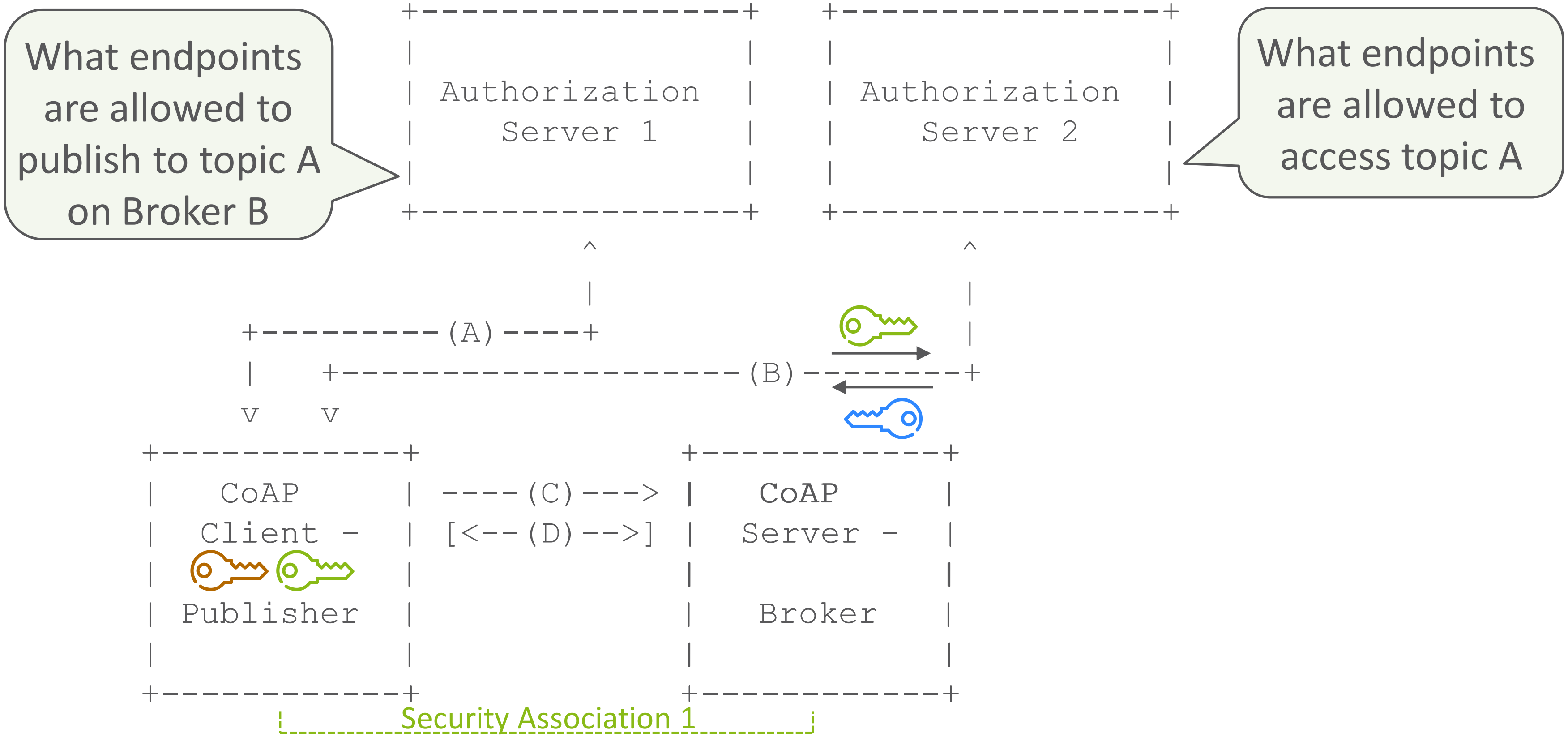
Application profiles

draft-palombini-ace-coap-pubsub

draft-tiloca-ace-oscoap-joining

Publisher Profile

- Use DTLS or OSCORE transport profile to establish secure communication between Publisher and Broker
- Use ACE token-less exchange to retrieve symmetric keying material (🔑)
- Send AS2 its own public key (🔑) corresponding to its private key (🔑)

