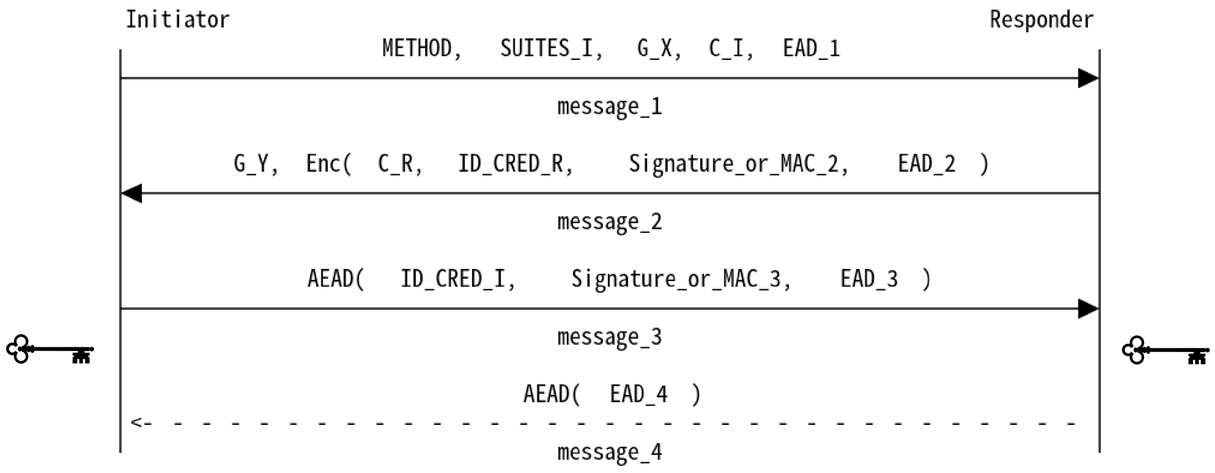
The EDHOC and OSCORE Profile of the ACE Framework for Access Control

EDHOC – Ephemeral Diffie-Hellman over COSE



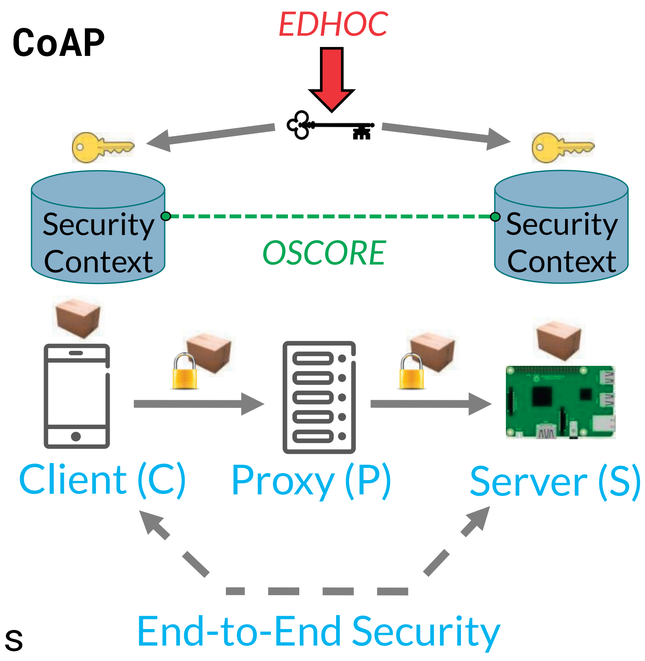
Mutually authenticated key agreement with forward secrecy and cryptoagility

OSCORE – Security for CoAP

End-to-end protection of CoAP messages, between producer and consumer

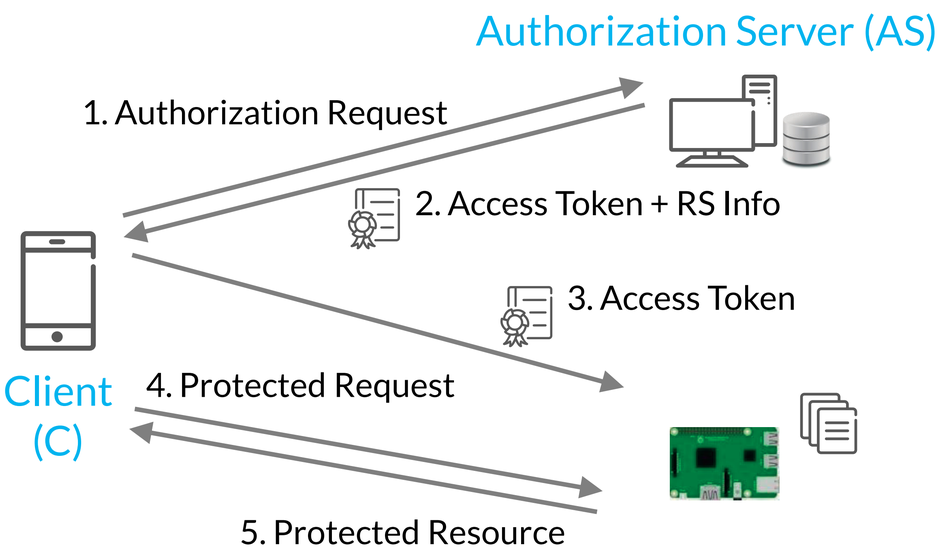
Selective protection of message fields, to enable operations from proxies

