Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: April 24, 2014

K. Moore
Network Heretics
October 21, 2013

# Recommendations for use of TLS by Electronic Mail Access Protocols
# draft-moore-email-tls-00

## Abstract

This memo requires support for Transport Layer Security (TLS) in all electronic mail user agents (MUAs) and the servers with which they communicate when using standard protocols, including Interactive Message Access Protocol (IMAP), Post Office Protocol (POP) and the variant of the Simple Message Transfer Protocol (SMTP) used in message submission.  It also requires support for TLS in mail protocol servers provided by electronic mail service providers, and encourages mail service providers to migrate to requiring TLS for all interaction with their servers.  In addition, this memo details specific recommendations for implementation and use of TLS with electronic mail protocols used in interactions between MUAs and mail service providers.

Use of TLS with SMTP for message relaying is described in a separate document, and not in scope for this document.

The recommendations in this memo do not replace the functionality of, and are not intended as a substitute for, end-to-end encryption of electronic mail.

## Status of This Memo

Copyright Notice

Table of Contents

## 1. Introduction

Most Internet electronic mail protocols, including SMTP Submission Protocol [RFC4409], Interactive Message Access Protocol (IMAP) [RFC3501], and Post Office Protocol (POP) [RFC1939], were originally designed to transmit all authentication credentials, commands, and application data in cleartext only. At the time that those protocols were originally designed, encryption was computationally expensive, and/or not widely available due to export limitations and other constraints. In the earliest days of these protocols, it was also typical that Internet service was provided through hardwired hosts and networks, which provided some degree of security against eavesdropping by limiting physical access to the server hosts and network media.

Recently it has become apparent that the potential for eavesdropping of electronic mail traffic has increased for a variety of reasons, including: "rogue" wireless LAN access points that monitor traffic, industrial espionage, and government-supported espionage by a variety of governments. For these reasons it now seems prudent to recommend a much wider use of TLS encryption than has been conventional in the past.

In brief, this memo now recommends that:

- TLS on a well-known port ("Implicit TLS") be for supported for Interactive Message Access Protocol (IMAP), Post Office Protocol (POP), and SMTP Submission protocol for all electronic mail user agents and servers;

- Electronic mail user agents (MUAs) require TLS for all newly configured connections to servers, unless explicitly configured by their users to not require TLS;

- When explicitly configuring an MUA to not require TLS, the MUA warn users that their mail traffic is insecure;

- Electronic mail service providers (MSPs) support use of Implicit TLS for IMAP, POP, and SMTP Submission; and

- MSPs encourage new users to configure their MUAs to require TLS when connecting to their servers, and encourage existing users to transition to MUA configurations that require TLS, using mechanisms appropriate for their user communities.

This document therefore defines profiles of the above protocols which impose additional requirements beyond those in the base protocol specifications. Specific details of these requirements, and additional requirements, are outlined below.

### 1.1. Definitions

Implicit TLS - The practice of automatically negotiating a TLS layer as soon as a TCP connection is established between client and server, on a TCP port configured on that server to perform such negotiation. This port may be assigned by IANA for that purpose, advertised by DNS SRV record, or used by private agreement between client and server. (See also STARTTLS mechanism)

Interactive Message Access Protocol (IMAP) - The protocol defined in [RFC3501] which is used for accessing and managing received electronic mail. This memo will also refer to "IMAP client" and "IMAP server" when appropriate.

mail account - A set of services provided by a Mail Service Provider for a particular sender and/or recipient, which may include (among others): mail submission, access to delivered mail, management of delivered mail, configuration of incoming mail filters, management of authentication credentials. A mail account will generally be implemented with a variety of protocol servers, for example IMAP, POP, Submission, and/or a webmail service, but will usually share a common set of authentication credentials across all of those servers.

Mail User Agent (MUA) - A client that performs one or more of the following: (a) submits electronic mail for delivery, (b) accesses mail delivered to one or more mailboxes, and/or (c) manages mail delivered to one or more mailboxes, on behalf of one or more (human or nonhuman) users. An MUA may function as any of an IMAP client, POP client, Submission client, or SMTP client, among other roles.

