
              2015, <https://www.rfc-editor.org/info/rfc7525>.

   [RFC7672] Dukhovni, V. and W. Hardaker, "SMTP Security via
              Opportunistic DNS-Based Authentication of Named Entities
              (DANE) Transport Layer Security (TLS)", RFC 7672,
              DOI 10.17487/RFC7672, October 2015,
              <https://www.rfc-editor.org/info/rfc7672>.

   [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
              2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
              May 2017, <https://www.rfc-editor.org/info/rfc8174>.

   [RFC8314] Moore, K. and C. Newman, "Cleartext Considered Obsolete:
              Use of Transport Layer Security (TLS) for Email Submission
              and Access", RFC 8314, DOI 10.17487/RFC8314, January 2018,
              <https://www.rfc-editor.org/info/rfc8314>.

   [RFC8461] Margolis, D., Risher, M., Ramakrishnan, B., Brotman, A.,
              and J. Jones, "SMTP MTA Strict Transport Security (MTA-
              STS)", RFC 8461, DOI 10.17487/RFC8461, September 2018,
              <https://www.rfc-editor.org/info/rfc8461>.

   [SMTPStatusCodes]
              Internet Assigned Numbers Authority (IANA), "Simple Mail
              Transfer Protocol (SMTP) Enhanced Status Codes Registry",
              2008, <http://www.iana.org/assignments/
              smtp-enhanced-status-codes>.

11.2. Informative References

   [RFC1939] Myers, J. and M. Rose, "Post Office Protocol - Version 3",
              STD 53, RFC 1939, DOI 10.17487/RFC1939, May 1996,
              <https://www.rfc-editor.org/info/rfc1939>.

   [RFC2033] Myers, J., "Local Mail Transfer Protocol", RFC 2033,
              DOI 10.17487/RFC2033, October 1996,
              <https://www.rfc-editor.org/info/rfc2033>.

   [RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION
              4rev1", RFC 3501, DOI 10.17487/RFC3501, March 2003,
              <https://www.rfc-editor.org/info/rfc3501>.

   [RFC4880] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R.
              Thayer, "OpenPGP Message Format", RFC 4880,
              DOI 10.17487/RFC4880, November 2007,
              <https://www.rfc-editor.org/info/rfc4880>.

   [RFC5228] Guenther, P., Ed. and T. Showalter, Ed., "Sieve: An Email
              Filtering Language", RFC 5228, DOI 10.17487/RFC5228,
              January 2008, <https://www.rfc-editor.org/info/rfc5228>.

   [RFC5598] Crocker, D., "Internet Mail Architecture", RFC 5598,
              DOI 10.17487/RFC5598, July 2009,
              <https://www.rfc-editor.org/info/rfc5598>.

   [RFC6409] Gellens, R. and J. Klensin, "Message Submission for Mail",
              STD 72, RFC 6409, DOI 10.17487/RFC6409, November 2011,
              <https://www.rfc-editor.org/info/rfc6409>.

   [RFC8551] Schaad, J., Ramsdell, B., and S. Turner, "Secure/
              Multipurpose Internet Mail Extensions (S/MIME) Version 4.0
              Message Specification", RFC 8551, DOI 10.17487/RFC8551,
              April 2019, <https://www.rfc-editor.org/info/rfc8551>.

Appendix A. Examples

   This section is informative.

A.1. REQUIRETLS SMTP Option

   The TLS-Required SMTP option is used to express the intent of the
   sender that the associated message be relayed using TLS. In the
   following example, lines beginning with C: are transmitted from the
   SMTP client to the server, and lines beginning with S: are
   transmitted in the opposite direction.

```
   S: 220 mail.example.net ESMTP
   C: EHLO mail.example.org
   S: 250-mail.example.net Hello example.org [192.0.2.1]
   S: 250-SIZE 52428800
   S: 250-8BITMIME
   S: 250-PIPELINING
   S: 250-STARTTLS
   S: 250 HELP
   C: STARTTLS
   S: TLS go ahead

   (at this point TLS negotiation takes place. The remainder of this
   session occurs within TLS.)

   S: 220 mail.example.net ESMTP
   C: EHLO mail.example.org
   S: 250-mail.example.net Hello example.org [192.0.2.1]
   S: 250-SIZE 52428800
   S: 250-8BITMIME
   S: 250-PIPELINING
   S: 250-REQUIRETLS
   S: 250 HELP
   C: MAIL FROM:<roger@example.org> REQUIRETLS
   S: 250 OK
   C: RCPT TO:<editor@example.net>
   S: 250 Accepted
   C: DATA
   S: 354 Enter message, ending with "." on a line by itself

   (message follows)
   C: .
   S: 250 OK
   C: QUIT
```

A.2. TLS-Required Header Field

   The TLS-Required header field is used when the sender requests that
   the mail system not heed a default policy of the recipient domain
   requiring TLS. It might be used, for example, to allow problems with
   the recipient domain's TLS certificate to be reported:

```
   From: Roger Reporter <roger@example.org>
   To: Andy Admin <admin@example.com>
   Subject: Certificate problem?
   TLS-Required: No
   Date: Fri, 18 Jan 2019 10:26:55 -0800
   Message-ID: <5c421a6f79c0e_d153ff8286d45c468473@mail.example.org>

   Andy, there seems to be a problem with the TLS certificate
   on your mail server. Are you aware of this?

   Roger
```

Author's Address

   Jim Fenton
   Altmode Networks
   Los Altos, California 94024
   USA

   Email: fenton@bluepopcorn.net