DTLS Profile for IoT

draft-hartke-dice-profile

IETF 88

Klaus Hartke

DICE Charter

“The first task of the working group is to define a DTLS profile that is suitable for Internet of Things applications and is reasonably implementable on many constrained devices.”

Table of Contents

1. Introduction
2. Profile
    1. Applicability
    2. Cipher Suites
    3. Extensions
    4. Other
3. Implementation Considerations
4. Privacy Considerations
5. Security Considerations
6. IANA Considerations
7. References

Profile Applicability

- Communication Model
- Threat Model
- Security Requirements
- Classes of Devices
- Trust Model
- ...

Cipher Suites

- Specific Cipher Suite(s)
  vs.
  Cryptographic Agility
- Server Authentication
  vs.
  Mutual Authentication
- X.509 Certificates
  vs.
  Raw Public Keys
  vs.
  Pre-Shared Keys
- Perfect Forward Secrecy
- ...

Extensions

- Signature Algorithms [RFC5246]
- Server Name Indication [RFC6066]
- Maximum Fragment Length [RFC6066]
- Certificate Status Request [RFC6066]
- Truncated HMAC [RFC6066]
- Supported Elliptic Curves [RFC4492]
- Supported Point Formats [RFC4492]
- Application Layer Protocol [I-D.ietf-tls-applayerprotoneg]
- Cached Info [I-D.ietf-tls-cached-info]
- Session Resumption without Server-Side State [RFC5077]
- Snap Start [I-D.agl-tls-snapstart]
- Renegotiation Indication [RFC5746]
- Heartbeat [RFC6520]
- ...

Other

- Compression
- Renegotiation vs. Reconnection
- Session Resumption
- Replay Protection
- Timer Values
- Certificate Revocation
- Encrypt-then-MAC [I-D.gutmann-tls-encrypt-then-mac]
- Hash Algorithm
- ...

Implementation Considerations

- Version negotiation
  [I-D.pettersen-tls-version-rollback-removal]
  [I-D.bmoeller-tls-downgrade-scsv]
- …

Next steps

- Same understanding of a DTLS profile?
  - Are any aspects out of scope?
  - Do additional aspects need to be included?
- Many choices depend on the usage scenario
  - Can we identify a single profile or should we aim for a (small) family of profiles?
- Identify the profile elements
  - Can we already identify DTLS functionality that is/isn't useful to have in any scenario?
    - E.g., compression