IoT TLS/DTLS Profiles

Hannes Tschofenig
RFC 7925 – TLS/DTLS 1.2 IoT Profiles

- TLS / DTLS 1.2 offered guidance on how to use algorithms and extensions based on different credential types.
- There are combinations of algorithms and extensions that are either not recommended, insecure or not adequate for IoT deployments.
- Changes the initial timeout and maximum time for DTLS when used over certain radio technologies.
- Describes how to convey DTLS over SMS
Focuses on TLS/DTLS 1.3 but also makes updates to RFC 7925

Much shorter than RFC 7925 because TLS 1.3 has recently been published, there are fewer extensions and algorithm recommendations are current.

Many recommendations from RFC 7925 (timeout, for example) are carried over.

In some cases there are additional considerations that need to be pointed out, which are not applicable to TLS 1.2 (such as the encrypted ClientHello)

Specifies the 0-RTT application profile for CoAP.

Recommends the use of GCM and CCM over CCM8
Request for feedback

- If you are deploying TLS 1.3 (and/or DTLS 1.3) to protect IoT communication, we would like to hear from you.
- Share your experience with us.