

# TLS/DTLS Profiles for the Internet of Things

draft-tschofenig-uta-tls13-profile-03

# Developments since RFC 7925

- When work on RFC 7925 was started, many IoT products had no or a custom communication security solution.
- In the meanwhile, IoT deployments use TLS and DTLS to protect communication protocols. CoAP and MQTT are the main choices for IoT.
- IoT device management solutions advanced and for LwM2M in several testfests more than 40 independent implementations have been tested (all using at least DTLS).
- Many high-quality embedded TLS/DTLS 1.2 now exist on the market.
- BUT: RFC 7925 only covers version 1.2.

# Profiles for Version 1.3

- RFC 8446 makes algorithm recommendations, very much like RFC 5246 does.
  - Those recommendations work well for the web.
- TLS 1.3 adds 0-RTT and says “Application protocols **MUST NOT** use 0-RTT data without a profile that defines its use.”
  - For HTTP this profile is provided with RFC 8470.
  - For IoT, we added this CoAP profile. MQTT still to be done.
- Luckily, TLS/DTLS 1.3 fix many problems and hence the recommendation is quite short.
- draft-tschofenig-uta-tls13-profile-03 updates RFC 7925.

# New IoT-related TLS Developments

- Bandwidth reduction techniques
  - CBOR compressed certificates, certificate compression, alternative certificate formats (e.g. CWT), and cTLS in general
- Connection IDs to reduce the need to re-run handshakes again.
- Record Size Limit Extension replaced Maximum Fragment Length Extension.
- Optimized retransmission during handshake
  - Per-fragment rather than per-flight

# Next Steps

- Call for adoption
- Survey of embedded TLS stacks with regards to RFC 7925 compliance.
- Soliciting feedback from companies deploying IoT products using those recommendations.