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

Recap

› **Proposed twofold update to RFC 9200**

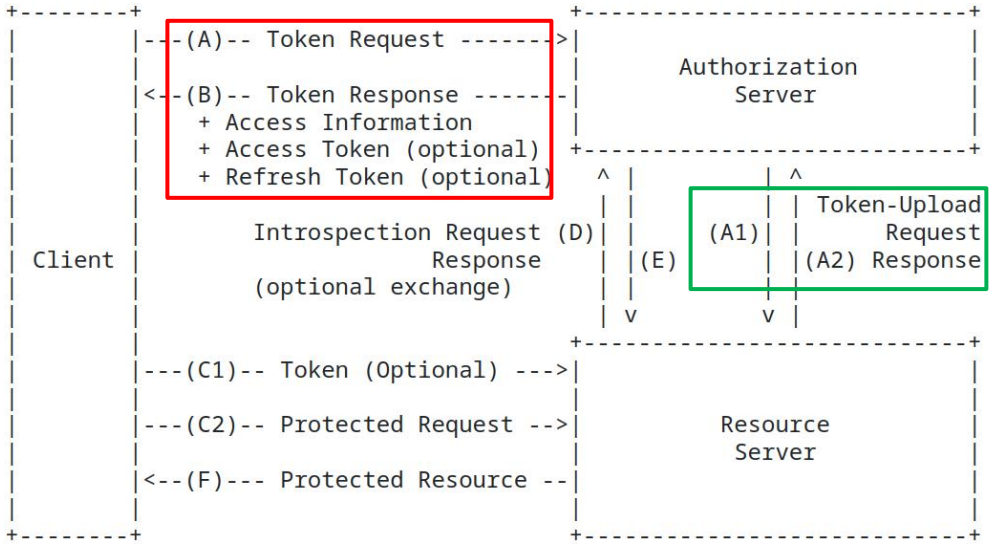
1. **Define an alternative workflow for uploading the access token (Unchanged since v -00)**
   - The AS uploads the access token to the RS, on behalf of C
   - Preferable if the C-RS communication leg is constrained, while the AS-RS leg is not

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:
{
  "access_token" : b64'S1AV32hk'/...
   (remainder of CWT omitted for brevity;
   CWT contains the client's RPK in the "cnf" claim)/,
  "expires_in" : 3600,
  "rs_cnf2" : [
    {
      "COSE_Key" : {
        "kty" : 2,
        "crv" : 1,
        "x" : h'bbc34960526ea4d32e940cad2a234148
                 ddc21791a12afbcbac93622046dd44f0',
        "y" : h'4519e257236b2a0ce2023f0931f1f386
                 ca7afda64fcde0108c224c51eabf6072'
      }
    },
    {
      "COSE_Key" : {
        "kty" : 2,
        "crv" : 1,
        "x" : h'ac75e9ece3e50bfc8ed6039988952240
                 5c47bf16df96660a41298cb4307f7eb6',
        "y" : h'6e5de611388a4b8a8211334ac7d37ecb
                 52a387d257e6db3c2a93df21ff3affc8'
      }
    }
  ],
  "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

```
2.01 Created
Content-Format: application/ace+cbor
Max-Age: 3600
Payload:
{
  "access_token" : b64'SlAV32hk'/...
   (remainder of CWT omitted for brevity;
   CWT contains the client's RPK in the "cnf" claim)/,
  "expires_in" : 3600,
  "anchor_cnf" : [
    {
      "x5chain" : h'308201363081dea003020102020301f50d30
                    0a06082a8648ce3d0403023016311430120 6
                    035504030c0b524643207465737420434130
                    1e170d3230303130313030303030305a170d
                    3231303230323030303030305a3022312030
                    1e06035504030c1730312d32332d34352d46
                    462d46452d36372d38392d41423059301306
                    072a8648ce3d020106082a8648ce3d030107
                    03420004b1216ab96e5b3b3340f5bdf02e69
                    3f16213a04525ed44450b1019c2dfd3838ab
                    ac4e14d86c0983ed5e9eef2448c6861cc406
                    547177e6026030d051f7792ac206a30f300d
                    300b0603551d0f040403020780300a06082a
                    8648ce3d0403020347003044022044 5d798c
                    90e7f500dc747a654cec6cfa6f037276e14e
                    52ed07fc16294c84660d02205a33985dfbd4
                    bfdd6d4acf3804c3d46ebf3b7fa62640674f
                    c0354fa056dbaea6'
    }
  ]
}
```

AS-to-C Token Response

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

Motivation

- **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

```
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 1: the AS successfully uploaded the access token

```
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'
    }
  }
}
```

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