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

draft-tiloca-ace-workflow-and-params-00

Marco Tiloca, RISE
Göran Selander, Ericsson

IETF 117 Meeting – San Francisco – July 24th, 2023
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
Contribution

- Proposed update to RFC 9200
  - Twofold update, addressing the two limitations in the previous slide

1. Define an alternative workflow for uploading the access token
   - The AS uploads the access token to the RS, on behalf of C

2. Define additional OAuth parameters to use in ACE
   - One new parameter, to enable the alternative workflow above
   - Two 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
(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 $\rightarrow$ access token not included in the Token Response $\rightarrow$ C skips step C1
  - False = failed upload $\rightarrow$ access token included in the Token Response $\rightarrow$ C performs step C1
Examples with alternative workflow

Example 1: the AS successfully uploaded the access token

```
2.01 Created
Content-Format: application/ace+cbor
Max-Age: 3560
Payload:
{
  "token_uploaded": true,
  "expires_in": 3600,
  "cnf": {
    "COSE_Key": {
      "kty": 1,
      "kid": "h'3d027833fc6267ce'",
      "k": "h'73657373696f6e6b6579'"
    }
  }
}
```

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

```
2.01 Created
Content-Format: application/ace+cbor
Max-Age: 3560
Payload:
{
  "access_token": "h'd08343a1'/..."
  (remainder of CWT omitted for brevity;
  CWT contains the symmetric PoP key in the "cnf" claim)/,
  "token_uploaded": false,
  "expires_in": 3600,
  "cnf": {
    "COSE_Key": {
      "kty": 1,
      "kid": "h'3d027833fc6267ce'",
      "k": "h'73657373696f6e6b6579'"
    }
  }
}
```
New parameters

› “token_uploaded” – Specific for the alternative workflow
  – 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

› Two more parameters – Independent of the specifically used workflow
  – “rs_cnf2” and “subject_ids”
  – Both 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
“rs_cnf2” and “subject_ids”

“rs_cnf2”
- 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

“subject_ids”
- Non-empty CBOR array
- MUST be present if and only if “rs_cnf2” is present
- Same number of elements as in “rs_cnf2”
- i-th element paired with the i-th element of “rs_cnf2”
- Each element identifies the i-th RS, as:
  - An absolute URI (RFC 3986) or an absolute CRI reference (draft-ietf-core-href), with only scheme and authority
Next steps

› Build on the open points and early proposals compiled in Appendix B

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

› Consider to define some more parameters
  – Some specific for the alternative workflow
  – Some independent of the used workflow

› Comments and feedback are welcome!
Thank you!

Comments/questions?

https://gitlab.com/crimson84/draft-tiloca-ace-workflow-and-params