# Problem description for ACE

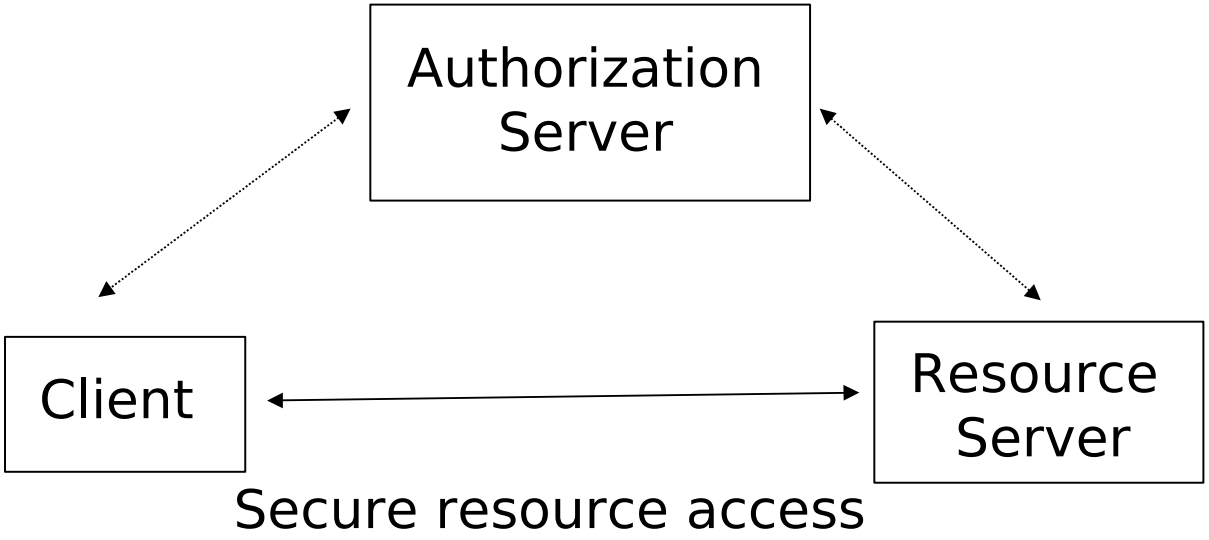
draft-seitz-ace-problem-description-01

Ludwig Seitz (ludwig@sics.se)

IETF ACE WG meeting
July 23, 2014

# Assumptions

- Client (C) securely accesses resource(s) on Resource Server (RS).
- RS protects resources against unauthorized access.
- Trusted third party: Authorization Server (AS)
  - offloads RS or C from heavy security related tasks
  - centralize authorization management



# Assumptions ctd

- One or both of C and RS is constrained
  - running on battery power, few KB RAM, few 100 KB flash memory, low bandwidth
  - unable to manage complex authorization policies
  - unable to manage many secure connections
  - without user interface
  - without constant network connectivity
  - unable to precisely measure time
  - required to save on wireless communication due to high power consumption

# Question for discussion: commSec

- C ↔ RS : Which commSec approach?
- DTLS:
  + Channel protection (including CoAP headers)
  + Efficient for long-term connection
  - High initial cost
  - No end-to-end security with middle-boxes
- Object Security (e.g. JWS/JWE)

+ Low initial cost

+ Works well with middle-boxes

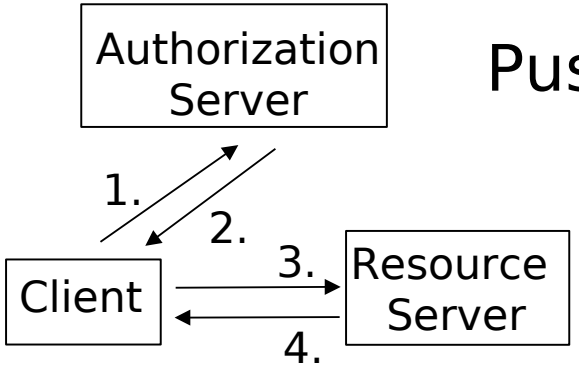
- Only the payload is protected

- Less efficient for long term connections

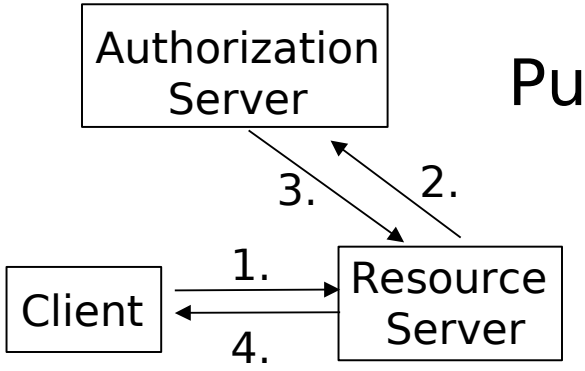
- Hybrid solutions

# Authorization

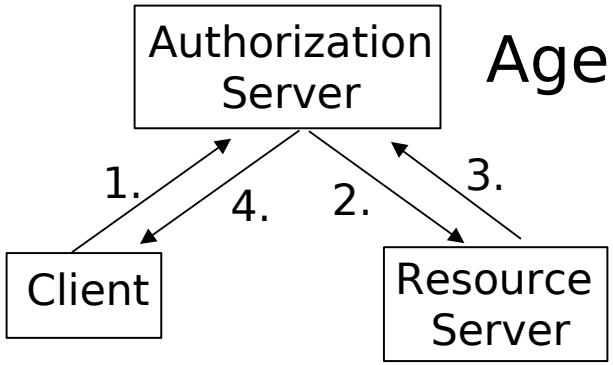
- AS – *Authorization Information* → RS (cf. RFC 2905)

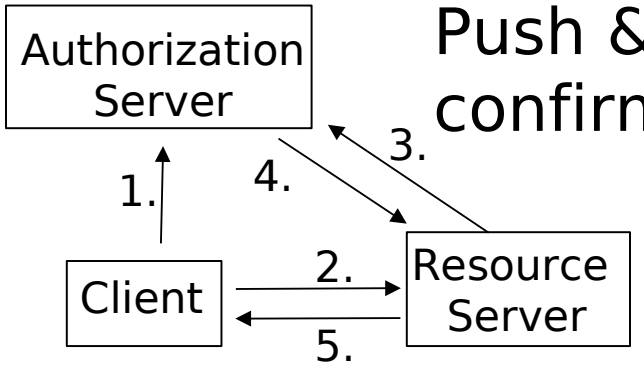



e.g. OAuth, Kerberos




e.g. EAP, ABFAB




e.g. OAuth token introspection

Thank you!

Questions/comments?