

REQUIRETLS

draft-fenton-smtp-require-tls-01

Jim Fenton
IETF 95

Problem statement

- STARTTLS is too opportunistic
 - Can't negotiate STARTTLS? Send message without.
 - Verify server's cert and then ignore the result
- Mail deliverability is paramount
 - No way to say, "prioritize security"
- Common answer: use end-to-end encryption
 - Doesn't protect message header
 - Metadata available to passive attackers

Goals

- Allow senders to specify when envelope and headers require protection
- Encourage TLS use
 - Receiving MTAs will want to receive REQUIRETLS-tagged mail
- Fine-grained
 - Don't affect messages not specifying REQUIRETLS
- Some control over certificate verification
 - Bad actors with root certs
 - Unknown trust by intermediate MTAs

Non-Goals

- MUA \leftrightarrow M*A except when accomplished via SMTP
- Choices of encryption algorithms
 - Could consider broader requirement for PFS?
- Logging

Sending a REQUIRETLS-tagged message

1. Find the SMTP server, using DNSSEC if so tagged.
2. Open SMTP session, fail if STARTTLS and REQUIRETLS not advertised.
3. STARTTLS, verifying certificate as required by message. Use “good” key lengths and algorithms.
4. Send message, with REQUIRETLS option on MAIL FROM command.

Possible issues/FAQ

- MTAs falsely advertising REQUIRETLS
 - MTAs trusted to handle mail should be trustable to do REQUIRETLS when advertised
- Mail forwarders/exploders
 - Apply REQUIRETLS to downstream recipients
- Mailing lists
 - It's up to the list operator
- Bounce handling
 - Use REQUIRETLS with same options.
 - Yes, some bounces may be lost.

REQUIRETLS negotiation

