Internet Engineering Task Force
Internet-Draft
Updates: 5321, 3207 (if approved)
Intended status: Informational
Expires: 21 January 2026

S. Nurpmeso, Ed.
20 July 2025

Secure SMTP/TLS SRV Announcement
draft-nurpmeso-smtp-tls-srv-06

Abstract

This specification defines a DNS (RFC 1035) SRV (RFC 2782) record that announces TLS (RFC 9325) secured SMTP (RFC 5321, RFC 3207), optionally including Implicit TLS.

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 21 January 2026.

Table of Contents

1. Introduction

[RFC2782] defines a widely adopted DNS-based service discovery protocol. [RFC6186] is a specification of SRV[RFC2782] records for the email protocols IMAP[RFC9051], POP3[RFC1939], and SUBMISSION[RFC6409]. This includes DNS service names for Implicit TLS protocol variants. SMTP[RFC5321] connections to MTAs ([RFC5598]) do not yet define SRV records for no ever spelled out reason. (According usage does exist, see for example the German De-Mail definition law.)

Moreover, no Implicit TLS SMTP protocol variant has ever been specified, despite noticeable achievable non-batchable packet roundtrip savings, and despite availability, or easy adoptability, of such a protocol variant in existing code bases. This specification adds a SMTP/TLS service name for SRV[RFC2782] records.

1.1. Conventions and Terminology

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 term "Implicit TLS" refers to the automatic negotiation of TLS whenever a TCP connection is made on a particular TCP port that is used exclusively by that server for TLS connections. The term "Implicit TLS" is intended to contrast with the use of the STARTTLS command in SMTP that is used by the client and the server to explicitly negotiate TLS on an established cleartext TCP connection.

The term "FOSS" refers to Free and Open Source Software.

2. SMTP/TLS SRV Service Name

The service name for TLS[RFC9325] enabled Secure[RFC3207] SMTP[RFC5321] is smtp-tls, the resulting DNS label _smtp-tls.

STARTTLS
: A domain that publishes an according DNS SRV[RFC2782] resource record announces availability of Secure SMTP, namely the STARTTLS[RFC3207] SMTP service extension on the normal SMTP[RFC5321] port, specified by IANA as port 25. The port number MUST be given as 25.

Implicit TLS
: Shall the SRV RR not equal IANA port number 25, support for Implicit TLS on the specified port is announced additionally. The port number SHOULD be given as 842.

  Servers SHOULD NOT announce STARTTLS in the EHLO command response of an Implicit TLS connection. If a client issues a STARTTLS[RFC3207] extension command during an Implicit TLS connection, the SMTP reply code 554 SHOULD be returned, if enhanced status codes[RFC3463] are used, 5.5.1 SHOULD be used.

DNS SRV RRs MUST take priority over MX[RFC5321] ones: no MX lookup SHOULD be performed, and no otherwise available MX RR MUST be used in the presence of a SRV RR.

After a successful _smtp-tls DNS SRV lookup cleartext communication SHOULD NOT be used. Servers and clients which make use of the _smtp-tls DNS SRV SHOULD follow the guidelines of TLS[RFC9325].

If a DNS SRV lookup fails with "NODATA" negative caching[RFC2308] (sections 2.2 and 5) conditions, not only a maximum, but also a minimum cache time limit SHOULD be used in order to reduce excessive DNS SRV RR lookups. (It MAY seem sensible to use the TTL of the domains MX or address RR, with a maximum limit, as via [RFC2308], section 5.)

3. Examples

3.1. STARTTLS

An announcement for the STARTTLS SMTP service extension.

```
_smtp-tls._tcp     SRV 0 0  25 mail.example.com.
```

3.2. Implicit TLS

An announcement of Implicit TLS, in addition to STARTTLS.

```
_smtp-tls._tcp     SRV 0 0 842 mail.example.com.
```

3.3. Prioritized Server Selection

A multi-server scenario where the main server supports Implicit TLS and STARTTLS, whereas the backup server only supports STARTTLS.

```
_smtp-tls._tcp     SRV 0 0 842 mail.example.com.
_smtp-tls._tcp     SRV 1 0  25 backup.example.com.
```

4. Guidance for MTAs

If, after a successful _smtp-tls DNS SRV lookup that announces Implicit TLS support, connecting to the announced port fails, a connection to the IANA SMTP port 25 SHOULD be established which MUST use the STARTTLS SMTP extension. If none of the shortcomings described next apply, the fallback connection MAY however be omitted.

| _Informative remark:_ This is meant to overcome two shortcomings: first the given port may be blocked along the network path; it may take time until an IANA registration takes places, and/or the network adapts; whereas expected to be a rare event for the System Ports range ([RFC6335]), defining a recovery strategy seems useful.

| Second DNS SRV lookups could return results unprotected by DNSSEC[RFC4033][RFC4034][RFC4035], or without perceived knowledge of whether DNSSEC was actually used, for example, when the DNS is accessed via some kind of furtherly unspecified intermediate proxy that needs to be trusted: in either case the possibility of DNS forge attacks exist; if the STARTTLS secured connection to the IANA SMTP port fails, the DNS result SHOULD be treated with maximum suspicion. The mail log record may give useful insight.

The section of [RFC6186] named "Guidance for MUAs" (section 4) in parts also applies to this specification.

5. Guidance for Service Providers

The equally named section of [RFC6186] (section 5) also applies to this specification.