Mail Service Provider (MSP) - A provider of electronic mail services including (a) submission of outgoing mail and/or (b) acceptance of incoming mail and providing recipients with the ability to access that mail. In this memo, the term Mail Service Provider applies not only to providers that offer such services to the public (whether for "free" or in exchange for monetary renumeration), but also to providers of mail services to private communities, including business enterprises.

Opportunistic TLS - The practice of negotiating TLS when it appears to a TLS-capable client that the server also supports TLS, but continuing the intended operation in cleartext when it appears to the client that the server does not support TLS.

pinning - The act of establishing a cached name association between the application service's certificate and one of the client's reference identifiers, whether or not any of the certificate's presented identifiers matches one of the client's reference identifiers. (See also section 1.8 of [RFC6125].)

Post Office Protocol (POP) - The protocol defined in [RFC1939] which is used for accessing and managing received electronic mail. Since POP is a client-server protocol, this memo will refer to POP client and POP server when appropriate.

presented identifier - Any of the identifiers presented to a client in a validated TLS server certificate. (See also section 1.8 of [RFC6125].)

reference identifier - Any of a set of identifiers pre-determined by a TLS client to be acceptable identifiers for a particular service, to be matched against the presented identifiers from the server's certificate. (See also section 1.8 of [RFC6125].)

STARTTLS mechanism - One of the protocol extensions defined in [RFC2595] or [RFC3207] for negotiating TLS after a cleartext application layer connection between client and server have already been established. (See also Implicit TLS.)

Submission protocol - the variant of SMTP defined in [RFC6409] and used exclusively for submission of outgoing messages by MUAs.

Transport Layer Security (TLS) - The protocol defined in [RFC5246] and its revisions for providing security services over a TCP stream.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

## 1.2. Goals and Rationale

This memo is one of several with the shared goal of encouraging use of strong encryption for all uses of Internet electronic mail protocols, and thus reducing the effectiveness of mass surveillance which is known to be conducted on a large scale by several parties. Other memos address other aspects of this problem, including opportunistic encryption for relayed mail using SMTP

[I-D.ietf-dane-smtp-with-dane], and improving TLS server identity checks [I-D.melnikov-email-tls-certs].

The primary goal for this memo is to encourage a much wider adoption of reliable encryption for email protocol traffic between Mail User Agents (MUAs) and mail servers. "Reliable encryption" means that a user can have confidence that his mail traffic is securely encrypted when it travels over the network. By contrast, if the traffic is not encrypted, the user should be made explicitly aware of this. Since TLS is the Internet standards-track encryption mechanism which is most widely implemented in email clients and servers, is well-maintained, and believed to be sufficiently extensible to accommodate newly identified threats and use cases, TLS is the mechanism specified for providing such a reliable encryption service.

Note: The goal of "reliable encryption" is a distinct goal from, and in contrast with, a goal to encrypt as much traffic as possible. Encrypting as much traffic as possible could be accomplished using Opportunistic TLS. However, this would not be the same as "reliable encryption", as it would not provide the user with assurance that his traffic is encrypted. It also appears that there are several ways in which Opportunistic TLS can easily be defeated by an attacker. So while in some sense encrypting as much traffic as possible is also a worthy goal, reliable encryption appears to be more important. Only reliable encryption provides protection in the case of an active attack.

In furtherance of the goal of reliable encryption, a number of new requirements are imposed on mail protocol engines. However, an additional goal of this memo is to facilitate continued operation between legacy clients and servers that meet the requirements in this memo, and between legacy servers and clients that meet the requirements in this memo. Another part of that goal is to facilitate such continued operation while providing an "upgrade path" such that the vast majority of clients and servers should be able to be modified to meet these requirements within a short time, without disruption of service or significant support costs.

An additional goal of this memo is to discourage exposure of reusable authentication credentials (such as passwords) over an unencrypted channel when using IMAP, POP, or SMTP Submission, or any other protocol for which the same credentials are used as with one of the above protocols.

It is explicitly not a goal of this memo to provide any assurance of either end-to-end encryption (from submission to delivery), or encryption of delivered email that has been stored in a mailbox. Unless additionally encrypted by other means such as S/MIME

[RFC3369], email messages will still be available in cleartext on each client and server that processes or stores those messages.

