TLS/DTLS 1.3 Profiles for the Internet of Things

draft-ietf-uta-tls13-iot-profile-08

Hannes, Thomas & Michael
What is this document about?

• Continuation of “TLS/DTLS 1.2 Profile for IoT” (RFC 7925)
  • Lots of deployment with version 1.2 available today.

• Describes recommendations for the use of version 1.3 with IoT.
  • Updates guidance initially published with RFC 7925.
Recent changes

• Extensive review by Michael
  • Some of the comments are still unaddressed and found at https://github.com/thomas-fossati/draft-tls13-iot/issues

• More details for the X.509 certificate profile
  • This is where we need more review.
Certificate Profile

• Focused on ECC certificates
• Uses IEEE 802.1AR terminology.
• Current text focuses on guidance for LDevIDs – not IDevIDs
Certificate Validity

• IoT devices often with unreliable time source.
• End-entity certificates with no maximum validity period.
• Requires the root CA certificates and the sub-ordinate CA certs to also have no maximum validity period.
• Revocation becomes an issue.
• No OCSP or CRLs mandated.
  • IoT devices often use a device management in combination with EST, CMP, etc. to update certificates and trust anchors.
Key Usage

• **Root Cert**
  • KeyUsage SHOULD be set. If set, it MUST be marked critical and the keyCertSign or cRLSign purposes MUST be set.
  • ExtendedKeyUsage extension MUST NOT be set.

• **Subordinate CA Cert**
  • KeyUsage MUST be set and MUST be marked critical. keyCertSign or cRLSign MUST be set, digitalSignature SHOULD be set.
  • ExtendedKeyUsage MAY be set depending on the intended usage of the public key. (Should it be “MUST NOT“?)

• **End Entity Cert**
  • KeyUsage: MUST be set and MUST be marked as critical. digitalSignature key usage purpose MUST be set. keyEncipherment or keyAgreement MUST be set for server-side generated keys
  • extendedKeyUsage MUST be present and contain at least one of id-kp-serverAuth or id-kp-clientAuth


Subject / SubjectAltName
End Entity Certificate

• RFC 7925 recommended the use of EUI-64. More flexible now.
• The subject alternative name extension MAY be set.
  • If it is set, it MUST NOT be marked critical, except when the subject DN contains an empty sequence.
• Device Serial Numbers can be used.
  • The Subject field MAY include a unique device serial number.
  • If the serial number is included, it MUST be encoded in the serialNumber attribute.
• Domain Names are encoded in a subjectAltName of type DNS-ID.
  • Domain names MUST NOT contain wildcard (*) characters.
  • The subjectAltName MUST NOT contain multiple names.
• Not following the encoding of HardwareModuleName of TPMs as recommended by IEEE 802.1AR.
• Lots of identifiers standardized (UUID, NAI, IMEI, ...). What do you use?
Looking for Reviewers

• Do you have experience with
  • IoT deployments of TLS/DTLS 1.3,
  • Embedded TLS/DTLS 1.3 implementations,
  • certificate management for IoT devices?

• Volunteers?
Looking for a Document Shepherd

• The UTA chairs are looking for a document shepherd for the document through the process

• Volunteer?