STS for MUAs (POP, IMAP, SMTP Submit)

draft-ietf-uta-email-deep-05
Keith Moore & Chris Newman
IETF 96 UTA WG
MUA STS Overview

• Focus on MUAs IMAP/POP/SMTP-Submission (does not cover SMTP relay)

• Confidentiality Assurance Level for mail account (UI indicator, TLS use, cert verification)

• Prefer Implicit TLS over STARTTLS

• Security Directives (like HSTS)

• In-band reporting, protocol fixes
Key Changes in -05

- Change terminology to MUA STS and STS directives; initial work on registry
- Change protocol syntax to key[=value];
- DSN header removed as it belongs in MTA relay STS.
- Editorial work (references, text cleanup)
- More details in draft
Alignment of MUA and MTA STS

- Email technology is already complex. Would like to limit new complexity caused by STS.
- Proposal: align MUA and MTA STS so appropriate technology is shared.
Alignment Proposal

- Split STS directive registry from MUA draft, have both drafts use same registry
- Preferred directive syntax:
  - name[=value];name[=value];…
- Shared reporting mechanisms
  - In band, out-of-band or both?
Shared STS Registry

• Most directives are protocol-specific
  • HTTP, SMTP relay, MUA use cases are very different.

• Proposal: remove optional syntax (space and double-quotes) from syntax for other protocols.

• Proposal: Expert Review, limited use flag
Non-alignment

- MTA relay STS uses DNSSEC or HTTPS while MUA STS uses in-band TLS
- MTA relay and HSTS use max-age directive, MUA STS does not
- Other directives protocol-specific