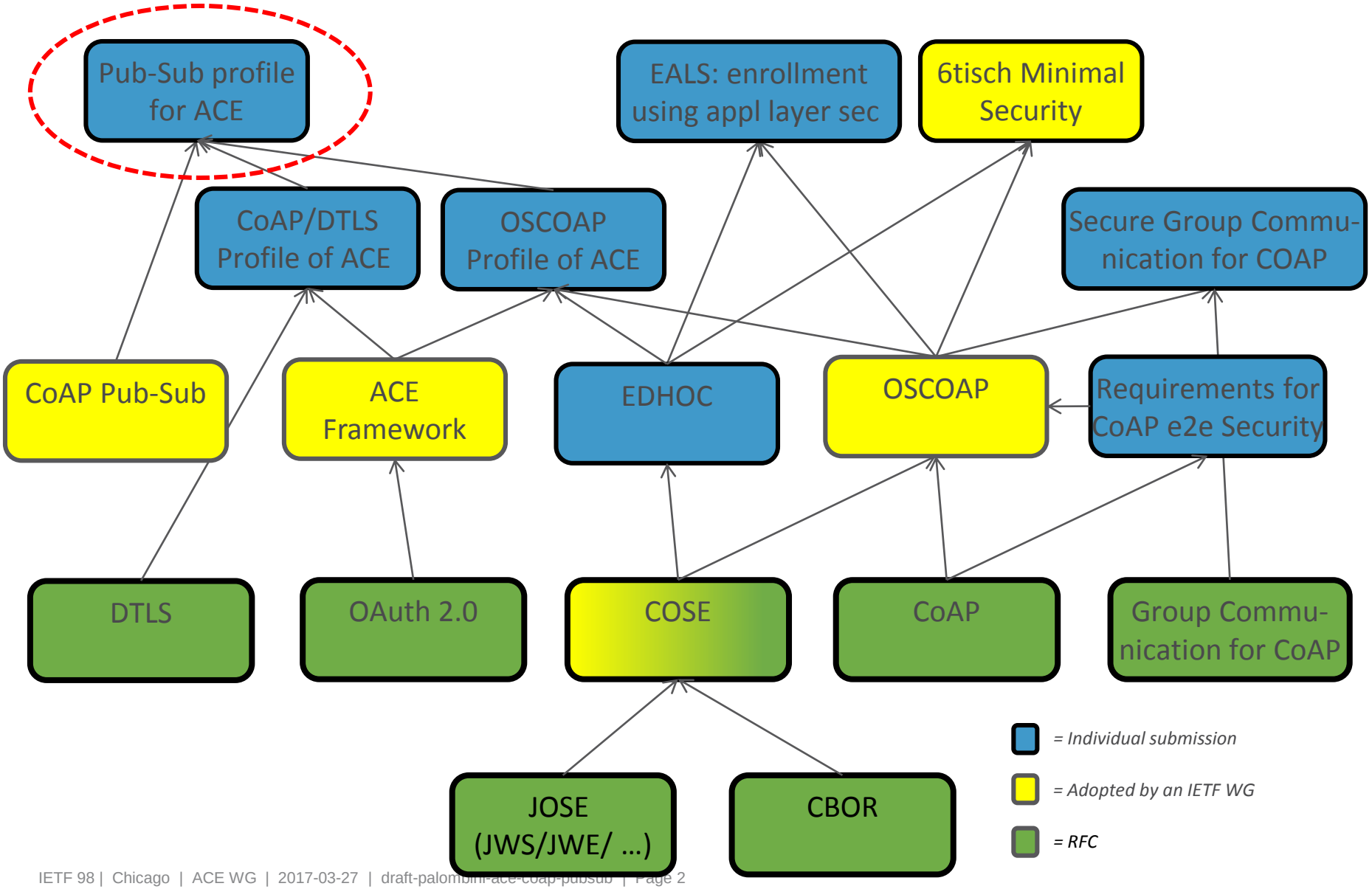
CoAP PubSub profile

draft-palombini-ace-coap-pubsub

Francesca Palombini, Ericsson

IETF 98, ACE WG, Chicago, Mar 27, 2017

