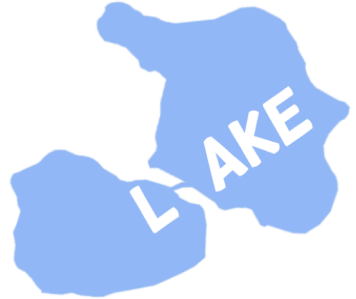
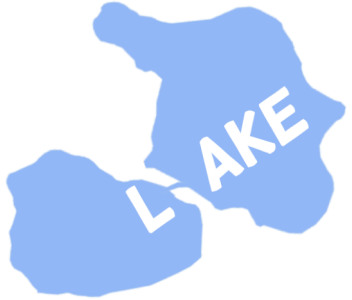


Chairs' update

LAKE @ IETF113

Progress

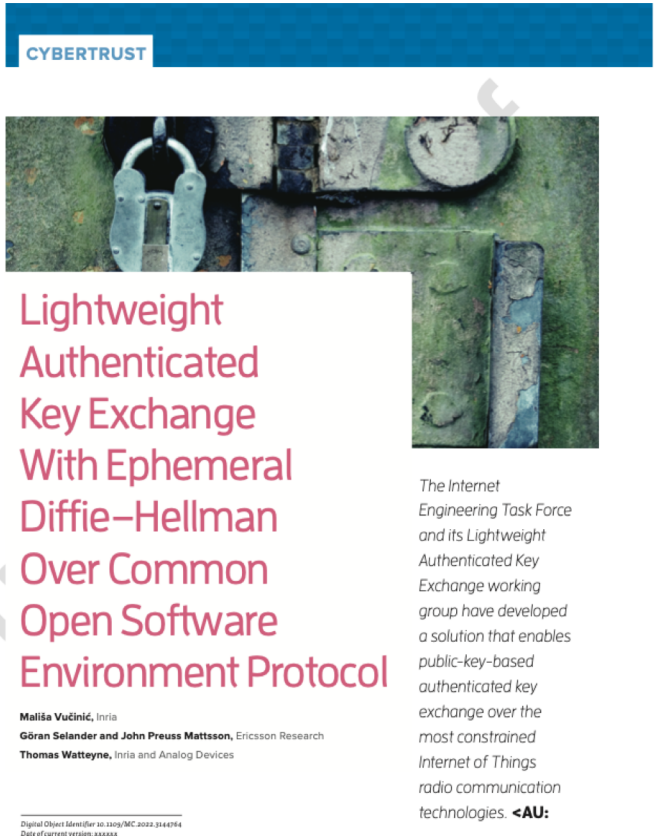


- Adopted draft-ietf-lake-traces containing the test vectors
- Declared draft-ietf-lake-edhoc-12 “ready for formal analysis” [1]
  - Invitation article published in IEEE Computer Magazine [2]
- EDHOC spec was frozen since IETF112, updated in github
- Chartered items progressed in github
  - Presented towards the end of the meeting today

[1] https://mailarchive.ietf.org/arch/msg/lake/dtEkPlVR4nMlNbQTy0kAjsf5Lx4/
[2] https://hal.inria.fr/hal-03434293v3/document

IEEE Computer Magazine article

- Summarizes the protocol
- Invites academic community
  - Symbolic model
  - Computational model
  - Implementation security
- Yes, corrected the title…



CYBERTRUST

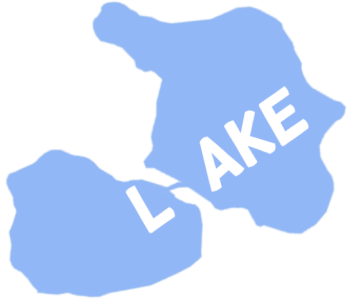
Lightweight Authenticated Key Exchange With Ephemeral Diffie–Hellman Over Common Open Software Environment Protocol

Mališa Vučinić, Inria
Göran Selander and John Preuss Mattsson, Ericsson Research
Thomas Watteyne, Inria and Analog Devices

Digital Object Identifier 10.1109/MC.2022.3144764
Date of current version: xxxxxx

The Internet Engineering Task Force and its Lightweight Authenticated Key Exchange working group have developed a solution that enables public-key–based authenticated key exchange over the most constrained Internet of Things radio communication technologies. **<AU:**

Today's meeting and milestone status



- Focus on community feedback
  - Implementers
  - Symbolic model progress
  - Computational model analysis progress
  - Implementation security progress
- March milestone
  - pushed until we collect more feedback from the academic community
  - To be discussed during the meeting

Milestones

Date	Milestone
Mar 2022	solution document to IESG (if needed)

Done milestones

Date	Milestone
Done	Adopt solution document or defer to existing external solution document draft-ietf-lake-edhoc
Done	WGLC on requirements document draft-ietf-lake-reqs