Admin Interface for the OSCORE Group Manager

draft-ietf-ace-oscore-gm-admin-08

Marco Tiloca, RISE
Rikard Höglund, RISE
Peter van der Stok
Francesca Palombini, Ericsson

IETF 116 meeting – Yokohama – March 30th, 2023
Recap

› **RESTful admin interface at the OSCORE Group Manager**
  – Create, (re-)configure and delete OSCORE groups
  – Support for both: i) Link Format and CBOR ; ii) CoRAL

› **Two new types of resources at the Group Manager**
  – A **single group-collection** resource, at /manage
  – One **group-configuration** resource per group, at /manage/GROUPNAME

› **Using ACE for authentication and authorization**
  – The Administrator is the Client
  – The Group Manager is the Resource Server
  – For secure communication, use transport profiles of ACE
Since IETF 115

› Ongoing work presented during two ACE interim meetings
  – On 2023-01-23 and 2023-02-20

› Version -08 submitted before the cut-off
  – This addresses most points discussed during the interim meetings

› Agreed to do a document split, taking out the content about CoRAL [1]
  – Details in a following slide

[1] draft-ietf-core-coral
Update summary

› Added discussion on multiple, concurrent Administrators (Section 4.1)

› Specified atomicity of write operations at the Group Manager
   – Upon creating/overwriting/updating/deleting a group-configuration resource

› Clarified effects of configuration overwriting/updating on group members
   – The possible retrieval of other group members’ public keys should not be “rushed”

› Reasons for the Group Manager to deviate from the recommended default values
   – E.g., the Group Manager does not support those

› New ACE Groupcomm Error "Unsupported group configuration"
   – Guidelines for the Administrator on how to react to that (Section 8)
   – IANA registration (Section 10.2)
Update summary

› **Use of CoRAL [1]**
  – More details on the format of message payloads and on interaction semantics
  – Revised all the examples of message exchange with CoRAL (Section 6)
    › Now written in CBOR diagnostic notation
    › Using Packed CBOR [2] (shared item tables are in Appendix B)

› **Added more security considerations, related to:**
  – Overwriting/update of group configurations
  – The Group Manager
  – The Administrators

› **Clarifications**
  – Consistency of parameter names
  – Slight content reordering in Sections 3 and 4
  – Various editorial improvements

[1] draft-ietf-core-coral
[2] draft-ietf-cbor-packed
Pending document split

› Rationale and plan
   – Avoid delays due to the progress of draft-ietf-core-coral
   – Doc 1: current document minus the CoRAL-related content (use, special features, examples, ...)
   – Doc 2: new WG document, with revised CoRAL-related content taken out of this ACE document

› History
   – Proposal made at the 2023-01-23 ACE interim meeting [1] – No objection
   – Checked and confirmed on the ACE mailing list [2] – No objection
   – Further confirmed at the 2023-02-20 ACE interim meeting [3]
     › Agreed to do the split after IETF 116
     › Agreed name for Doc 2: draft-ietf-ace-oscore-gm-admin-coral

Next steps

› Do the document split
  – Create Doc 2 from draft-ietf-ace-oscore-gm-admin-08
  – The split is not straightforward: the CoRAL content is well blended

› Submit Doc 2 as draft-ietf-ace-oscore-gm-admin-coral-00
  – Expected only simple, consistency updates until draft-ietf-core-coral is close to completion
  – Note: Doc 2 is not intended to Obsolete or Update the upcoming Doc 1

› Polish and overall revise the resulting Doc 1, in particular:
  – Consistency of content presentation, following the removal of the CoRAL-related parts
  – Review examples (e.g., use of double quotes in message payloads in Link-Format)
  – Double-check and ensure consistency with other related documents in ACE and CoRE

› Submit Doc 1 as draft-ietf-ace-oscore-gm-admin-09
  – If no issues remain, version -09 might be ready for WG Last Call
Thank you!

Comments/questions?

https://github.com/ace-wg/ace-oscore-gm-admin
Overview

**Group-collection resource**
- Retrieve the list of OSCORE groups
  - All groups (GET)
  - Group selected by filters (FETCH)
- Create a new OSCORE group (POST)
  - A group-configuration resource is created
  - A group-membership for joining nodes is also created, see *draft-ietf-ace-key-groupcomm-oscore*

**Configuration Properties**
- Security algorithms and parameters

**Status Properties**
- Any other information (e.g., group name)

**Group-configuration resource**
- Retrieve the group configuration (GET)
- Retrieve part of the group configuration (FETCH)
- Overwrite the group configuration (PUT)
- Update the group configuration (PATCH/iPATCH)
- Delete the group (DELETE)

Figure 1: Resources of a Group Manager