Related Work



CoAP PubSub

- draft-ietf-core-coap-pubsub

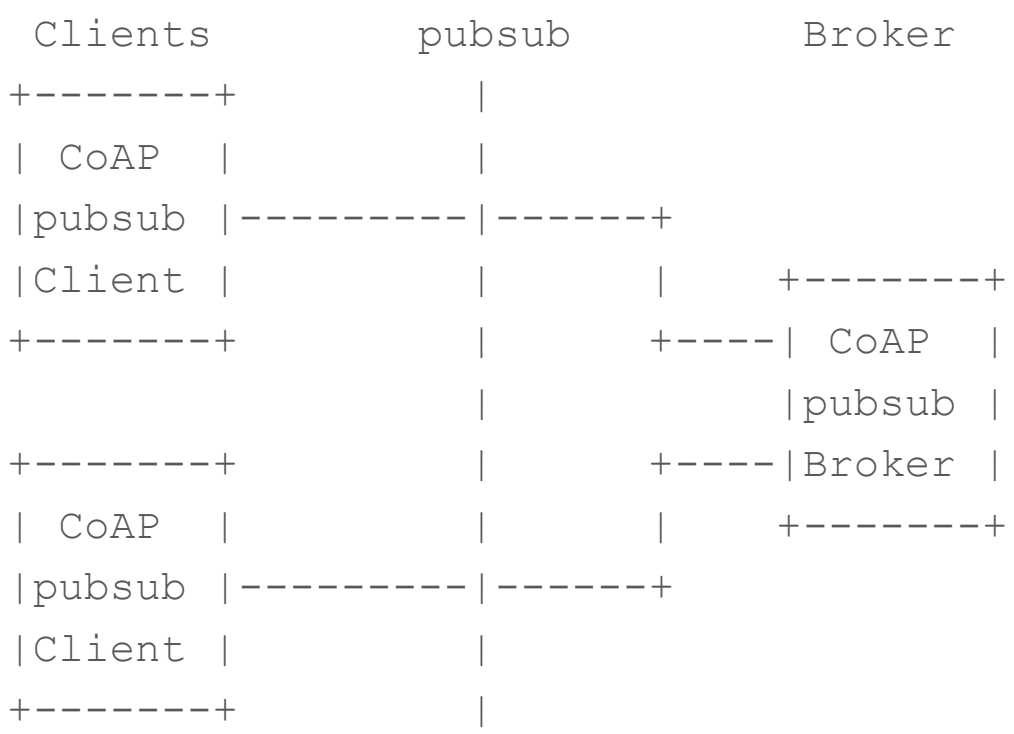
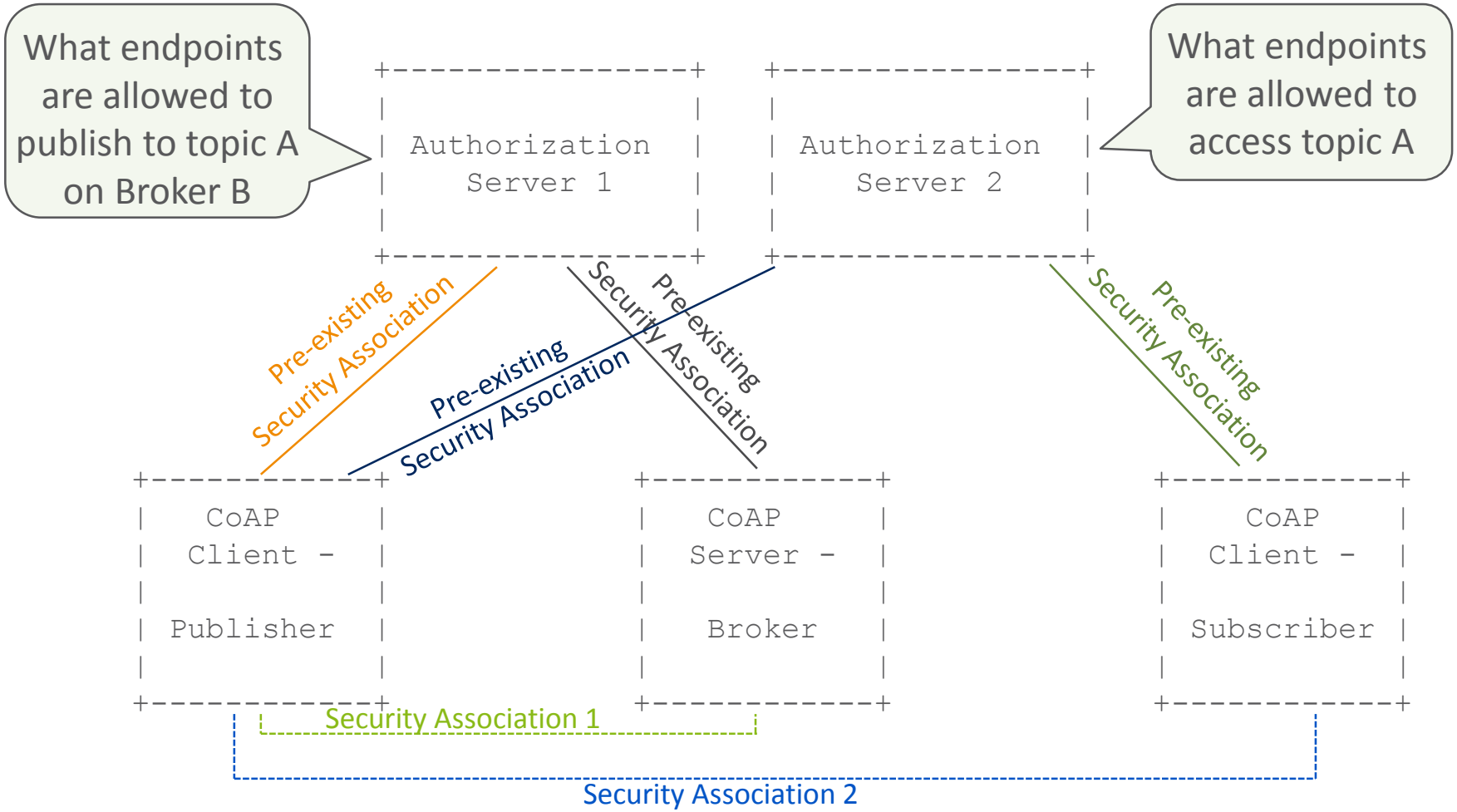


