Key Provisioning for Group Communication using ACE

draft-ietf-ace-key-groupcomm-10

Francesca Palombini, Ericsson
Marco Tiloca, RISE

ACE WG, IETF 109, November 18, 2020

Quick Recap

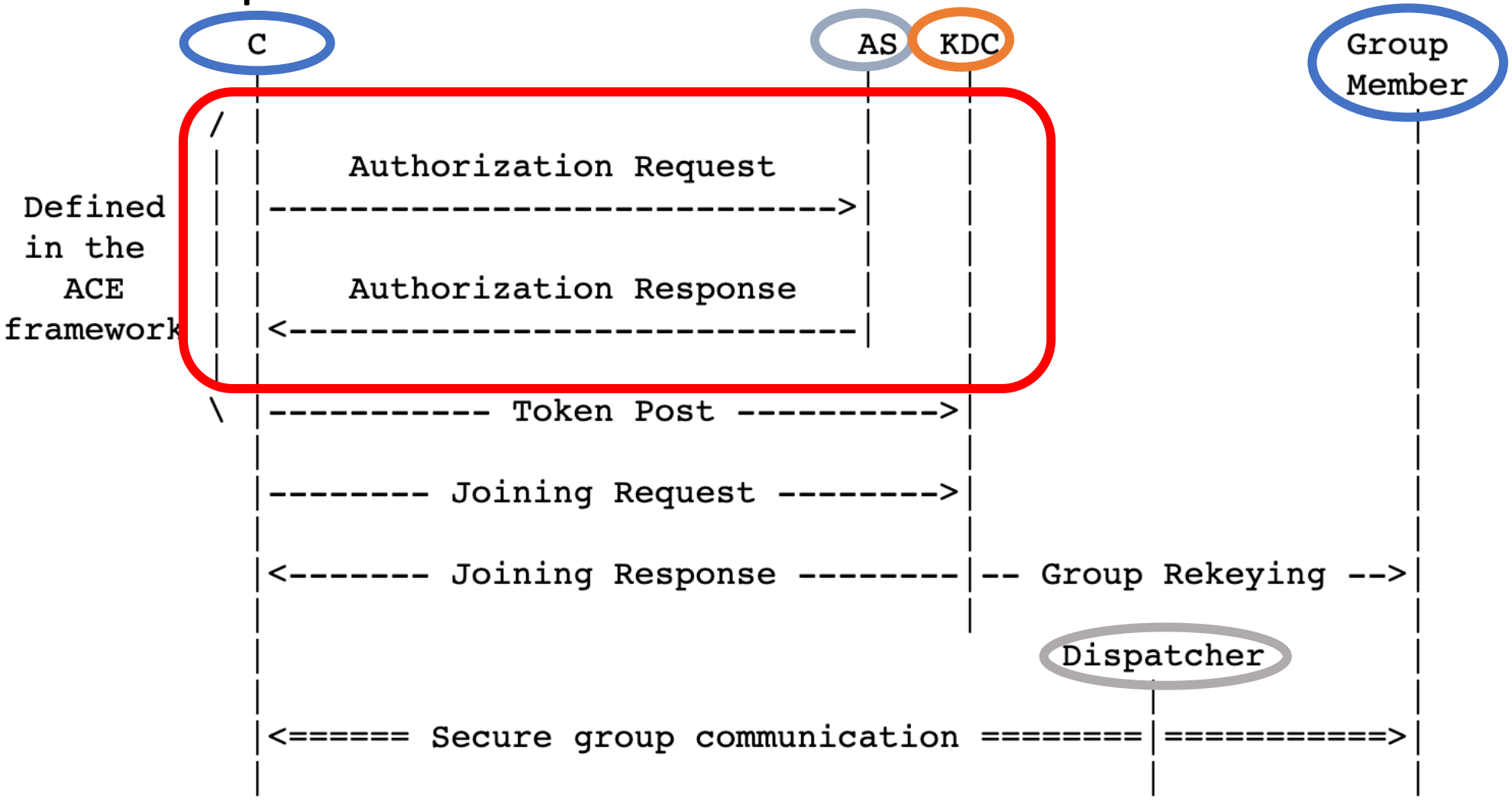
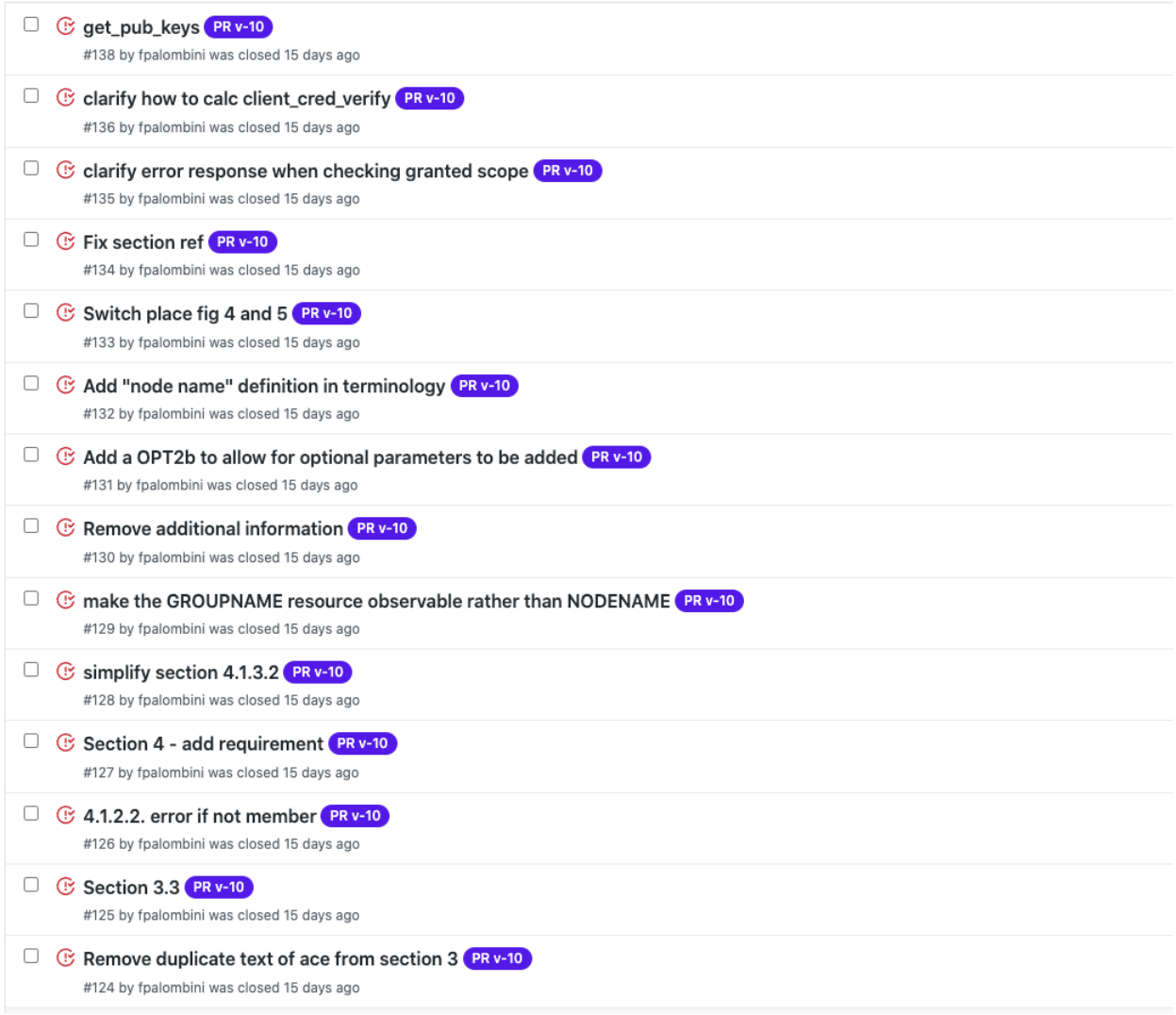


