Key Provisioning for Group Communication using ACE

draft-ietf-ace-key-groupcomm-04

Francesca Palombini, Ericsson
Marco Tiloca, RISE

Interim, ACE WG, Feb 25, 2020

Updates since the January interim

- Fixes and editorial improvements – Issues #40 #44 #45 #47#48 #49 #52 #57
- Clarified REQ3 on value of ’cs_alg’ – Issue #50
- Clarified stopping using old keying material – Issue #54
- Different reasons for message processing failures, and related policies – Issue #55
- Possible group rekeying following a request for individual new keying material – Issue #56

Action points from January interim:

- Added ’control_path’ parameter in Joining Request, pointing at a client’s resource (e.g., for rekeying)
- Added sub-resource and handler for uploading a new public key (e.g., if the signature algorithm changes)

TODO left

- Token to cover more than one group/topic at once – Issue #42

- Continue including Peter's review (editorials and clarifications) https://mailarchive.ietf.org/arch/msg/ace/_PDsf5rnGtVw6y3nSQTJun0t7P4

- Continue including Jim's review – Issues #46 #51 #53 https://mailarchive.ietf.org/arch/msg/ace/mR-qwWEhmmOFIVL2ToH5pc2GXqs

Thanks!