Figure 1: CoAP pubsub Architecture

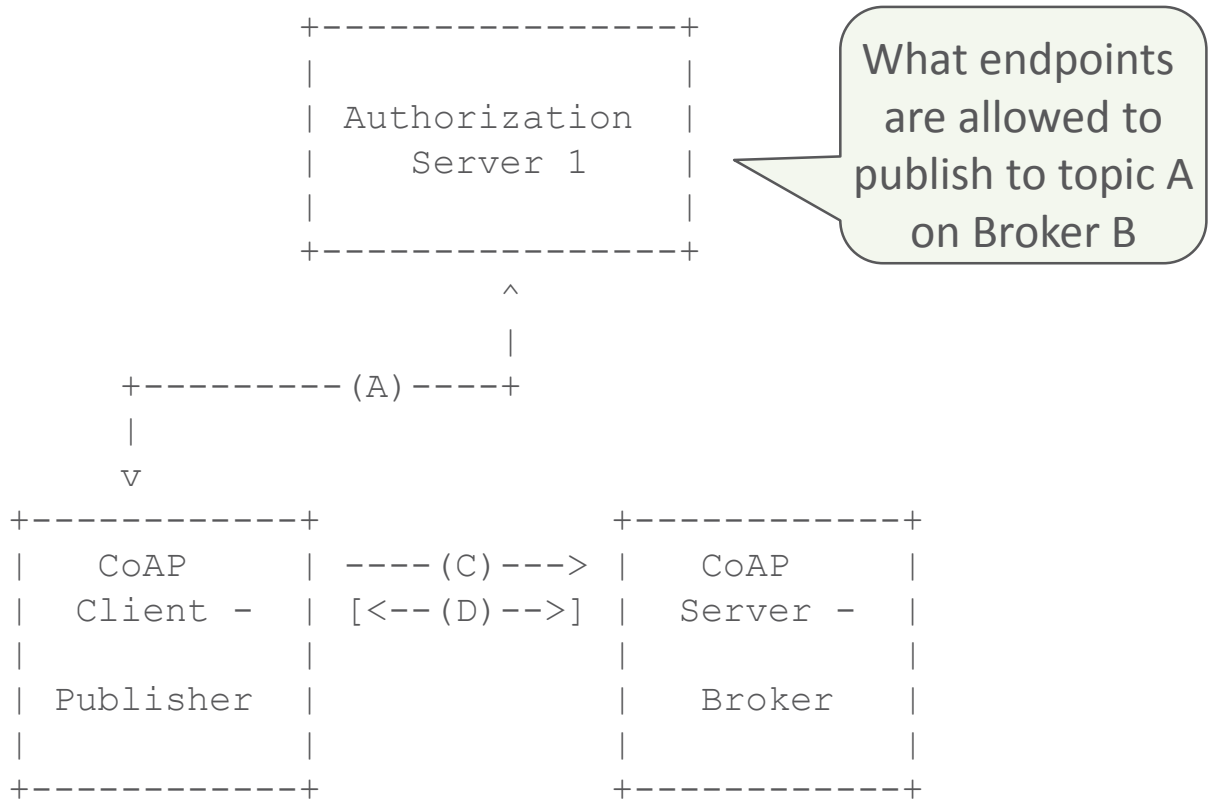
Architecture CoAP PubSub with Authorization Servers

