Security for Low Latency Group Communication

Hannes Tschofenig
Background

- The group focused on unicast communication so far as the main use case.
- However, there are group communication use cases described in RFC 7744 describing the lighting domain.
- This group communication interaction needs security as well.
- Prior work on group communication security dates back to the work in DICE.
- Mainly used for lighting domain.
Two Input Documents

- **Fluffy: Simplified Key Exchange for Constrained Environments (Ned, Thomas)**

- **Security for Low-Latency Group Communication (Abhinav, Hannes, Walter, Sandeep)**
Architecture

• Authentication, Authorization + Group Key Distribution
  – Keys need to be distributed (or obtained by the relevant entities)
  – Only authorized entities need to get access to the keys.
  – Fitting the exchanges into the already defined ACE framework

• Actual data protection
  – Application layer security
  – New DTLS Record Layer (DICE)
Questions

• Should the ACE group work on a solution for securing low latency group communication?
• Do you have concerns regarding the focus on symmetric key cryptography?
• Are you willing to review?
• Are you interested to contribute/implement/deploy?
• Protecting data packets:
  – New DTLS record layer?
  – Application Layer security utilizing COSE?
• Key Distribution:
  – Push approach?
  – Pull approach?
  – Both?