## 1.3. Approach

The basic approach is to recommend that TLS and the Implicit TLS mechanism be used for all interactions between MUAs and servers: that all MUAs and servers support TLS and Implicit TLS, that MUAs use TLS by default for all newly configured server connections unless explicitly configured otherwise by their users, and that mail service providers encourage existing clients to upgrade to MUAs that support TLS and upgrade existing MUA configurations to require TLS.

After much consideration, TLS over a well-known port ("Implicit TLS") is recommended instead of the STARTTLS mechanism, for the following reasons:

- It appears to be the desired end-state. In a future world where TLS were always used, there would no longer be a need for the STARTTLS mechanism. Even if it were still necessary for some MSPs to continue to support cleartext operation for legacy or very lightweight clients, all MUAs capable of using TLS could eventually be expected to migrate to configurations using Implicit TLS.

- Implicit TLS capability is discoverable using SRV records as described in [RFC6186], whereas discovering STARTTLS capability requires opening a connection to the server.

- Use of Implicit TLS appears to be less susceptible to both MUA misconfiguration and to unintended downgrading to cleartext operation, even for legacy MUAs. If an MUA's configuration explicitly specifies either use of TLS or use of the well-known port assigned by IANA for use with Implicit TLS (often termed the "SSL port"), it seems unlikely that the MUA will downgrade to the "non-SSL port" under any circumstances, even if the server is unreachable or TLS negotiation fails. In addition, if a mail service provider advertises Implicit TLS as its preferred mechanism to connect to servers (via SRV records and/or human-readable documentation), the mail service provider can defeat automatic downgrading to cleartext operation by MUAs (even with legacy MUAs) simply by not providing a working server that supports cleartext operation on the same IP address recommended for use with new configurations. (Cleartext access for existing users and configurations can still be maintained on the existing IP address.)

- In earlier unpublished drafts of this memo, the author attempted to recommend STARTTLS in preference to Implicit TLS. The ability of the same server to support both TLS and cleartext operation seemed to conflict with the desire for a server to be able to disable cleartext operation for new users or users who had migrated to require TLS. It was found difficult to describe how servers requiring TLS for some users and permitting cleartext access for others, could do so without introducing the possibility for MUAs to expose the user's username and password in cleartext even when that user was required to use TLS - because with most of the password-based authentication mechanisms defined for these protocols, the server does not have the opportunity to refuse an authentication attempt until the user's password has been transmitted. Rather than recommend STARTTLS or allow either mechanism, it seemed simpler and less error-prone to just specify Implicit TLS as the required and recommended TLS negotiation mechanism for new MUA-to-server configurations.

## 2. Implementation Requirements

This section details requirements for implementations of electronic mail protocol clients and servers. Note that a requirement for a client or server implementation to support a particular feature is not the same thing as a requirement that a client or server running a conforming implementation be configured to use that feature. Requirements for MSPs are distinct from requirements for protocol implementations, and are listed in a separate section.

### 2.1. Mail Server Requirements

The following requirements apply to IMAP, POP, and Submission server implementations:

All IMAP, POP, and Submission servers MUST be configurable to support the use of TLS and the Implicit TLS mechanism when communicating with MUAs.

IMAP, POP, and Submission servers SHOULD also support the STARTTLS mechanism for the sake of backward compatibility with existing MUAs and configurations that use it.

Servers which support STARTTLS SHOULD be capable of requiring TLS before performing any operation other than capability discovery and STARTTLS.

IMAP, POP, and Submission servers which support STARTTLS SHOULD be capable of disabling STARTTLS operation and/or disabling operation on any port that isn't configured to use Implicit TLS, so that the service provider may force all users to use Implicit TLS.

### 2.2. Mail User Agent Requirements

This section describes requirements on Mail User Agents (MUAs) using IMAP, POP, and/or Submission protocols.

Note: Requirements pertaining to use of Submission servers are also applicable to use of SMTP servers (whether on port 25 or on another port as advertised by a SRV record with _smtp._tcp or _smtps._tcp label) for mail submission.

#### 2.2.1. MUAs Configurable to Require TLS

MUAs which are configurable to communicate with user-specified IMAP, POP, and/or Submission servers MUST be configurable (on a per-server or per-account basis) to require the use of TLS when communicating with those servers.

