

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

*draft-ietf-ace-workflow-and-params-01*

**Marco Tiloca**, RISE  
Göran Selander, Ericsson

IETF 119 Meeting – Brisbane – March 19<sup>th</sup>, 2024

# Recap

## › Updates to RFC 9200, mostly about two points

### 1. Define an alternative workflow for uploading the access token

- 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

## › Since IETF 118

- The draft was adopted as a WG document
- This version -01 was submitted before the IETF 119 cut-off

# Updates in v -01 (1/4)

## › Simple updates

- Editorial fixes and readability improvements
- Clarifications on the use of the new parameters in the ACE messages
- Added security considerations inherited from other documents

## › Term “token series” moved up to Section 1.1 “Terminology”

- *Token series: the set comprising all the access tokens issued by the same AS for the same pair (Client, Resource Server).*

*Profiles of ACE can provide their extended and specialized definition, e.g., by further taking into account the public authentication credentials of C and the RS.*

- More visible and easier to find for other profiles of ACE
  - › E.g., *draft-ietf-ace-edhoc-oscore-profile* uses and specializes this concept

# Updates in v -01 (2/4)

## › On the new ACE parameters

- “token\_uploaded” → “token\_upload”, due to updated semantics (see below)
- No changes for “rs\_cf2”, “aud2”, and “anchor\_cnf”

## › On the alternative workflow

- It used to silently build on a lot of assumptions:
  - › C supports the alternative workflow
  - › C understands a successful Access Token Response not including an Access Token
  - › The AS is aware of such a support for C (e.g., as learned at C registration time)
- Now C explicitly opts-in for using the alternative workflow
  - › C includes “token\_upload” with value true in the Access Token Request to the AS
  - › Only in this case, if the AS supports the alternative workflow, then the AS MAY use it
- Anything else is unchanged; see Section 2 “New ACE Workflow” for details

# Updates in v -01 (3/4)

## › Updated two requirements on ACE profiles, from Appendix C of RFC 9200

- Their formulation predates RFC 9175 and its update on the CoAP Token processing

## › Fifth requirement

- OLD: *Specify the security protocol the client and RS must use to protect their communication (e.g., OSCORE or DTLS). This must provide encryption and integrity and replay protection (Section 5.8.4.3).*
- NEW: *Specify the security protocol the client and RS must use to protect their communication (e.g., OSCORE or DTLS). **In combination with the used communication protocol**, this must provide encryption, integrity and replay protection, **and a binding between requests and responses** (Section 5.8.4.3 and Section 6.5).*

## › Tenth requirement

- OLD: *Specify the communication and security protocol for interactions between the client and AS. This must provide encryption, integrity protection, replay protection, and a binding between requests and responses (Sections 5 and 5.8).*
- NEW: *Specify the communication and security protocol for interactions between the client and AS. **The combined use of those protocols** must provide encryption, integrity protection, replay protection, and a binding between requests and responses (Sections 5 and 5.8).*

# Updates in v -01 (4/4)

- › **Deprecated format defined in RFC 9200 for error responses specifying an error code**

- Payload: CBOR map with parameters “error”, “error\_description”, and “error\_uri”

- › **Defined and recommended use of Problem Details (RFC 9290)**

- Payload: CBOR map as a Concise Problem Detail data item

- › **The Concise Problem Detail data item:**

- MUST include the new Custom Problem Detail entry “ace-error”
  - › MUST include only one element, with key 0 and value from the usual IANA registry “OAuth Error Code CBOR Mappings”
  - › This specifies what “error” conveyed in the old format
- MAY include additional Standard Problem Detail entries, e.g.:
  - › “detail”, to specify what “error\_description” conveyed in the old format
  - › “instance”, to specify what “error\_uri” conveyed in the old format

```
Header: Bad Request (Code=4.00)
Content-Format: application/concise-problem-details+cbor
Payload:
{
  / title /      -1: "Incompatible ACE profile",
  / detail /     -2: "The RS supports only the OSCORE profile",
  / ace-error /  TBD: {
    / error_code /      0: 8 / incompatible_ace_profiles /
  }
}
```

Figure 7: Example of Error Response with Problem Details

- › **The new format is RECOMMENDED; if a C/RS/AS supports it, then C/RS/AS MUST use it in outgoing messages**

# Next steps

- › **Examples: avoid text strings as placeholders for to-be-registered integer abbreviations**
  - Instead, use what is proposed in *draft-bormann-cbor-e-ref*
- › **Work through the roadmap compiled in Appendix B**
  - On the alternative workflow
    - › Allow the dynamic update of access rights
    - › Allow the re-uploading of the same access token
    - › Allow its use for any profile of ACE
  - Possible definition of some more parameters
    - › Some specific for the alternative workflow, some independent of the used workflow
- › **Comments are welcome!**

Thank you!

Comments/questions?

<https://github.com/ace-wg/ace-workflow-and-params>



Backup

# Alternative workflow

## > (A) C-to-AS Token Request as usual

- C explicitly opts-in for the new workflow, including the new parameter “token\_upload” with value true
- The final choice about using it is on the AS

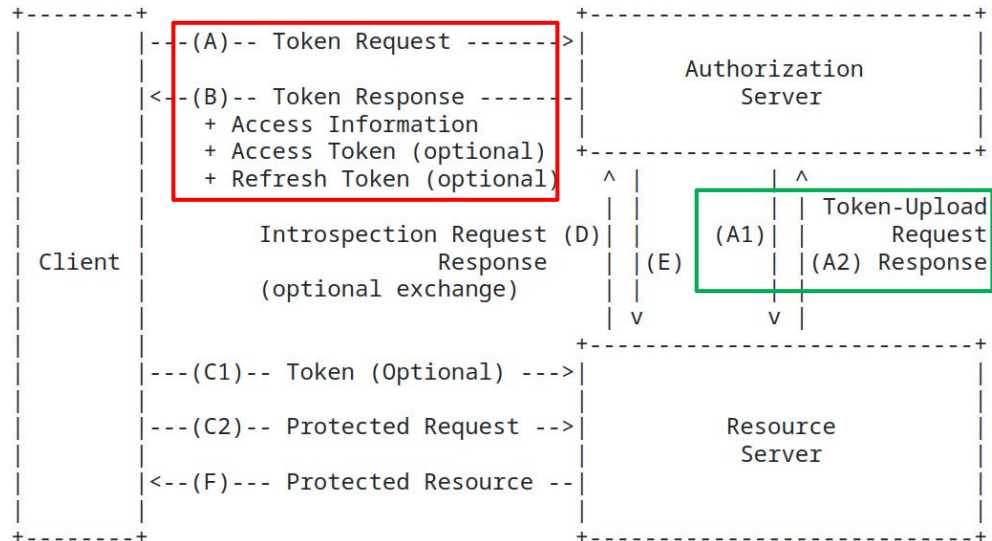
## > (A1) The AS uploads the access token to RS, on behalf of C

- No plan to replace the original workflow!
- The AS can dynamically choose the workflow to use, e.g., based on the specific RS

## > (A2) The AS receives a response from RS

## > (B) AS-to-C Token Response

- New parameter “token\_upload”
- **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



# Examples with alternative workflow

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

Example 1: the AS successfully uploaded the access token

```
Header: Created (Code=2.01)
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_upload" : 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

