REQUIRETLS
draft-ietf-uta-require-tls

Jim Fenton
IETF 104

Current Status

- In IESG evaluation
  - Currently two DISCUSS positions
- Current state: New Draft Required

Changes slated for -08

- Name of header field: RequireTLS -> TLS-Required
- Bounce messages no longer automatically exempt from REQUIRETLS
- More complete description of re-originated messages (not yet written)
  - Vacation, SIEVE
  - Not just mailing lists

Proposed new Security Consideration

8.4. Policy Conflicts

In some cases, the use of the TLS-Required header field may conflict with a recipient domain policy expressed through the DANE [RFC7672] or MTA-STS [RFC8461] protocols. Although these protocols encourage the use of TLS transport by advertising availability of TLS, the use of ”TLS-Required: No” header field represents an explicit decision on the part of the sender not to use TLS, such as to overcome a configuration error. Since TLS-Required is the more fine-grained mechanism, it is expected that this directive will generally be followed.