MUAs MAY also be configurable (on a per-server or per-account basis) to use Opportunistic TLS when connecting to IMAP, POP, and Submission servers. Such a configuration MUST NOT be the default. Note that support for an Opportunistic TLS configuration option does not satisfy the requirement that MUAs be able to require use of TLS when communicating with a particular server.

In addition, MUAs MAY be configurable (on a per-server or per-account basis) to not use TLS, to permit it to interoperate with legacy servers that do not support TLS.

Whenever requested to establish any configuration that does not require TLS to talk to a server or account (including a configuration using Opportunistic TLS), an MUA SHOULD warn its user that his or her mail traffic (including password, if applicable) will be exposed to attackers.

#### 2.2.2. Non-configurable MUAs and nonstandard access protocols

MUAs which are not configurable to use user-specified servers MUST use TLS or similarly other strong encryption mechanism when communicating with their mail servers. This generally applies to MUAs that are pre-configured to operate with one or more specific services, whether or not supplied by the vendor of those services.

MUAs using protocols other than IMAP, POP, and Submission to communicate with mail servers, MUST use TLS or other similarly robust encryption mechanism in conjuction with those protocols.

### 2.2.3. Implicit TLS vs. STARTTLS

User-configurable MUAs MUST support the ability to use the Implicit TLS mechanism when communicating with servers that support it.

User-configurable MUAs SHOULD also support the STARTTLS mechanism for the sake of backward compatibility with IMAP, POP, and Submission servers that do not support Implicit TLS with these services.

### 2.2.4. Use of SRV records in Establishing Configuration

User-configurable MUAs SHOULD support use of [RFC6186] to determine (for mail service providers that advertise such information) which options are available for configuration of connections to IMAP, POP, and Submission servers. However, when using configuration information obtained by this method, MUAs SHOULD behave as if the user had explicitly required TLS, unless the user has explicitly requested to disable it. (Compare with section 6 of [RFC6186]). This will have the effect of causing the MUA to ignore advertised configurations which do not support TLS, even when those advertised configurations have a higher priority than other advertised configurations. (The specific user interface by which a user requests to disable encryption is an implementation detail, but the user interface should make it clear to users that disabling encryption will likely result in their email being spied upon.) Note: [RFC6186] does not define a label for use with SRV records to indicate that a Submission server supports Implicit TLS on a particular port. This memo defines the _submissions._tcp label for that purpose.

When using [RFC6186] configuration information, Mail User Agents SHOULD NOT automatically establish new configurations which do not require TLS for all servers, unless there are no advertised configurations using TLS. If such a configuration is chosen, prior to attempting to authenticate to the server or use the server for message submission, the MUA SHOULD warn the user that traffic to that server will not be encrypted and that it will therefore likely be intercepted by unauthorized parties. (The specific wording is to be determined by the implementation, but it should adequately capture the sense of risk given the widespread incidence of mass surveillance of email traffic.)

When establishing a new configuration for connecting to an IMAP, POP, or Submission server, an MUA MUST NOT blindly trust SRV records

unless they are signed by DNSSEC and have a valid signature. Instead, the MUA SHOULD warn the user that the DNS-advertised mechanism for connecting to the server is not authenticated, and request the user to manually verify the connection details by reference to his or her mail service provider's documentation.

Similarly, an MUA MUST NOT consult SRV records to determine which servers to use on every connection attempt, unless those SRV records are signed by DNSSEC and have a valid signature. However, an MUA MAY consult SRV records from time to time to determine if an MSP's server configuration has changed, and alert the user if it appears that this has happened. This can also serve as a means to encourage users to upgrade their configurations to require TLS if and when their MSPs support it. However, MUAs SHOULD NOT automatically upgrade configurations to require TLS without explicit user approval.

### 2.2.5. Manual configuration of MUA connection to servers

Configurable MUAs SHOULD permit manual user configuration and re-configuration of server name or address, port number, and whether to use STARTTLS and/or Implicit TLS, for IMAP, POP, and Submission servers, regardless of any information obtained using [RFC6186] procedures or other means.

Note: While many users will always use the IMAP or POP and Submission servers provided by the same MSP to which their incoming mail is delivered, there are many valid use cases for having these servers provided by multiple parties. It is therefore useful for an MUA to permit users to configure each of those services separately.

