IETF Hackathon

IETF 123
19–20 July 2025
Madrid, Spain

IETF

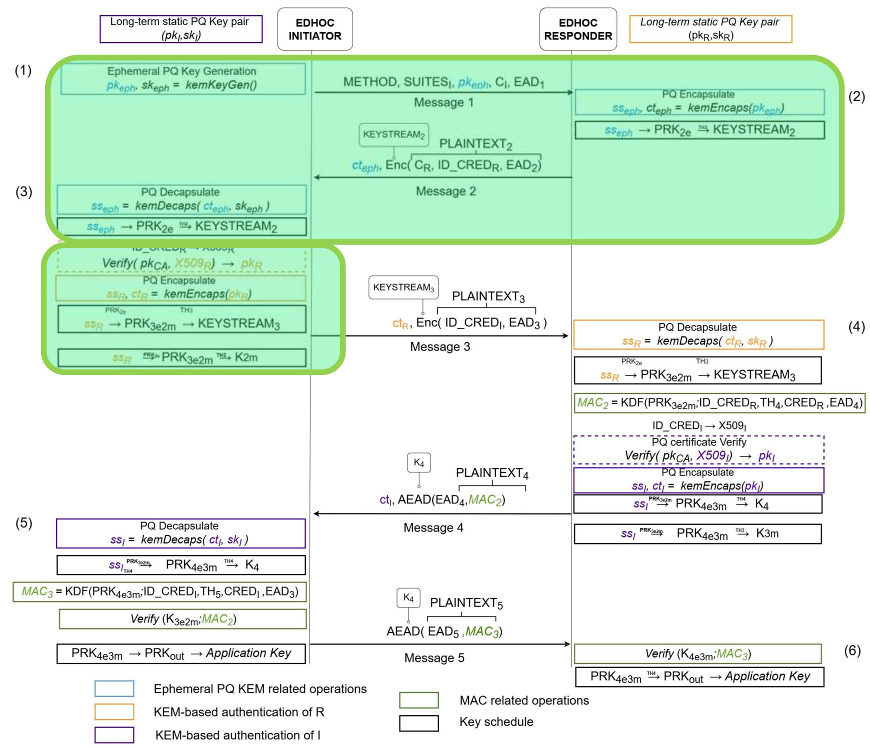
Hackathon Plan

- New authentication method for EDHOC based on Key Exchange Mechanism (KEM)
  - https://datatracker.ietf.org/doc/draft-pocero-authkem-edhoc/
  - https://datatracker.ietf.org/doc/draft-pocero-authkem-ikr-edhoc/

- Extend the KEM-based authentication method on top of the PQ-EDHOC repository, which itself builds upon the uOSCORE-uEDHOC library to support PQC signature-based EDHOC.

What got done

- [New ietf-123-hackathon branch]()
- Added a new KEM-based test vector (ML-KEM-512)
- All messages formatting
- Generation and processing of Message 1 and 2
- Compute the PRK_3e2m key from a combination of:
    - Ephemeral KEM shared secret
    - Responder's Authentication KEM shared secret



Next Steps

- Complete rest of the handshake implementation
- Test in Cortex-M4-based constrained devices
- Benchmark and compare with PQC-signature EDHOC in real-world 6lowpan scenario on the following metrics:
  - Processing time
  - Memory overhead
  - Network overhead
  - Power consumption

Wrap Up

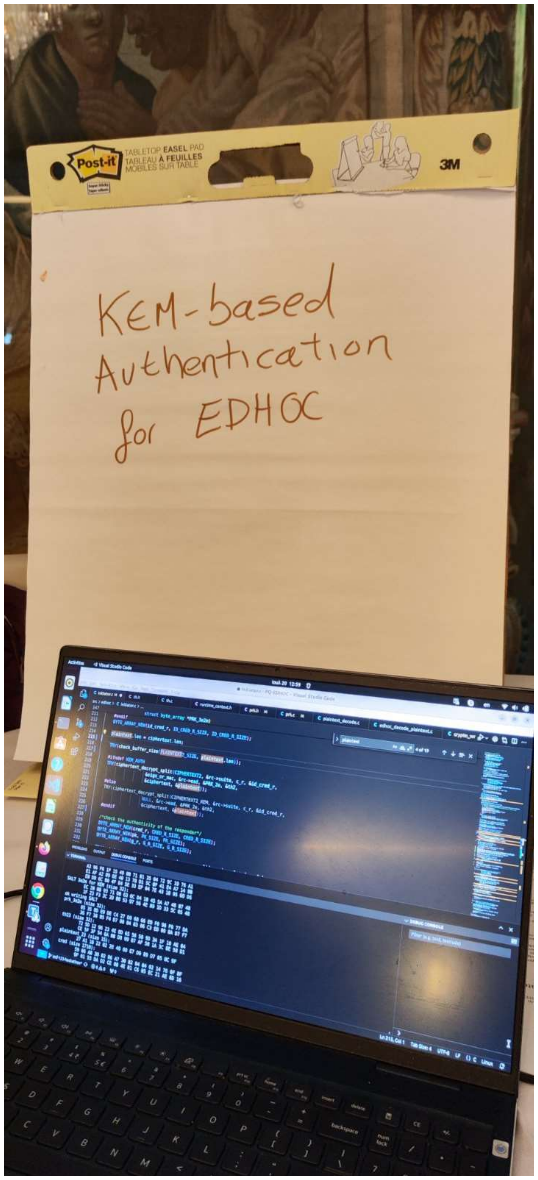
Team members:

Lidia Pocero-Fraile (pocero@athenarc.gr) (First timer)

Christos Koulamas (@athenarc.gr)

Apostolos Fournaris (fournaris@athenarc.gr)

Evangelos Haleplidis (haleplidis@athenarc.gr)



Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the European Commission can be held responsible for them.