Practical Issues with DTLS

draft-hartke-dice-practical-issues

IETF 88

Klaus Hartke
DICE Charter

“The third task of the working group is to investigate practical issues around the DTLS handshake in constrained environments.

Many current systems end up fragmenting messages, and the re-transmission and re-ordering of handshake messages results in significant complexity and reliability problems.

Additional reliability mechanisms for transporting DTLS handshake messages are required as they will ensure that handling of re-ordered messages needs to be done only once in a single place in the stack.

The DICE working group may also look at alternative TLS transports in cooperation with the TLS WG.”
Step 0. DTLS is the right choice for Constrained Environments – but we have the feeling that there is room for improvement

Step 1. Document practical issues with DTLS in Constrained Environments

Step 2. Solve the issues:

- Implementation Guidance
- Profile: Cipher Suites and Extensions
- Improvements in TLS
- New, optimized transport for TLS

Step 3. Define the scope of the work
- Document the requirements
- Establish criteria for the evaluation of possible solutions

Step 4. Propose solutions

Step 5. Evaluate the proposed solutions
- Adopt a solution as working group document


Keoh, S., Kumar, S., and Z. Shelby, “Profiling of DTLS for CoAP-based IoT Applications”, draft-keoh-dtls-profile-iot-00 (work in progress), June 2013.


Bormann, C., “6LoWPAN Generic Compression of Headers and Header-like Payloads”, draft-bormann-6lo-ghc-00 (work in progress), October 2013.