If a user explicitly selects a configuration for a server that does not use TLS, the MUA SHOULD, prior to authenticating to the server as that user, warn the user that traffic to the server will not be encrypted and thus will likely be intercepted by unauthorized parties. (The specific wording is to be determined by the implementation, but it should adequately capture the sense of risk given the widespread use of mass surveillance).

Whenever a MUA is explicitly configured to connect to a specific IP address rather than a DNS name, the MUA MUST also either be configured to explicitly compare the server certificate against a known certificate ("pinning"), or be explicitly configured as to which reference identifier(s) will be matched with the TLS server certificate's presented identifiers.

### 2.2.6. Verification of new or edited server configurations

Any time the configuration of an MUA is altered to change the servers with which the MUA communicates, the MUA SHOULD verify that it can connect to the servers, validate the TLS certificates, compare them with TLSA records if those are present and have valid DNSSEC signatures, and authenticate to the servers on behalf of the user.

If TLSA verification of the server's public key fails the MUA should not attempt to authenticate to the server.

If the server's TLS certificate does not present any identifiers that match any of the appropriate reference identifiers for the server name, the MUA MAY offer to "pin" the server certificate for use in future comparisons.  In such cases the MUA SHOULD instruct the user to check with the MSP to determine whether the MSP thinks that it has a valid certificate that is issued by a trusted certificate authority, before the user approves the configuration that "pins" the certificate.

### 2.2.7.  Downgrading of TLS-required Configurations

Once a configuration that requires TLS to connect to a server has been established, Mail User Agents MUST NOT attempt to authenticate to that server, or use that server for mail submission, without successfully negotiating TLS (including server certificate validity checks and reference identifier matching checks), unless the user has explicitly reconfigured the MUA to do so.

An MUAs configured to use STARTTLS for a particular server SHOULD warn its user when a server which previously advertised STARTTLS capability is apparently no longer doing so, but MUST NOT downgrade the connection to cleartext unless explicitly (re)configured by the user to do so.

### 2.2.8.  Requirements for MUA use of TLS

An MUA configured to require TLS when connecting to a particular server MUST successfully negotiate TLS (including successful certificate validity and reference identifier checks) before attempting to use that server.  The TLS layer MAY use either Implicit TLS or STARTTLS, according to the client's configuration for that server.

An MUA that is configured to require TLS for a particular server MUST negotiate TLS (including successful certificate validity and reference identifier checks) before attempting to authenticate to that server. This TLS layer MAY be negotiated using either Implicit TLS or the STARTTLS mechanism, according to the client's configuration for that server. Note: This requirement applies even if the authentication mechanism doesn't use cleartext credentials.

MUAs MUST abort the connection and refuse to interact with any server for which TLS negotiation signals any of the alert messages specified in section 7.2 of [RFC5246], or any other indication that the connection may be insecure (whether due to man-in-the-middle attack or other reason). Exception: Connections to a server with a self-signed certificate MAY be accepted if the Mail User Agent is explicitly configured ("pinned") to accept a self-signed certificate for that server.

MUAs MUST use the procedure defined in [RFC6125] to determine whether a server's TLS certificate contains an identifier which matches the DNS name to which the MUA is attempting to connect, and MUST abort the TLS session if the server's certificate does not present an identifier that matches one of the MUA's predetermined reference identifiers for that server.

It is important to avoid using DNS names obtained from SRV records (rather than from explicit user configuration) as reference identifiers when comparing with presented identifiers in TLS server certificates, unless those SRV records were signed with DNSSEC and the signatures were verified by the MUA.

Note in Draft: [I-D.melnikov-email-tls-certs] describes a profile of [RFC6125] for use in MUA checking of presented identifiers in TLS server certificates.

### 2.2.9. Use of SMTP by MUAs for other than mail submission

Some Mail User Agents use SMTP for purposes other than submitting mail, e.g. to determine whether a particular recipient can receive a message of a particular size. Such uses SHOULD use TLS if the server advertises STARTTLS in response to EHLO.

To avoid exposing message metadata which could be used for traffic analysis, MUAs SHOULD NOT send MAIL or RCPT to an SMTP server without negotiating TLS.