› draft-palombini-ace-coap-pubsub



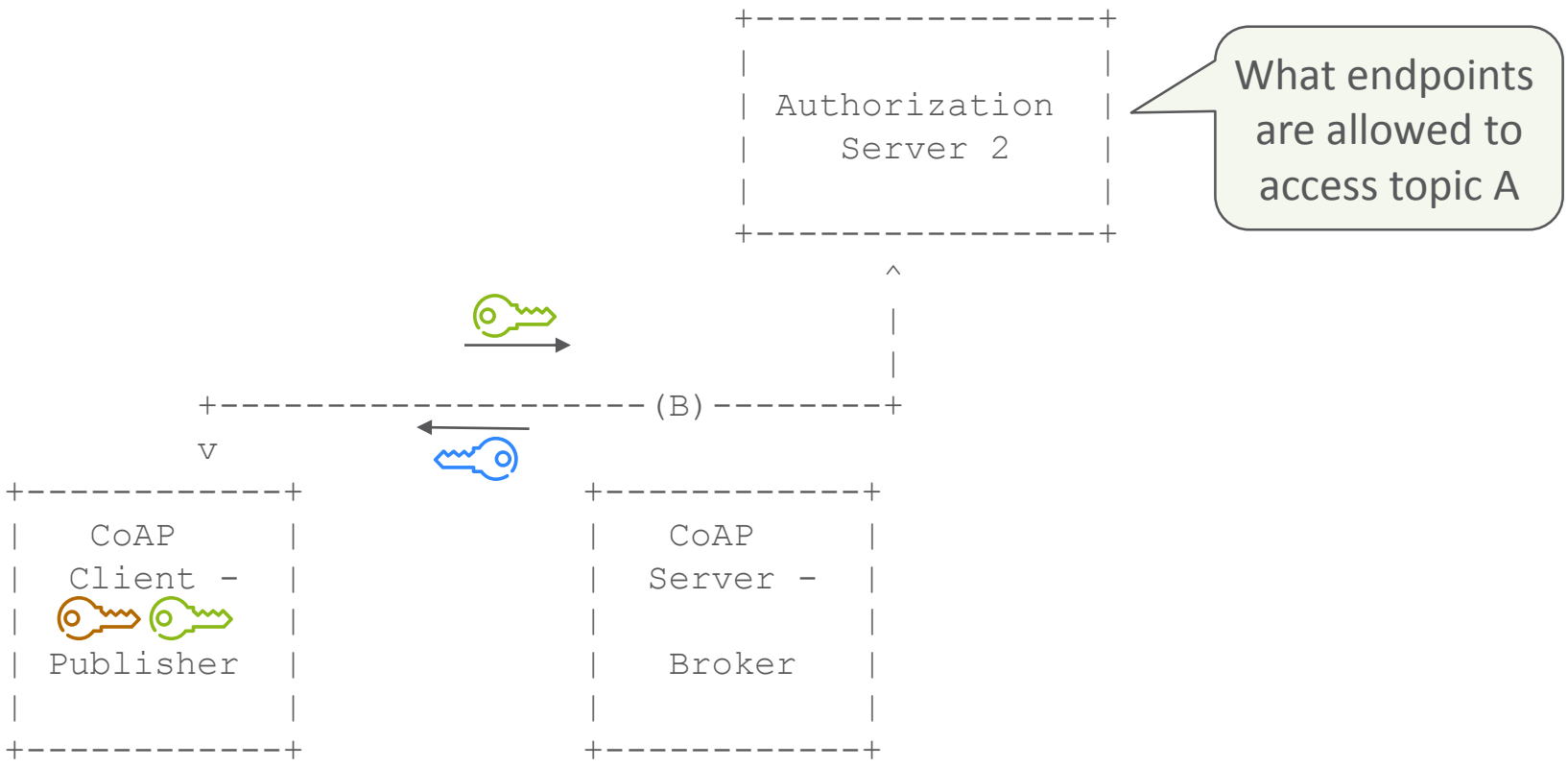
Publisher Profile – Phase 1

- Use DTLS or OSCOAP profile to establish secure communication between Publisher and Broker



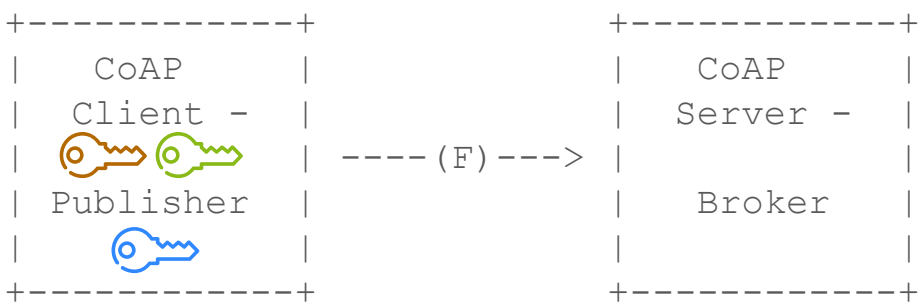
Publisher Profile – Phase 2

- Use ACE token-less exchange to retrieve symmetric keying material (🔑)
- Send AS2 its own public key (🔑) corresponding to its private key (🔑)



