Key Management for OSCORE Groups in ACE

draft-ietf-ace-key-groupcomm-oscore-12

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

IETF 112, ACE WG, November 9th, 2021
Updates since IETF 111

› Updates triggered by the revision of draft-ietf-ace-key-groupcomm
  – No changes were triggered by Groupo OSCORE, i.e. draft-ietf-core-oscore-groupcomm

› Moved to draft-ietf-ace-key-groupcomm
  – Definition of parameters 'kdc_nonce', 'kdc_cred' and 'kdc_cred_verify'
  – Definition of the resource /ace-group/GROUPNAME/kdc-pub-key

› Alignment to draft-ietf-ace-key-groupcomm
  – Consistent use of "Token Transfer Request" and "Token Transfer Response"
  – Use of the new parameter 'rekeying_scheme'
  – Categorization of newly defined operations
  – Categorization of new parameters and inherited conditional parameters
  – Public keys of just joined Clients can be in rekeying messages
  – Revised appendix with addressed profile requirements
Updates since IETF 111

› Clarifications and refinements
  – Definition of parameters 'ecdh_info' and 'gm_dh_pub_keys'
    › Consistent with 'sign_info' from ace-key-groupcomm
  – Access to the resource ace-group/
  – What resources are accessible to Verifiers
  – Error handling
    › Defined for the new resources defined in this document
    › Proper use of CoAP error codes
    › What to do in case of enhanced error responses
  – IANA considerations
    › Meaning of registered CoRE resource type
    › Revised names of new IANA registries
  – Changed UCCS to CCS, i.e., CWT Claims Set
Summary and next steps

› Version -12 is stable and aligned to:
  – draft-ietf-ace-key-groupcomm-14
  – draft-ietf-core-oscore-groupcomm-13 // Group OSCORE @ CoRE WG

› Implementation for Eclipse Californium
  – Support for OSCORE groups using the group mode and the pairwise mode
  – https://bitbucket.org/marco-tiloca-sics/ace-java/

› No further issues or open points are known

› Ready for WGLC ?

› Note: Group OSCORE in the CoRE WG is stable and will go through a 2nd WGLC
  – However, it might still affect document altogether
Thank you!

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