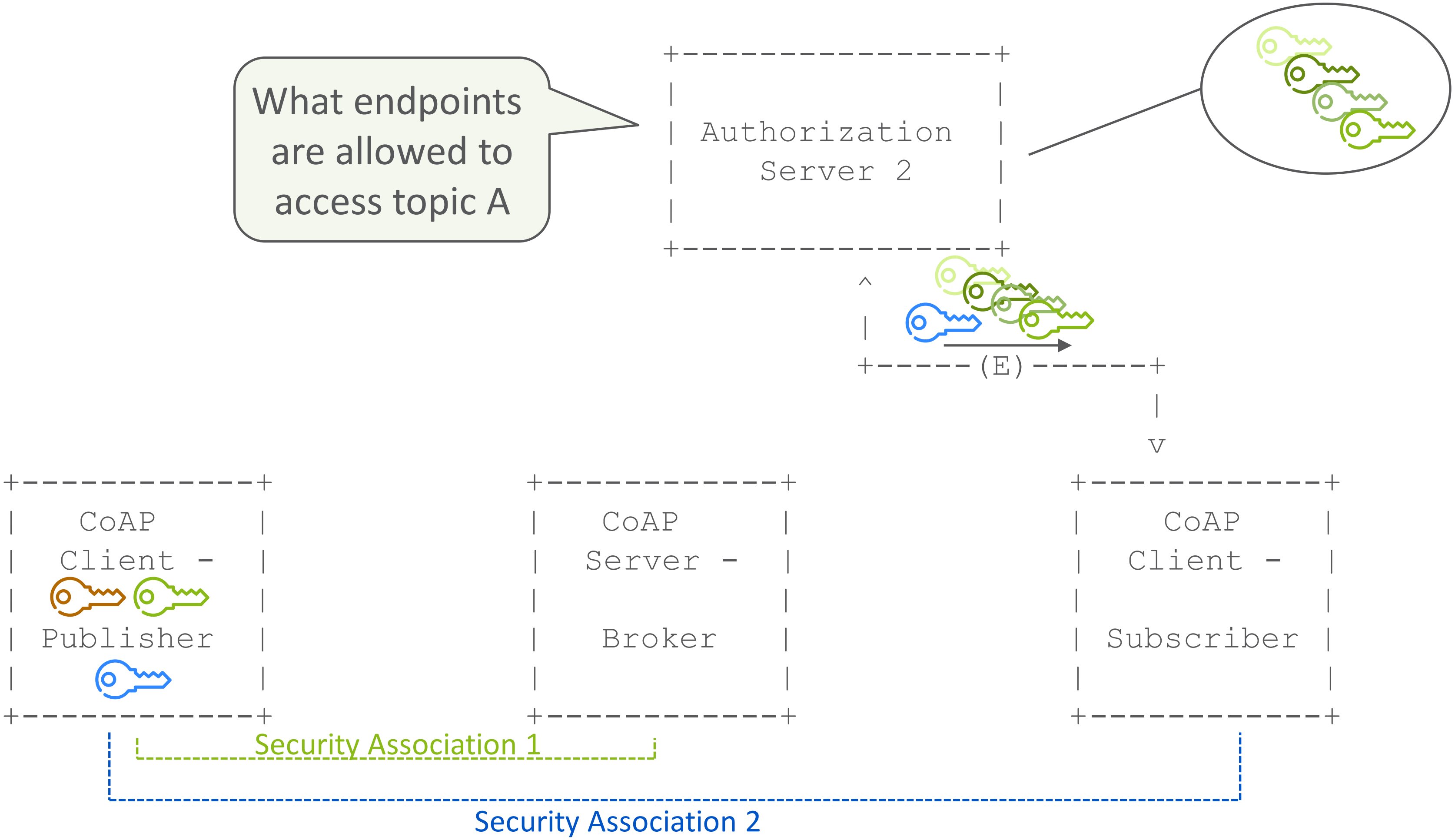


What endpoints are allowed to publish to topic A on Broker B

What endpoints are allowed to access topic A

Subscriber Profile

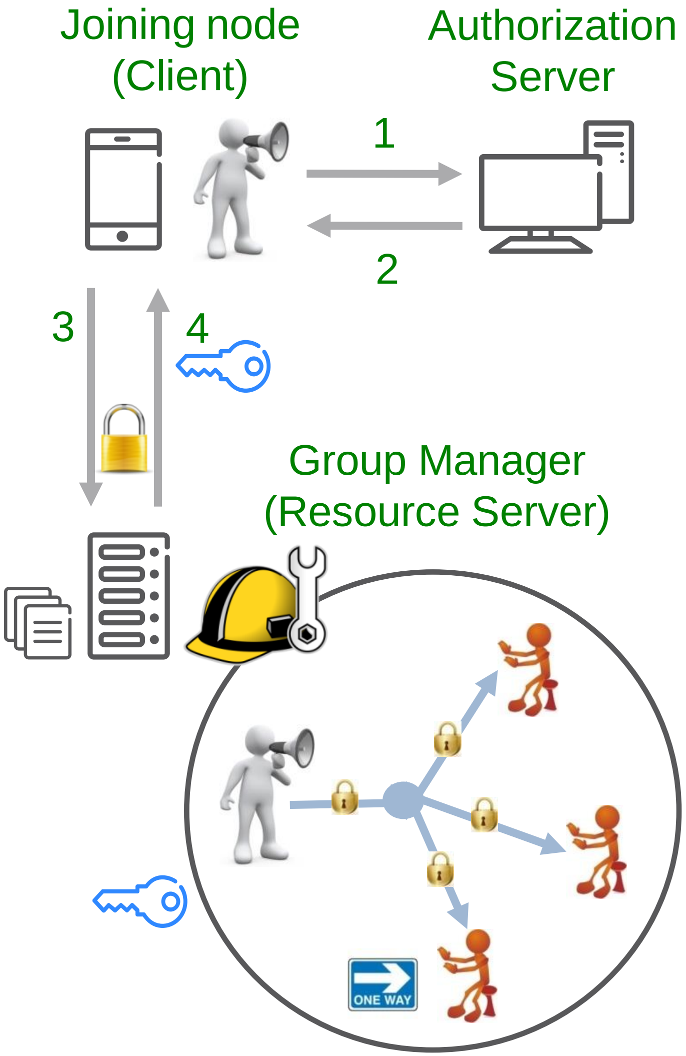
- Use ACE token-less exchange to retrieve symmetric keying material (🔑)
- AS2 sends the public keys of authorized Publishers (🔑)



What endpoints are allowed to access topic A

Group joining and key provisioning

- Join OSCORE multicast groups over the ACE framework
  - Joining node → Client
  - Group Manager → Resource Server (one *join resource* per group)
  - The AS enforces join policies on behalf of the Group Manager



- CoAP is used as application-layer protocol

- Use specific transport profiles of ACE
  - Details on authorization process
  - Secure communication between Client and GM

Thank you!