Device Pairing Using Short Authentication Strings draft-ietf-dnssd-pairing-01.txt

Daniel Kaiser, Christian Huitema

IETF 98

March 28, 2017

Changes since draft-00

- Review by Steve Kent
- Simplifications
- Precisions

Rewrote the QR code section

- Was a bit confusing, now very direct
- Phase 1, Discovery
  - Use DNS-SD to discover “_pairing._tcp”; Or,
  - Optionally, scan QR code, get “server” location from code
- Phase 2, Agreement
  - TLS session, use DH-Anon
- Phase 3, Authentication
  - Compute SAS, manual verification
  - Optionally, scan QR code, read server’s SAS

Simplifications & Clarifications

- Removed speculative language
  - For example, left “intra user pairing” variants out of “specification” part
- MUST implement TLS_DH_anon_WITH_AES_256_CBC_SHA256.

Steve Kent Suggested Split in 2 Drafts

- Style of the first part seems inappropriate for a standards track document
  - Reads like research paper
- Split in two?
  - First part becoming an informational document,
  - Second part focusing on standard track specification of the protocol
  - Reference to the informational document as appropriate.

Next steps

- Split the documents?
- Complete implementations and tests
  - Availability of TLS_DH_anon_WITH_AES_256_CBC_SHA256
  - Availability of RFC 5705 key extractor
- Last call?