Key Management for OSCORE Groups in ACE

draft-ietf-ace-key-groupcomm-oscore-13

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

IETF 113, ACE WG, March 22nd, 2022
Updates since IETF 112

- Most updates triggered by the revision of `draft-ietf-core-oscore-groupcomm`
  - Recycling of Group IDs is now optional to support for the Group Manager
  - Clear distinction between “public key” and “authentication credential”

- Renaming and rephrasing consistent with “public key” vs. “authentication credential”
  - All parameters, structure elements and message exchanges defined in this document
  - E.g.: `gm_dh_pub_keys` → `kdc_dh_creds` ; `pub:key:enc` → `cred_fmt` ; ...

- More items still to be renamed
  - All those defined in `draft-ace-key-groupcomm` and inherited in this document
  - Not changed yet! Will do when processing `draft-ace-key-groupcomm` based on the AD review
Updates since IETF 112

› Revised IANA considerations
  – Updated textual description of the integer registered in “ACE scope semantics”
    › Membership and key management operations at the ACE Group Manager for Group OSCORE
  – Updates triggered by the revision of draft-ietf-ace-aif
    › No need for new media-type; registered two content-formats (1 using CBOR, 1 using JSON)

› Further planned update based on IESG reviews to draft-ietf-ace-aif
  – New text in AIF: The set of numbers is converted into a single number 'REST-method-set' by taking two to the power of each (decremented) method number and computing the inclusive OR of the binary representations of all the power values.
  – Rephrase accordingly as to how to compute the AIF Toid in ‘scope’, to express roles in a group
Summary and next steps

› Version -13 is stable and aligned to draft-ietf-core-oscore-groupcomm-14

› Just got a WGLC review from Göran – Thanks!
  – https://mailarchive.ietf.org/arch/msg/ace/SIB_rte0orqkvDEtTAw-1F7Cdzo/

› Plan for next version -14
  – Address WGLC from Göran – More comments are expected afterwards
  – Align to draft-ietf-ace-key-groupcomm, based on the AD review

› Input from Francesca (CoRE AD): Please request publication in synch with
  – draft-ietf-core-groupcomm-bis  // Expected to start WG Last Call
  – draft-ietf-core-oscore-groupcomm  // Expected to start Shepherd write-up

Note: draft-ietf-core-oscore-groupcomm has completed the 2nd WGLC
  – However, changes on it might still affect this document in the future
Thank you!

https://github.com/ace-wg/ace-key-groupcomm-oscore