Figure 2: Message Flow Upon New Node's Joining

What happened since IETF 108



- Version -09 was submitted:
  - Based on a follow up review from Jim (as discussed at IETF 108): https://mailarchive.ietf.org/arch/msg/ace/r6ikostngv7h-SysA2WouLJEErs/
  - Details at: https://github.com/ace-wg/ace-key-groupcomm/pull/122

- Version -10 was submitted:
  - Based on a review from Christian: https://mailarchive.ietf.org/arch/msg/ace/q03pyqFHFT4CpdsckLLlifPB3w0/
  - Details at: https://github.com/ace-wg/ace-key-groupcomm/pull/139

V-10 Updates

(Hopefully) made it easier for implementers:

- Added CoAP message examples for all exchanges
- Add example for input to signature
- Remove duplicate text from framework
- Remove duplicate text from other sections of the doc
- Modified error code if not member from 4.00 to 4.01
- Clarifications

Issue - Scope encoding

- KDC acts also as RS for other resources (accessible via other profiles of Ace, such as OSCORE profile)
- C ----> KDC : POST /authz-info with scope encoded as CBOR byte string
- How does the KDC know the format of scope ?
  - How does the KDC know which profile of Ace the RS/KDC is being posted a token for?
  - Etc: for ace-key-groupcomm CBOR array wrapped in a CBOR byte string

/!\ More general problem – valid for RSs supporting several profiles /!

Issue - Scope encoding

2 possible solutions:

- Prefix scope with a byte
  - Needs to be agreed between RS and AS
  - If same scope reused for several RSs, they need to sync with the AS

- Register CBOR tags – one for each different encoding / application profile
  - Longer than the prefix (+1?)
  - Ace key groupcomm OSCORE profile
  - One for each application profile encoding… Is that too much?

- Register a new Token claim that tells you the encoding of scope
  - Same problem as registering CBOR tags

We could describe both: register tags and describe in appendix how either of prefix of tag can be used

Plan forward

- Implement this scope encoding solution
- Other minor clarifications
- Submit v-11
- WGLC