draft-ietf-uta-tls-for-email

UTA WG
IETF 104

Thanks to: Co-author Stephen Farrell, UTA chairs, and the UTA working group participants.

draft-ietf-uta-tls-for-email

- Deprecate TLS 1.0 & TLS 1.1 for Email services.
- Updates RFC8314.

Scope

- Some participants are asking about ciphers choice recommendation.
- Address the outstanding erratum (https://mailarchive.ietf.org/arch/msg/uta/cZ-K8Sql0-J_5kUy50epg_sRPtU)
- Update the reference to MTA-STS (https://mailarchive.ietf.org/arch/msg/uta/cZ-K8Sql0-J_5kUy50epg_sRPtU)
- Possibly include reference to REQUIRETLS, especially for message submission (https://mailarchive.ietf.org/arch/msg/uta/cZ-K8Sql0-J_5kUy50epg_sRPtU)
- Change format (https://mailarchive.ietf.org/arch/msg/uta/6ZHi1RlE2CW3eLMub2HLXaiK8dY)
- Warn users (https://mailarchive.ietf.org/arch/msg/uta/210vUfGQVr_CZRqHFZlbqgoc4lg)

Scope

- Original aim is for TLS 1.0 & TLS 1.1 deprecation.
- Should other points be included within the I-D ?
- Or should we have another I-D to address other issues ?

Questions

- We are happy to answer them.