Group OSCORE - Secure Group Communication for CoAP

draft-ietf-core-oscore-groupcomm-14

Marco Tiloca, RISE
Göran Selander, Ericsson
Francesca Palombini, Ericsson
John Mattsson, Ericsson
Jiye Park, Universität Duisburg-Essen

IETF 113, CoRE WG, March 25th, 2022
Updates since IETF 112

› Version -14 submitted before the cut-off

› Received and processed two reviews from the 2nd WGLC – Thanks!
  – Esko Dijk
    › Part 1 – Main comments [1]
    › Part 2 – Editorial comments [2]
  – Rikard Höglund – Editorial comments and suggestions for clarifications [3]
    › Comments on the Editor’s Copy already addressing Esko’s review

[1] https://mailarchive.ietf.org/arch/msg/core/7aOZ4YXBI0lvCBOYlHOftDzuCVY/
Updates since IETF 112

Some points from Esko’s review got additional discussion

- Early proposal on the list about how to address them [4], later confirmed
- Selected points discussed and agreed at the CoRE interim in January 2021 [5]
  - Made clear distinction between “authentication credential” and “public key”
  - Added considerations on storing authentication credentials
  - Made optional for the Group Manager to recycle Group IDs
    - Now single, self-contained Section 3.2.1.1, with optional feature and specific approach
    - Related follow-up clarification on the list [6]
  - “Mandatory-to-Implement Compliance Requirements” → “Implementation Compliance”
  - Improved classification of references as Normative or Informative
  - Challenge-response synchronization with the Echo Option moved to the document body

Next steps

› Version -14 addresses the two reviews from the 2nd WGLC

› No further open issues or open points we are aware of

› Ready for the Shepherd write-up
Thank you!

Comments/questions?

https://github.com/core-wg/oscore-groupcomm