STS for MUAs (POP, IMAP, SMTP Submit)

draft-ietf-uta-email-deep-06

Keith Moore & Chris Newman
IETF 98 UTA WG
MUA STS Overview

- **Scope:** MUA-to-server interactions (IMAP/POP/SMTP Submission) 
  Does not apply to SMTP relay

- **User-specified minimum confidentiality assurance level, plus...**

- **Server-specified security directives (like HSTS)**

- **Prefer Implicit TLS over STARTTLS**

- **In-band reporting, protocol fixes**
Key Changes in -06

- Change confidentiality assurance levels from (no confidence, high confidence) to (0, 1) leaves room to define higher levels than “high”

- Added `pkix+dane` as a value for the `tls-cert` security directive
  from server: both PKIX and DANE supported
  from client: both PKIX and DANE were used
Notable Clarifications in -06

- *Minimum* confidentiality assurance level
- Both minimum confidentiality assurance level and security directives must be satisfied
- Client MAY use protocols that meet minimum confidentiality assurance level [* and security directives] even if other protocols do not 
  (e.g. can read mail even if cannot send)
- TLS version $\geq 1.1$ required for confidentiality assurance level 1
- Either PKIX or DANE suffices for confidentiality assurance level 1
- Interaction with anti-virus / anti-spam mechanisms
Possible remaining work

- `tls-cert=pkix+dane` with other protocols?
- Define confidentiality assurance level > 1?
- Separate out IANA portions? (agreed to in Berlin but I missed that detail)
- Explicitly define what the client must do when a connection doesn’t meet minimum confidentiality assurance levels and/or security directives