Alternative Workflow and OAuth Parameters for the Authentication and Authorization for Constrained Environments (ACE) Framework

draft-tiloca-ace-workflow-and-params-01

Marco Tiloca, RISE
Göran Selander, Ericsson

IETF 118 Meeting – Prague – November 10th, 2023
Proposed twofold update to RFC 9200

1. Define an alternative workflow for uploading the access token (Unchanged since v -00)
   - The AS uploads the access token to the RS, on behalf of C
   - Preferable if the C-RS communication leg is constrained, while the AS-RS leg is not

2. Define additional OAuth parameters to use in ACE
   - One new parameter, to enable the alternative workflow above
   - New parameters, for effectively enabling the issue of an access token for a group-audience

Early ideas shared during the ACE session at IETF 116; v -00 well received at IETF 117
Alternative workflow (as in v-00)

› (A) C-to-AS Token Request as usual

› (A1) The AS uploads the access token to RS, on behalf of C
  – No plan to replace the original workflow!
  – The AS can dynamically choose the workflow to use, e.g., based on the RS

› (A2) The AS receives a response from RS

› (B) AS-to-C Token Response
  – New parameter “token_uploaded” (CBOR simple value)
  – True = successful upload → access token not included in the Token Response → C skips step C1
  – False = failed upload → access token included in the Token Response → C performs step C1
New parameters

▶ “token_uploaded” – **Specific** for the alternative workflow (Unchanged since v -00)
  – For the AS-to-C response; CBOR simple value “true” (0xf5) of “false” (0xf4)
  – It MUST be present if and only if the AS attempted to upload the access token to RS
  – If the parameter is “true”, the access token MUST NOT be present, otherwise it MUST

▶ Three more parameters – **Independent** of the specifically used workflow
  – “rs_cnf2”, “aud2” (*), and “anchor_cnf” (**)
  – All for the AS-to-C response
  – Possible to use when
    › The access token is issued for a group-audience; and
    › Public authentication credentials are used for the RSs

* It replaces “subject_ids” from v -00, with a different semantics
** New addition in v -01
“rs_cnf2” and “aud2”

“rs_cnf2” (Unchanged since v-00)
- Structured version of “rs_cnf” (RFC 9201)
- Non-empty CBOR array
- Each element is the public authentication credential of a RS in the group-audience (same semantics of the “cnf” claim)
- Not required that each element has the same semantics

“aud2” (NEW)
- Non-empty CBOR array of text strings
- General meaning: identifiers of the RSs in the group-audience
  - Each element is the identifier that C would use in the “aud” parameter to request an access token for that RS
  - If “rs_cnf2” is present, then “aud2” MUST be present
    - Same number of elements as in “rs_cnf2”
    - i-th element paired with the i-th element of “rs_cnf2”

2.01 Created
Content-Format: application/ace+cbor
Max-Age: 3600
Payload:

```json
"rs_cnf2": {
  "COSE_Key": {
    "kty": 2,
    "crv": 1,
    "x": "h'bcb34960526e4d32e940cad2a234148ddc21791a12afbcbac93e22046idd44f0',
    "y": "h'4519e257236b2a0ce2023ef0931f1f386ca7afda64fcd6c0185c5eabf6072'
  }
},
"COSE_Key": {
  "kty": 2,
  "crv": 1,
  "x": "h'ac75e9ece3e50bfc8ed60399889522405c47bf16df96660a41298cb4307f7eb6',
  "y": "h'e6de611388a4b8a8211334ac7d37ecb52a387d257e6db3c2a93df21ff3affc8'
}
"aud2": ["rs1", "rs2"]
```

AS-to-C Token Response
“anchor_cnf”

“anchor_cnf” (NEW)

- Non-empty CBOR array
- Each element is the public authentication credential of a trust anchor (same semantics of the “cnf” claim)
- Not required that each element has the same semantics

Way of use

- Separately through other means, C obtains CRED, i.e., the public authentication credential of an RS
- C uses CRED only if successfully validated through any public authentication credential in “anchor_cnf”
- If the AS-to-C Token Response also includes “aud2”, then ...
  - CRED has to be associated with one of the RSs in “aud2”

Smaller overhead compared to using “rs_cnf2”

- It also suits RSs deployed after the access token is issued
Summary and next steps

› As a way forward, consider early proposals compiled in Appendix B

  – On the alternative workflow
    › Allow its use for any profile of ACE
    › Allow the dynamic update of access rights
    › Allow a re-posting of the same access token

  – Possible definition of some more parameters
    › Some specific for the alternative workflow, some independent of the used workflow

› The alternative workflow is considered in draft-ietf-ace-edhoc-oscore-profile

  – That document also benefits of “rs_cnf2”, “aud2”, and “anchor_cnf”

› WG Adoption Call?

  – Pending since IETF 117, where v -00 was presented
Thank you!

Comments/questions?

https://gitlab.com/crimson84/draft-tiloca-ace-workflow-and-params
Backup
The ACE framework considers a single execution workflow
- The Client (C) requests an access token from the Authorization Server (AS)
- Then C uploads the access token to the Resource Server (RS)

In some deployments, this is not ideal
- The C-RS communication leg might be constrained, while the AS-RS leg is not

The AS can issue a single access token for a “group-audience” (Section 6.9 of RFC 9200)
- The group-audience includes multiple RSs intended to consume the access token
- Possible when using asymmetric authentication credentials (e.g., “RPK mode” of RFC 9202)

Practical limitation
- The AS-to-C Token Response cannot include the authentication credentials of multiple RSs
- The “rs_cnf” parameter can specify only one authentication credential
Examples with alternative workflow

Example 1: the AS successfully uploaded the access token

---

Example 2: the AS attempted to upload the access token but failed

---