Key Provisioning for Group Communication using ACE

draft-palombini-ace-key-groupcomm-02

+

Key Management for OSCORE Groups in ACE

draft-tiloca-ace-oscoap-joining-05

draft-palombini-ace-key-groupcomm-02 + draft-tiloca-ace-oscoap-joining-05

- First presented at IETF98 / IETF99
- Positive feedback and support from the working group and other SDOs interested in Group Communication (OCF, Fairhair)
- “High priority” during the interim meeting Oct 2017
- Several review comments and feedback (which are included in last versions)
- Ready for working group adoption

Key Provisioning for Group Communication using ACE

draft-palombini-ace-key-groupcomm-02

Francesca Palombini, Ericsson
Marco Tiloca, RISE

IETF 103, Ace WG, Bangkok, Nov 8, 2018

Status Update

- Addressed two detailed reviews from Jim and Peter – Thanks!
- Broader scope: now covering also group rekeying
- Editorial improvements:
  - High-level presentation of message exchange
  - Clarifications and polishing
- Next steps:
  - Define error messages
  - Define request to leave the group
  - Can Observation help for group rekeying?

Key Management for OSCORE Groups in ACE

draft-tiloca-ace-oscoap-joining-05

Marco Tiloca, RISE
Jiye Park, Universität Duisburg-Essen
Francesca Palombini, Ericsson

IETF 103, Ace WG, Bangkok, Nov 8, 2018

Status Update

- Aligned with *draft-palombini-ace-key-groupcomm-02*
- Included group rekeying process
  - Re-use the Join Response as rekeying message (new Section 7)
- Editorial improvements:
  - Overview figure of related documents
  - Overview text for message exchanges
  - Clarifications and polishing
- Next steps:
  - Keep alignment with *draft-palombini-ace-key-groupcomm*

Editor Versions:

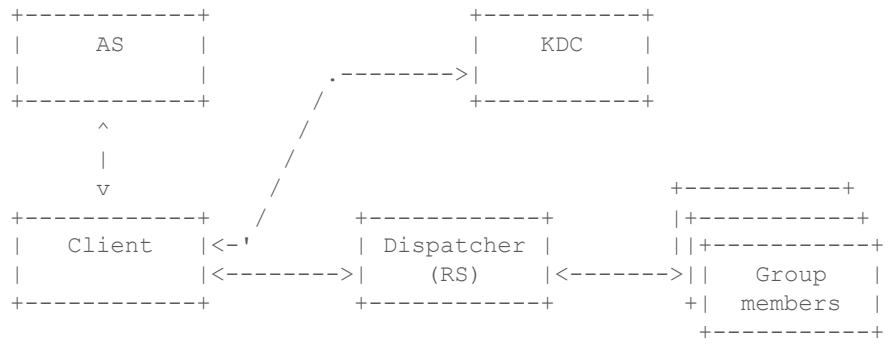
https://github.com/EricssonResearch/ace-key-groupcomm

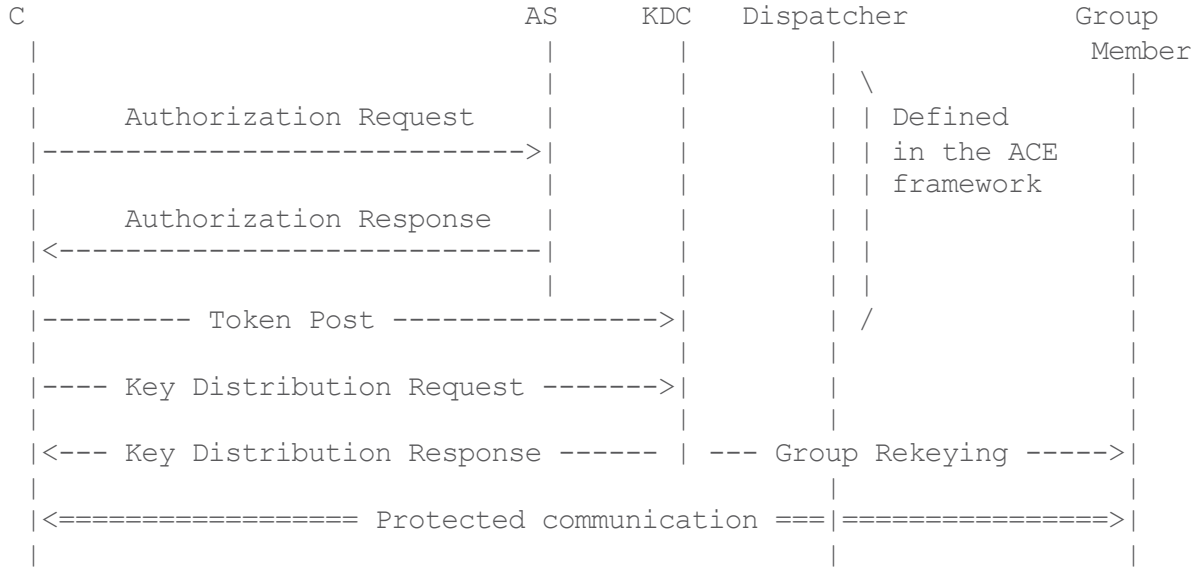
https://gitlab.com/crimson84/draft-tiloca-ace-oscoap-joining

Recap

ace-key-groupcomm

- Message formats and exchanges for:
  - Authorizing to join group communication
  - Providing keying material to joining nodes (clients)
  - Distribute new keying material to the group (rekeying)
  - Use of ACE framework and profiles
- Out of Scope:
  - Group Communication Protection





Recap

ace-oscoap-joining

- Message content and exchanges for:
  - Joining an OSCORE group through its Group Manager (GM)
  - Provisioning keying material to joining nodes and groups (rekeying)
- Use message format and architecture from *ace-key-groupcomm*:
  - Define the content of message fields
  - The GM is the KDC and acts as RS in ACE
  - The GM is the repository of public keys of group members
- Out of Scope:
  - Authorization to access resources at group members
  - Actual secure communication in the OSCORE group