Email and TLS

draft-newman-email-deep-02

Keith Moore & Chris Newman

IETF 91 UTA WG

DEEP Overview

- Focus on MUAs IMAP/POP/Submission
- Privacy Assurance Level for mail account (UI indicator, TLS use, cert verification)
- Prefer Implicit TLS over STARTTLS
- Security Tags, Latching (like HSTS)
- DEEP Reporting, Protocol Details

Privacy Assurance Level

- high privacy assurance requires TLS with cert verification for all account connections
- UI indication for high privacy assurance
- "no privacy assurance" MUST attempt TLS but opportunistic ok. No "lock" UI.
- Server admin can turn on security latches to upgrade privacy assurance level.

Implicit TLS vs. STARTTLS

- Implicit TLS never standardized for IMAP, POP and Submission email protocols.
- Ports registered 993, 995, (465)
- But it’s more widely used and deployed than STARTTLS for these protocols.
- For more email TLS use, standardize & promote most easily deployed option

Planned Changes

- Technical content believed complete
- Rename "low" privacy assurance to "no" privacy assurance
- Other word-smithing
- Add reference to TLS BCP
- Changes from WG and/or open issues

Controversial Issue (port 465)

- Register “submissions” service (RFC 6409 + implicit TLS) on port 465. Submissions widely deployed, but port registered for a different use. Creates wart in registry.
- Alternatives ignore reality and harm interop of TLS + submission.
- Proposal: move forward with current text revisit if consensus not achieved.

Certificate Pinning Text

- New text in version 02
- Could benefit from technical review by certificate experts
- Proposal: ask for reviewers in WG

DANE for Submission

- Should we fully define DANE for SMTP Submission? Should we prefer DANE?
- Similar to DANE for SMTP relay but with SRV (RFC 6186) instead of MX. Cert validation works if Submission server explicitly configured but solution for SRV records may not be deployed.
- Proposal: later add-on document if needed

Proposal to Split Document

- It's not clear to me what the benefit of splitting this document into two or more parts would be.
- Splitting the document would delay publication
- Proposal: don't split the document

Merge with TLS Certs Document

- Suggestion to merge this document with draft-melnikov-email-tls-certs
- Groups related information together
- Avoid publication delay of email-tls-certs
- Proposal: merge when open issues resolved if email-tls-certs not gone to IESG yet.

Concern with DANE vs. PKIX

- This allows DANE as alternative to PKIX cert verification for high privacy assurance.
- Are there scenarios where DANE is less secure than PKIX in problematic way?
- Proposal: ask for input on this issue. Leave text alone if no objections.

Timeout for latches?

- HSTS has a timeout. Should we add a timeout to email security latch protocol?
- No timeout: Service providers can’t back out of commitment without breaking users
- Timeout: Service providers may have to change software due acquisition, etc.
- Proposal: Mild pref for simple (no timeout)

UTA WG Adoption?

- Hoping to WG last call this after one more editing cycle.
- Needs more review by email folks.
- Does the WG want to adopt this?

Other Open Issues