Work in progress towards

Key Provisioning for Group Communication using ACE

draft-ietf-ace-key-groupcomm-14

Francesca Palombini, Ericsson
Marco Tiloca, RISE

ACE WG Interim Meeting, October 12th, 2021

What is going on

- **Working on the two WGLC reviews**
  - Göran [1a] – Responses at [1b][1c]
  - Cigdem [2a] – Response at [2b]

- **Required changes split into three categories**
  - Editorial/nits DONE
  - Clarifications ALMOST DONE
  - Design changes DONE (?)

[1a] https://mailarchive.ietf.org/arch/msg/ace/pr2gBhvqy9j8AfUdQVTZLwamXac/
[1b] https://mailarchive.ietf.org/arch/msg/ace/dEU04pB3u-iYNBwSlfjJaqkEvgo/
[1c] https://mailarchive.ietf.org/arch/msg/ace/Yo2T3febqosQJ94qcVxo9YaR1nc/
[2a] https://mailarchive.ietf.org/arch/msg/ace/gv_uRo2Y45jqOLJghVSbAARWky0/
[2b] https://mailarchive.ietf.org/arch/msg/ace/IL72zPmsIgF2j0Bgm7zO2fUTEm8/

Selected clarifications (1/2)

- **General**
  - Early definition of "group" as security group
  - Format/encoding of scope in Token Request/Response and token
- **Token transferring to the KDC**
  - Fixed ambiguity of "POST /token" and "Token POST“
  - Semantics of request/response to/from /authz-info
  - Early explanation of what 'kdcchallenge' is intended for
  - Semantics of 'sign_info' and 'get_pub_keys'
- **Joining process**
  - Approaches for early knowledge of group configuration
  - Association between public key and (NODENAME, GROUPNAME, token)
  - More details in case of of re-joining
  - More details on 'control_uri' and 'group_policies‘
  - Example of administrative keying material transported in 'mgt_key_material'

Selected clarifications (2/2)

- **Revised presentation of KDC interface**
  - Overview, operations and error handling
  - Resource 1: handler 1 and example; handler 2 and example; ...
  - Resource 2: handler 1 and example; handler 2 and example; ...
  - ...

- **Error handling**
  - Revised use of CoAP error codes
  - Common checks and actions collected in a single early section
  - Resource-specific checks that are common to all handlers are mentioned ASAP

- **And many more editorial improvements …**

Design changes (1/3)

- **New parameters**
  - Imported from *key-groupcomm-oscore* : 'kdc_nonce', 'kdc_cred', 'kdc_cred_verify'
    - Potentially relevant to all profiles, e.g., due to signed one-to-many rekeying messages
  - Brand new parameters 'group_rekeying_scheme' and 'control_group_uri'
    - Intended especially, but not only, to support advanced rekeying schemes (e.g., over multicast)
    - New IANA registry for values of 'group_rekeying_scheme'
    - 'group_rekeying_scheme' = 0 is the basic point-to-point rekeying scheme

- **New resource ace-group/GROUPNAME/kdc_pub_key**
  - Imported from *key-groupcomm-oscore*
  - Used to retrieve the KDC's public key as group member

Design changes (2/3)

- **Reasoned categorization of parameters – Expected support by ACE Clients**
  - MUST/SHOULD/MAY support categories; profiles may upgrade requirements to be stricter
  - Some are "conditional to support"; a profile must say if they are MUST/SHOULD/MAY to support
  - Profiles must categorize possible new parameters accordingly

- **Guidelines on enhanced error responses, with ‘error’ and ‘error_description’**
  - Expected reaction from ACE Clients supporting these error responses
  - No need to use ‘error_description’ if no human intervention is expected

- **Reasoned categorization of KDC functionalities**
  - What is minimally supported by ACE Clients (primary operations)
  - What can be additionally supported by ACE Clients (secondary operations)
  - Profiles must categorize possible new functionalities accordingly
  - Profiles must say if the KDC does not provide some of these functionalities

Design changes (3/3)

- **Considerations and discussion on group rekeying and possible approaches**
  - All in a dedicated new Section 6 “Group Rekeying Process”
  - Minimal ACE Groupcomm parameters to be included
  - Public keys of about-to-join new members can be provided in a rekeying done upon their joining
  - Presented relevant approaches at a high-level
    - (A) Point-to-point, possibly aided by CoAP Observe, with practical recommendations
    - (B) Based on separate pub-sub rekeying topics
    - (C) Based on one-to-many messages sent over multicast
    - For (B)(C), proposal of message protection using COSE and administrative keying material

- **(B)(C): details expected from separate specifications profiling the group rekeying scheme**

- **This new Section 6 needs a good re-review!**

New requirements

- **Mandatory-to-address requirements**
  - REQ2 : registration of “Toid” and “Tperm” if AIF-based scopes are used
  - REQ8 : define if the KDC has a public key to be provided with ‘kdc_cred’
  - REQ9 : specify if part of the KDC interface is not supported
  - REQ12: categorize possible new operations as primary or secondary for ACE Clients
  - REQ21: specify approaches to compute/verify the PoP evidence for the KDC’s public key
  - REQ29: categorize possible new parameters as MUST/SHOULD/MAY be supported by ACE Clients
  - REQ30: define if conditional parameters from this document MUST/SHOULD/MAY be supported

- **Optional-to-address requirements**
  - OPT9 : define a default group rekeying scheme for ACE Client to consider
  - OPT10: specify functionalities implemented at ‘control_group_uri’
  - OPT14: specify any additional parameters to include in a “Point-to-Point” rekeying message
  - OPT15: specify if option parameters from this document MUST/SHOULD be supported

- Note: the numbering might change!

Next steps

- Finish addressing the WGLC comments
  - All points should be covered (have to double check); need to harmonize & polish
- Some more clarifications from IETF 111
  - Clarify scope and goal of this document within the ACE Groupcomm landscape
  - Clarify trust in the KDC and related security assumption

Editor's copy: https://ace-wg.github.io/ace-key-groupcomm/draft-ietf-ace-key-groupcomm.html

- Submit version -14 before the cut-off

- Related: align *key-groupcomm-oscore* to this document (already ongoing)

Thank you!