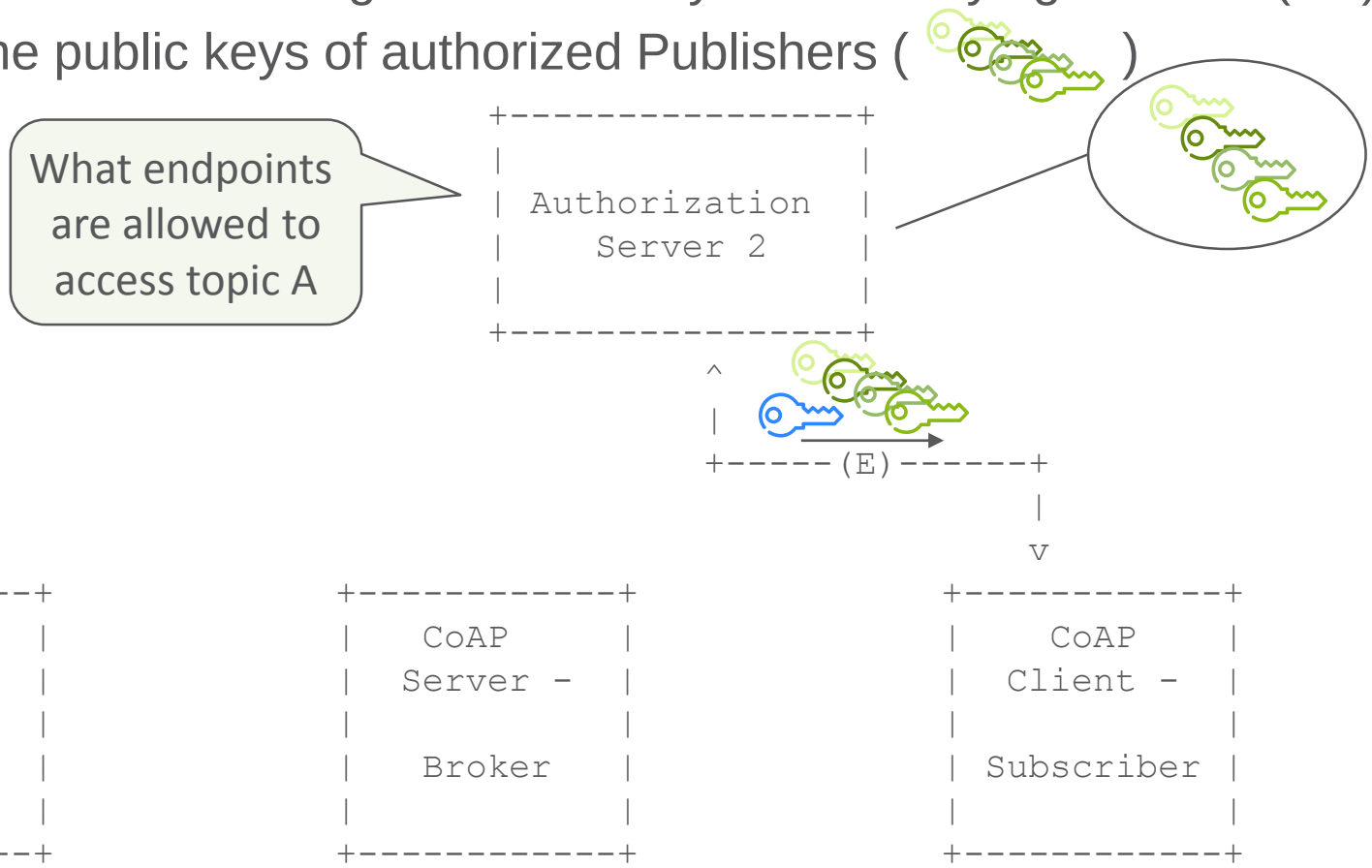
Publisher Profile – Phase 3

- The CoAP payload of the publication is wrapped in a COSE_Encrypt0 object ( )
- The COSE_Encrypt0 object includes a countersignature ( )



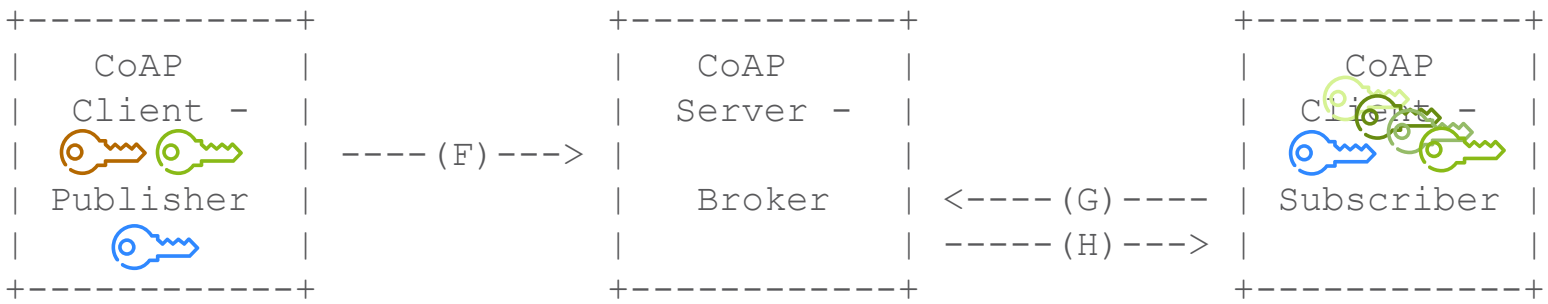
Subscriber Profile – Phase 1

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



Using COSE Object to protect the resource representation

- The CoAP payload of the publication is wrapped in a COSE_Encrypt0 object ( )
- The COSE_Encrypt0 object includes a countersignature ( )
- The subscriber decrypts ( ) and verifies the signature ( ) according to COSE



Main Features

- AS1 has control over the broker (who can publish to a certain topic)
- AS2 has control over the topic (who can read the publication)
- Everybody is allowed to subscribe, not everyone is allowed to publish or read the publication
- Subscribers need to know the public keys of all authorized publishers, plus the symmetric key of a topic
- Publishers only need to know the symmetric key
- The Broker is only trusted with verifying that the Publisher is authorized to publish (access token), but is not trusted with the publications itself, which it cannot read nor modify

Notes

- Leaving the group can be done with rekeying, how that is done is out of scope for this draft
- If you want more control over who is allowed to subscribe to a topic, you can add a ACE exchange between subscriber and broker
- Symmetric only can be done, but then any authenticated subscriber colluding with the broker could forge publications

Thank you!

Comments/questions?

https://ericssonresearch.github.io/coap-pubsub-profile