### 2.2.10. Other network-accessible services used by MUAs

MUAs which are configured to access other services requiring authentication, and using the same reusable credentials (e.g. passwords) with those servers as are used to authenticate to servers using TLS, MUST NOT expose those credentials over an unencrypted connection.

### 2.2.11. Additional Considerations for Webmail and other Split-MUA Clients

A webmail MUA is any MUA that is designed to be used via a web browser. Typically a webmail MUA has two portions - a "front-end" portion which runs in the user's web browser, and a "back-end" which runs on a web server. The webmail MUA typically uses HTTP to communicate between the front-end and back-end, and the back-end is responsible for communicating with message stores and mail submission services. Other "split MUA" arrangements also exist, notably to support mobile and other devices with modest local compute capability and/or bandwidth limitations.

The above requirements are also applicable to Webmail and other split MUA arrangements. For example, the requirements listed above for use of TLS between IMAP, POP, and Submission clients and servers also apply to communications between the back-ends of split MUAs and servers for those protocols. If the communications between the back-end of a split MUA and those servers doesn't use TLS, it MUST use a similarly-secure encryption mechanism.

In addition, split MUAs MUST use TLS or a similarly-secure encryption mechanism, to communicate between the front-end (web browser in the case of a webmail MUA) and the back-end.

### 2.2.12. Use of DANE by MUAs

MUAs SHOULD be able to use the DANE TLSA records in DNS [RFC6698] to verify that the public key presented in a certificate ostensibly received from a server, is actually a key authorized for use by that domain name. Use of TLSA records can provide a trust anchor in addition to that provided by the TLS server certificate, and help protect against rogue certificate authorities and compromised certificate authority private keys. There are multiple cases which must be considered:

- No TLSA record for the target domain exists. In this case verification of the server's certificate SHOULD rely entirely on whether the signing certificate authority is trusted by the client or whether the client has been explicitly configured ("pinned") to trust that particular certificate. However a MUA MAY be configurable to require both a signed TLSA record and a TLS server certificate signed by a trusted certificate authority.

- One or more TLSA records exist for the target domain but are either unsigned, or the DNSSEC signature is invalid, or DNSSEC signature cannot be verified. In this case the client SHOULD refuse to connect to the server until the signature on the TLSA records can be verified, unless the client has been explicitly configured ("pinned") to trust a particular server certificate. This might either be an indication of an attack or a configuration error, but seems better to detect the configuration error and cause it to be fixed, than ignore it.

- One or more TLSA records exist and have a valid DNSSEC signature but no TLSA records match the X.509 certificate presented by the server. In this cases the client MUST gracefully terminate the session with the server without attempting to authenticate or request services, as this may indicate a man-in-the-middle attack.

- TLSA record exists and has a valid DNSSEC signature, and the public key specified in a TLSA record matches the public key in the X.509 certificate presented by the server. However, the server certificate is not signed by a trusted certificate authority, nor has the MUA been explicitly configured ("pinned") to accept that particular certificate. In this case the connection MUST gracefully terminate the session with the server without attempting to authenticate or request services.

- The TLSA record has a valid DNSSEC signature, TLS has been successfully negotiated with no errors or alerts, and the server's certificate is valid and signed by a trusted certificate authority. In this case the session MAY proceed.

### 2.2.13. Use of DNSSEC

All uses of DNSSEC by MUAs (including use of SRV and TLSA records) SHOULD explicitly verify the chain of DNSSEC signatures from the root, rather than trusting a recursive caching DNS name server to do so. It is acceptable to obtain RRSIG, DNSKEY, DS, etc., resource records from a recursive caching name server. But a recursive caching name server SHOULD NOT be assumed to be trustworthy enough to validate signatures.

### 2.3. Requirements Common To Both Servers and MUAs

TLS version 1.2 [RFC5246] SHOULD be supported.

Per [RFC6176], SSL version 2.0 MUST NOT be supported. MUAs MUST either disable SSL 2.0 support in their TLS implementations or immediately close a connection with a server if SSL 2.0 is negotiated. Servers MUST NOT advertise support for version 2.0 of SSL.

The renegotiation indication extension described in [RFC5746] SHOULD be supported.

