

# Short Distribution Chain (SDC) Workflow and New OAuth Parameters for the Authentication and Authorization for Constrained Environments (ACE) Framework

*draft-ietf-ace-workflow-and-params-07*

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

IETF 125 Meeting – Shenzhen – March 17<sup>th</sup>, 2026

# Recap

## Set of updates to RFC 9200 (and other related RFCs)

- › **Define the new SDC 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
- › **Extend parameters for the OAuth 2.0 token endpoint**
  - New parameters enabling the new workflow, also with dynamic update of access rights
  - New parameters effectively enabling the issue of an access token for a group-audience
  - Extended semantics of the “ace\_profile” parameter
- › **Extend parameters for the OAuth 2.0 authz-info endpoint**
  - New parameter for dynamic update of access rights when using the new workflow
- › **Allow C and the AS to coordinate on exchanging authentication credentials by value or reference**
- › **Define a new ACE error code for failed proof-of-possession verification at the AS**
- › **Deprecate the original payload format of error responses**
  - Instead, use the problem-details format from RFC 9290
- › **Amend two requirements on transport profiles of ACE**

# Updates from version -06 to -07

- › **Editorial fixes and improvements**
- › **Inclusion of parameters in access token request/response**
  - Clearer and more consistent phrasing, e.g.:
    - › is OPTIONAL in → is OPTIONAL to include in
    - › is REQUIRED → MUST be included
  - If the access token is not the first in a token series
    - › "ace\_profile" MUST NOT be included in the access token request/response
    - › "rs\_cnf2", "audience2", "anchor\_cnf" MUST NOT be included in the access token response
- › **"rs\_cnf" in the access token request – Improved description of its *non-use***
  - Same purpose: C tells the AS if/how including RS' authentication credential in the access token response
  - If C does not have RS' authentication credential ...
    - › C MUST NOT include rs\_cnf = null (= give me nothing)
    - › C SHOULD NOT include rs\_cnf = false (= give me a reference, that's fine)
      - Exception: C will be able to use the reference for retrieving the credential via other means

# Updates from version -06 to -07

## › Specified parameter encoding when messages are encoded in JSON

- In the access token request/response to/from the AS
- In the token upload from the AS to RS
- CBOR array → JSON array
- CBOR text string → JSON string
- CBOR byte string → Binary representation encoded in base64url without padding

## › IANA considerations

- Added missing request for entry to update, in the "OAuth Parameters" registry
  - › Name: access\_token
  - › Parameter Usage Location: authorization response, token response, **as-rs request**
  - › Change Controller: IETF
  - › Reference: [RFC6749][**RFC-XXXX**]

# Updates from version -06 to -07

## › Clarifications

- Successful access token response → Access token response
- Where appropriate: mentioning of “successful response”, not necessarily 2.01 (Created)

## › Editorial suggestion from Dave Robin at IETF 124 – Thanks!

- Sec. 2.1 “Token Upload”, under Sec. 2 “The Short Distribution Chain (SDC) Workflow”
- Suggestion: *A lot of text was added on the dynamic update of access rights. That makes this section “noisy”. Move it to a later section and add a forward pointer here.*
- Done
  - › Five paragraphs deleted from Section 2.1. Their content was moved to Section 3.7.
  - › Section 2.1 shortly mentions that updating access right is possible in the SDC workflow, with the help of the “updated\_rights” parameter
  - › Forward pointer to Section 3.7 “updated\_rights”, where details are specified

# Updates from version -06 to -07

## › Special case (already noted in version -06):

- C has an access token T\_OLD and asks the AS:
  - › To issue an access token T\_NEW for dynamically updating its access rights
  - › To use the new SDC workflow for uploading T\_NEW to RS
- The AS issues T\_NEW (same token series as T\_OLD) and tries to upload it to RS
- The upload fails, because RS has deleted T\_OLD to supersede
- The AS replies to C, specifying T\_NEW and “token\_upload” = 1
- ... Then what?

## › End of Section 3.7 “updated\_rights” – Explained epilogue in the special case above:

- Also requested by Dave Robin at IETF 124
- C tries to upload T\_NEW to RS, using the corresponding secure communication association
- RS deleted T\_OLD, hence the secure association, so it replies to C with an error response
- C can ask the AS for yet another access token, which would start a new token series

# Planned improvement (1/2)

## › In that special case, the AS can:

- Receive the error response from RS
- Declare the upload of T\_NEW failed
- Invalidate T\_NEW and terminate the token series of T\_NEW
- **Start a new token series, with its first token T\_NEW\_2**, where
  - › “scope” is the same as in T\_NEW
  - › Anything else is aligned with the old access token request REQ that started the terminated token series of T\_NEW
- If REQ did include “to\_rs” (information from C to relay to RS) ...
  - › Then the AS replies to C with T\_NEW\_2
- If REQ did not include “to\_rs” (information from C to relay to RS) ...
  - › Then the AS tries to upload T\_NEW\_2 to RS on behalf of C, as per the SDC workflow
  - › No loops; T\_NEW\_2 is the first access token in a new token series