Independent of the transport used – It works where CoAP works



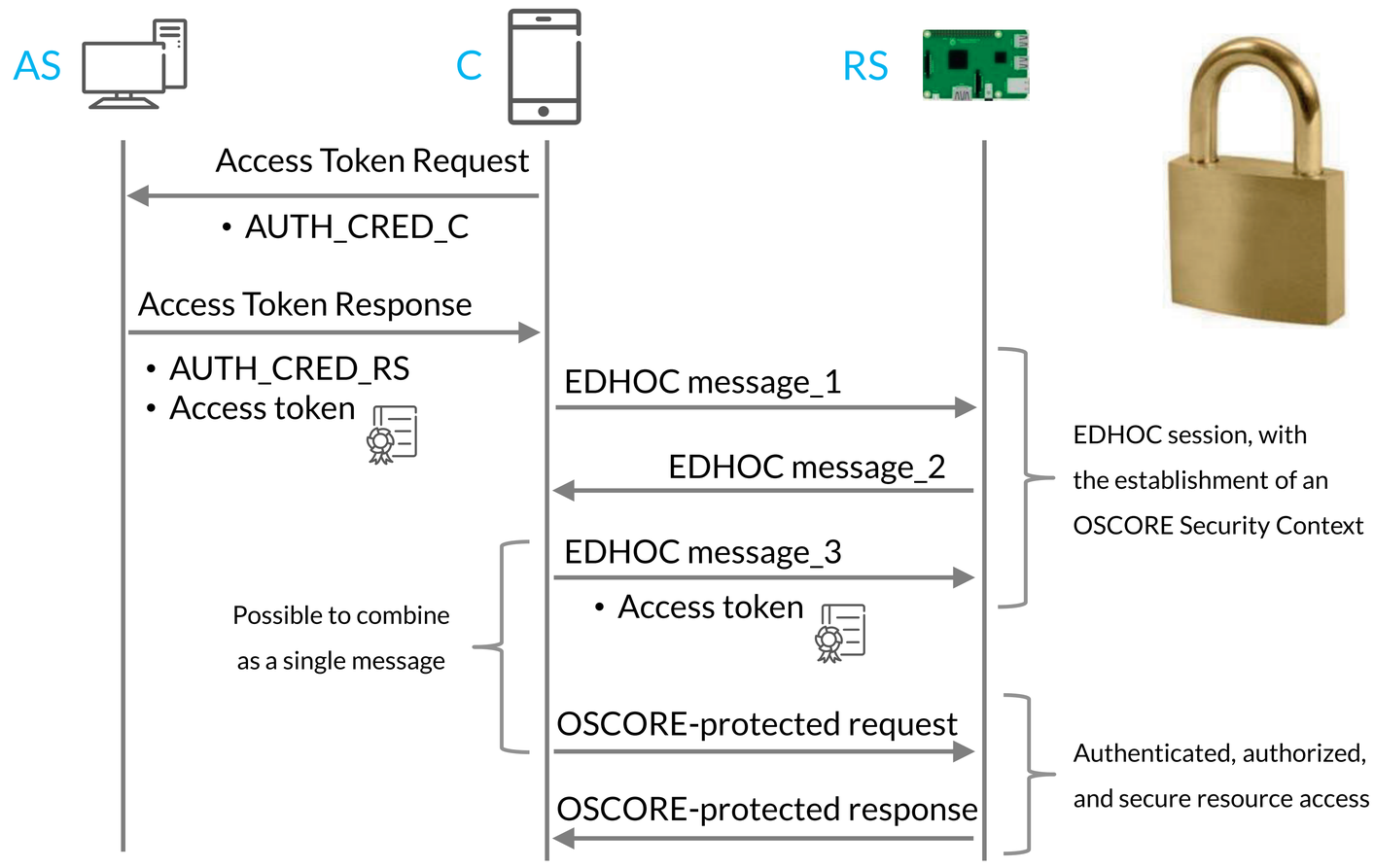
ACE framework – Access control in constrained environments

- Efficient enforcement of fine-grained access control
- A Client accesses protected resources at a Resource Server, according to access tokens issued by an Authorization Server
- Evaluation of access policies at the Authorization Server
- Separate transport profiles of the framework specify:
  - Communication and security protocols
  - Secure association between Client and Resource Server
  - Details about the message format and processing



EDHOC and OSCORE profile of ACE

- C obtains an access token from the AS
- C and RS run EDHOC to establish an OSCORE Security Context
- C provide RS with the access token within an EDHOC message
- The OSCORE Security Context derived from EDHOC is bound to the access token
- C accesses resources at RS per the access token, protecting messages with OSCORE



Ongoing standardization work in the ACE Working Group of the Internet Engineering Task Force (IETF):
G. Selander, J. Preuß Mattsson, M. Tiloca, and R. Höglund, "*Ephemeral Diffie-Hellman Over COSE (EDHOC) and Object Security for Constrained Environments (OSCORE) Profile for Authentication and Authorization for Constrained Environments (ACE)*" (work in progress)
https://datatracker.ietf.org/doc/draft-ietf-ace-edhoc-oscore-profile/

This work has been partially funded by: the Sweden's Innovation Agency VINNOVA through the Celtic-Next project CYPRESS; and the H2020 projects SIFIS-Home (Grant agreement 952652).

RISE Research Institutes of Sweden
www.ri.se / info@ri.se

CONTACT
Marco Tiloca - marco.tiloca@ri.se
Rikard Höglund - rikard.hoglund@ri.se