The Server Name Indication extension [RFC6066] SHOULD be supported.

## 3. Mail Service Provider Requirements

### 3.1. Server Requirements

Mail Service Providers MUST use server implementations that conform to this specification.

### 3.2. MSPs MUST provide Submission Servers

Mail Service Providers which accept incoming mail for delivery using the Internet Protocol MUST provide one or more Submission servers for this purpose, separate from the SMTP servers used to process incoming mail. Those submission servers MUST be configured to support Implicit TLS and MAY be configured to support STARTTLS also.

MSPs MAY also support submission of messages via one or more designated SMTP servers to facilitate compatibility with existing MUA configurations and legacy MUAs.

Discussion: SMTP servers used to accept incoming mail or to relay mail are expected to accept mail in cleartext. This is incompatible with the purpose of this memo which is to encourage encryption of traffic between mail servers. There is no such requirement for Submission servers to accept mail in cleartext or without authentication. For other reasons, use of separate Submission servers has been best practice for many years.

Submission servers SHOULD require authentication as a condition of accepting mail.

### 3.3. TLS Server Certificate Requirements

MSPs MUST maintain valid server certificates for all servers. Those server certificates MUST present DNS-IDs and SRV-IDs conforming to [RFC6125] and which will be recognized by MUAs meeting the requirements of this memo. In addition, those server certificates MAY provide other DNS-IDs, SRV-IDs, or CN-IDs needed for compatibility with legacy MUAs.

A single certificate MAY be used for multiple electronic mail protocol servers (including webmail) which all providing service for a particular mail domain, but use of the same certificate for services other than electronic mail is discouraged.

If a protocol server provides service for more than one mail domain, its server certificates MAY advertise multiple domains. This will generally be necessary unless and until it is acceptable to impose the constraint that the server and all clients support the Server Name Indication extension to TLS.

### 3.4. Recommended DNS records for mail protocol servers

This section discusses not only the DNS records that are recommended, but also implications of DNS records for server configuration and TLS server certificates.

#### 3.4.1. MX records

It is recommended that MSPs advertise MX records for handling of inbound mail (instead of relying entirely on A or AAAA records), and that those MX records be signed using DNSSEC. This is mentioned here only for completeness, as handling of inbound mail is out of scope for this document.

#### 3.4.2. SRV records

MSPs SHOULD advertise SRV records to aid MUAs in determination of proper configuration of servers, per the instructions in [RFC6186].

MSPs SHOULD advertise servers that support Implicit TLS in preference to those which support cleartext and/or STARTTLS operation.

#### 3.4.3. TLSA records

MSPs SHOULD advertise TLSA records to provide an additional trust anchor for public keys used in TLS server certificates. However, TLSA records MUST NOT be advertised unless they are signed using DNSSEC.

#### 3.4.4. DNSSEC

All DNS records advertised by an MSP as a means of aiding clients in communicating with the MSP's servers, SHOULD be signed using DNSSEC.

### 3.5. MSP Server Monitoring

MSPs SHOULD regularly and frequently monitor their various servers to make sure that: TLS server certificates remain valid and are not about to expire, TLSA records match the public keys advertised in server certificates and are signed using DNSSEC, server configurations are consistent with SRV advertisements, and DNSSEC signatures are valid and verifiable. Failure to detect expired certificates and DNS configuration errors in a timely fashion can result in significant loss of service for an MSP's users.

### 3.6. Encourage Transition to TLS Required Configurations

Mail Service Providers SHOULD encourage their users to transition to requiring TLS for communications with their servers.

Each MSP must determine which transition measures are most appropriate for its own user community. Possible mechanisms include, but are not limited to: using [RFC6186] to advertise servers which implement Implicit TLS; allowing individual users to configure their accounts so that the servers will refuse their authentication unless using TLS; requiring new users to always use TLS; providing or recommending MUA implementations that implement TLS and the ability to require TLS.

Note: there is a tradeoff here between encouraging use of TLS and not breaking access for existing users or users with legacy mail clients. Whether to enable "TLS required" for all users, new users only, or particular users that have expressed a preference to always use TLS, is a policy decision which should be re-evaluated periodically as conditions change - e.g. as more clients are upgraded to support TLS and [RFC6186]. Similarly, whether and when to require existing users to use TLS (and perhaps to upgrade their mail clients) is a policy decision that will differ from one service provider to the next depending on conditions and business needs.

