Supplement 230

UPDATE BCP SECURE COMMUNICATIONS PROFILES

PREPARED BY LAWRENCE TARBOX & ROB HORN, ON BEHALF OF DICOM WORKING GROUP 14

23 JUNE 2022

Introduction / Scope

- This supplement updates the Secure Communications profiles to reflect the new versions of IETF's BCP-195 (Best Current Practices) and the Japanese-requested enhancements to BCP-195 (principally changes to minimum cipher suit requirements)
- This supplement will retire the 3 Secure Communications profiles based on the old versions of BCP-195 and create 2 new profiles referencing the new version of BCP-195
- The latest BCP-195 can be found at https://tools.ietf.org/html/bcp195

Primary Changes to Supporting Standards and Recommendations

- BCP now references RFC 8996 (see https://www.rfc-editor.org/rfc/rfc8996.html)
  - Deprecates TLS 1.0 and TLS 1.1
  - Deprecates old hashing algorithms and cipher suites that are no longer considered secure
  - Recommends new minimum cipher suites and other minor changes
- New Japanese recommendations "Guidelines for Configuration of TLS" Ver 3.0.1 (2020.7)
  - https://www.cryptrec.go.jp/report/cryptrec-gl-3001-3.0.1.pdf (Japanese Only)
  - https://www.ipa.go.jp/security/ipg/documents/ipa-cryptrec-gl-3001-3.0.1.pdf (Japanese Only)
  - Requires the use of TLS 1.3 when possible, but permits TLS 1.2 as fallback
  - Changes to cipher suite recommendations, more stringent than BCP-195, minimum key lengths

DICOM Changes

- Part 3.15
  - Update Normative References
  - Retire B.9 "BCP 195 TLS…", B.10 "Non-Downgrading BCP 195 TLS…", and B.11 "Extended BCP 195 TLS…" Secure Transport Connection Profiles
  - Create B.12 "BCP 195 RFC 8996 TLS Secure Transport Connection Profile", which is largely similar to B.10, but with different references, slightly different recommendations.
  - Create B.13 "Extended BCP 195 RFC 8996 TLS Secure Transport Connection Profile", which is similar to B.11, but with substantive changes to required cipher suite support and recommendations. The cipher suite changes go beyond the new B.12.