6. IANA Considerations

IANA is asked to allocate port number 842 for the Implicit TLS operation mode of SMTP[RFC5321]. The author wants to point out that the contra arguments given in section 7 of [RFC2595] that created according POP3S and IMAPS assignments in 1999 are contradicted by operational reality in the internet, and here that includes the IETF by means of [RFC8314]. A dedicated port enables administrators to apply strict policies, for example in firewalls.

7. Security Considerations

First of all, the equally named section of [RFC6186] (section 6) also applies to this specification.

Due to fact that one and a half decade passed since RFC 6186 it follows a reiteration of the reasoning. This specification avoids downgrade attacks on the opportunistic approach of STARTTLS, accomplished via the mechanism used for many other IETF standardized protocols, most notably [RFC2782] (IMAP, POP3, SUBMISSION). With its Implicit TLS capability it grants the SMTP protocol the same level of confidentiality through TLS[RFC9325] as is already standardized for the other email protocols; this is considered a value by itself, even for the possibly lesser sensitive MTA-to-MTA communication.

Implicit TLS reduces the number of packet roundtrips, that at a protocol stage where the widely used command pipelining[RFC2920] performance improvement extension cannot be used; these roundtrips are anachronistic (also environmentally): for example the about 4.2 million known DANE for SMTP[RFC7672] enabled domains at the time of this writing alone, which must use TLS by standard definition, likely generate (several) billion(s) of useless sequential and blocking roundtrip packets each and every day.

The security of DNS[RFC1035] is out of scope for this specification, but DNSSEC[RFC4033][RFC4034][RFC4035] and secure DNS transport[RFC7858][RFC8094][RFC8310][RFC8484][RFC9250] etc exists. Selection of the appropriate transport layer security protocol is out of scope for this specification, please see for example TLS[RFC9325].

8. References

8.1. Normative References

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, DOI 10.17487/RFC2782, February 2000, <https://www.rfc-editor.org/info/rfc2782>.

[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>.

[RFC3463] Vaudreuil, G., "Enhanced Mail System Status Codes", RFC 3463, DOI 10.17487/RFC3463, January 2003, <https://www.rfc-editor.org/info/rfc3463>.

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

8.2. Informative References

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[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>.

[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>.

[RFC2308] Andrews, M., "Negative Caching of DNS Queries (DNS NCACHE)", RFC 2308, DOI 10.17487/RFC2308, March 1998, <https://www.rfc-editor.org/info/rfc2308>.

[RFC2595] Newman, C., "Using TLS with IMAP, POP3 and ACAP", RFC 2595, DOI 10.17487/RFC2595, June 1999, <https://www.rfc-editor.org/info/rfc2595>.

[RFC2920] Freed, N., "SMTP Service Extension for Command Pipelining", STD 60, RFC 2920, DOI 10.17487/RFC2920, September 2000, <https://www.rfc-editor.org/info/rfc2920>.

[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>.

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

[RFC6186] Daboo, C., "Use of SRV Records for Locating Email Submission/Access Services", RFC 6186, DOI 10.17487/RFC6186, March 2011, <https://www.rfc-editor.org/info/rfc6186>.

[RFC6335] Cotton, M., Eggert, L., Touch, J., Westerlund, M., and S. Cheshire, "Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry", BCP 165, RFC 6335, DOI 10.17487/RFC6335, August 2011, <https://www.rfc-editor.org/info/rfc6335>.

[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>.

[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>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC8094] Reddy, T., Wing, D., and P. Patil, "DNS over Datagram Transport Layer Security (DTLS)", RFC 8094, DOI 10.17487/RFC8094, February 2017, <https://www.rfc-editor.org/info/rfc8094>.

[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>.

[RFC8310] Dickinson, S., Gillmor, D., and T. Reddy, "Usage Profiles for DNS over TLS and DNS over DTLS", RFC 8310, DOI 10.17487/RFC8310, March 2018, <https://www.rfc-editor.org/info/rfc8310>.

[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>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

[RFC9051] Melnikov, A., Ed. and B. Leiba, Ed., "Internet Message Access Protocol (IMAP) - Version 4rev2", RFC 9051, DOI 10.17487/RFC9051, August 2021, <https://www.rfc-editor.org/info/rfc9051>.

[RFC9250] Huitema, C., Dickinson, S., and A. Mankin, "DNS over Dedicated QUIC Connections", RFC 9250, DOI 10.17487/RFC9250, May 2022, <https://www.rfc-editor.org/info/rfc9250>.

[RFC9325] Sheffer, Y., Saint-Andre, P., and T. Fossati, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 9325, DOI 10.17487/RFC9325, November 2022, <https://www.rfc-editor.org/info/rfc9325>.

Appendix A. Acknowledgements

Thanks to Jan Ingvoldstad. Thanks to Jeremy Harris for spending time and revealing the many problems of early draft variants, as well as comments on how to do it better; very special thanks to him for a kickstart implementation of this very draft in the widely used FOSS MTA Exim. Jeremy Harris, Viktor Dukhovni and Wietse Venema commented on the initial odd usage of port 0 for the STARTTLS discovery case. Thanks to Alex Brotman for hinting on the fallback strategy. Thanks have to go to Jonas Stalder, also for finding IETF tooling bugs, despite his wishes not to be mentioned (anymore).

Author’s Address

Steffen Nurpmeso (editor)
Email: steffen@sdaoden.eu