## 4. Security Considerations

This entire memo is about security considerations.

The mechanisms in this memo are intended to address certain specific identified threats, including:

- A downgrading attack by thwarting connection to or TLS negotiation on the "SSL port", by a MUA implementing Opportunistic TLS. This is addressed by encouraging MUAs to implement "TLS required" operation so that the MUA will not downgrade.

- Compromised certificate authority private keys, and rogue certificate authority issuing certificates to impersonators, to generate fake certificates that can be used with man-in-the-middle attacks. This is addressed by encouraging support for DNSSEC-signed TLSA records in both clients and servers, thus providing an additional trust anchor beyond the TLS server certificate.

- An interception proxy, firewall, or other middlebox hiding STARTTLS capability advertisement or blocking the STARTTLS command, thus forcing a downgrade. This is addressed by encouraging MUAs to support "TLS required" configurations and users to migrate to them, as well as by encouraging Implicit TLS in preference to STARTTLS.

- Attacks on DNS queries, including cache poisoning, man-in-the-middle, and forged responses. These are addressed by encouraging use of DNSSEC and by insisting on strict verification of presented identifiers obtained from TLS server certificates against a predetermined set of reference identifers that are based either on explicit user input or DNSSEC-signed DNS responses.

In exchange for the perceived benefits listed above, the mechanisms described in this memo may increase the vulnerability of mail services to denial-of-service attacks. This appears to be a necessary and appropriate compromise.

Use of TLS is not a substitute for end-to-end encryption such as S/MIME. In particular, TLS does not and cannot protect against compromise of the message servers that see the messages in cleartext. Users are encouraged to use end-to-end encryption whenever available.

## 5. IANA Considerations

IANA is requested to allocate a well-known port for use with a Submission protocol server configured to use Implicit TLS. The recommended service identifier for this port is "submissions", for consistency with identifiers for other "SSL ports", even though this looks like a plural.

If there is a registry of labels for SRV records, IANA is requested to define a label of _submissions._tcp for use in advertising Submission servers using Implicit TLS.

## 6. References

### 6.1. Normative References

[RFC1939] Myers, J. and M. Rose, "Post Office Protocol - Version 3", STD 53, RFC 1939, May 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2595] Newman, C., "Using TLS with IMAP, POP3 and ACAP", RFC 2595, June 1999.

[RFC3207] Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security", RFC 3207, February 2002.

[RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, March 2003.

[RFC4409] Gellens, R. and J. Klensin, "Message Submission for Mail", RFC 4409, April 2006.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5746] Rescorla, E., Ray, M., Dispensa, S., and N. Oskov, "Transport Layer Security (TLS) Renegotiation Indication Extension", RFC 5746, February 2010.

[RFC6066] Eastlake, D., "Transport Layer Security (TLS) Extensions: Extension Definitions", RFC 6066, January 2011.

[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, March 2011.

[RFC6176] Turner, S. and T. Polk, "Prohibiting Secure Sockets Layer (SSL) Version 2.0", RFC 6176, March 2011.

[RFC6186] Daboo, C., "Use of SRV Records for Locating Email Submission/Access Services", RFC 6186, March 2011.

[RFC6409] Gellens, R. and J. Klensin, "Message Submission for Mail", STD 72, RFC 6409, November 2011.

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, August 2012.

## 6.2. Informative References

[RFC3369] Housley, R., "Cryptographic Message Syntax (CMS)", RFC 3369, August 2002.

[I-D.melnikov-email-tls-certs]
Melnikov, A., "Updated TLS Server Identity Check Procedure for Email Related Protocols", draft-melnikov-email-tls-certs-01 (work in progress), October 2013.

[I-D.ietf-dane-smtp-with-dane]
Dukhovni, V. and W. Hardaker, "SMTP security via opportunistic DANE TLS", draft-ietf-dane-smtp-with-dane-00 (work in progress), October 2013.

Author's Address

Keith Moore
Network Heretics
PO Box 1934
Knoxville, TN  37901
United States

EMail: moore@network-heretics.com