# Planned improvement (2/2)

- › Besides the improved sequence of steps, what do we actually need?
- › The AS needs to know that what occurred is exactly that special case
  - The RS can tell so in its error response to the AS, using a new ACE error code
  - Originally intended for responses from the AS, but not forbidden to use from elsewhere
- › The AS needs to remember the access token request that started a token series
  - This is already the case, to enable the dynamic update of access rights
- › The AS has to be able to tell C that “actually, a new token series has been started”
  - We can use the same, new parameter “token\_upload” in the access token response
  - With new values, for this special case and its follow-up starting of a new token series

# Related errata on RFC 9200

- › [https://www.rfc-editor.org/errata\\_search.php?rfc=9200](https://www.rfc-editor.org/errata_search.php?rfc=9200)
  
- › **7 technical errata reported on RFC 9200**
  - Errata ID: 8232 - Section 5.8.2 - Example
  - Errata ID: 8233 - Appendix F.1 - Example
  - Errata ID: 8234 - Appendix F.1 - Example
  - Errata ID: 8235 - Appendix F.2 - Example
  - Errata ID: 8236 - Appendix F.2 - Example
  - Errata ID: 8237 - Section 5.8.5 - IANA registration of "ace\_profile"
  - Errata ID: 8238 - Section 8.9 - IANA registration of "ace\_profile"
  
- › **Please review them**

# Next steps

- › **Extend “Security Considerations” section**
- › **Add “Operational Considerations” section**
  - See <https://datatracker.ietf.org/doc/html/draft-ietf-opsawg-rfc5706bis>
  - RFC 9200 does not have one; this can be another formal point of update to RFC 9200
- › **Revise inclusion rules for the “from\_rs” parameter in the access token response**
  - The presence/absence of the “to\_rs” parameter in the access token request should play no role
- › **Improve the dynamic update of access rights in the new SDC workflow**
  - If the AS fails precisely because RS has locally terminated the token series ...
  - ... the AS can seamlessly start a new token series and (possibly) upload the first access token to RS
- › **Add guidelines for using the “anchor\_cnf” parameter with group-audiences**
  - See also <https://github.com/ace-wg/ace-workflow-and-params/issues/2>
- › **Comments and reviews are welcome!**

Thank you!

Comments/questions?

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

Backup

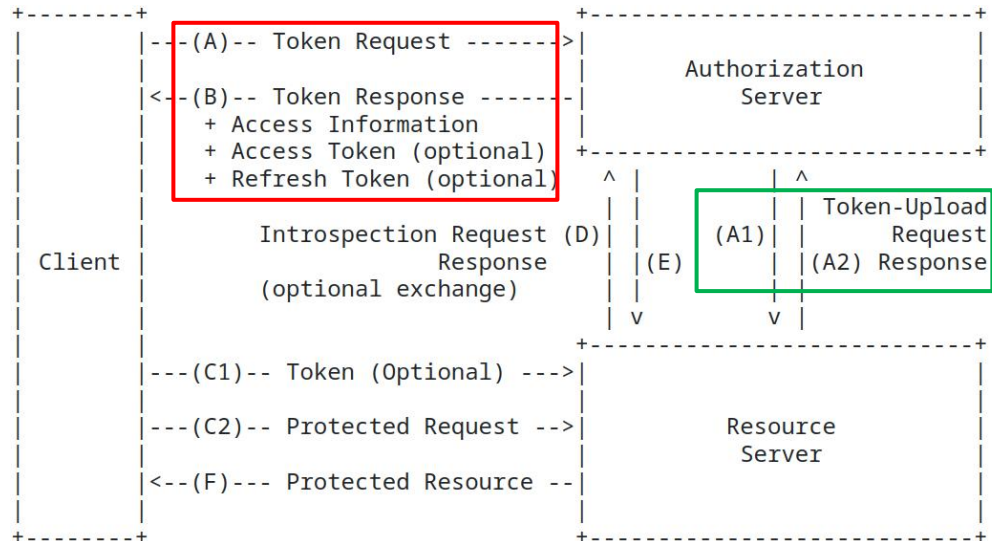
# New SDC workflow

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

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

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

- No intention 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”, with value 0 (successful upload) or 1 (failed upload)
- **0** → The Response includes: the access token; or a token hash; or neither. Then, C skips step C1.
- **1** → The Response includes the access token. Then, C performs step C1.

# Examples with new SDC workflow

```
Access Token Response
Header: Created (Code=2.01)
Content-Format: 19 (application/ace+cbor)
Max-Age: 3560
Payload:
{
  e'token_upload' : 0,
  / expires_in / 2 : 3600,
  / cnf / 8 : {
    / COSE_Key / 1 : {
      / kty / 1 : 4 / Symmetric /,
      / kid / 2 : h'3d027833fc6267ce',
      / k / -1 : h'73657373696f6e6b6579'
    }
  }
}
```

Example 1: the AS successfully uploaded the access token

```
Access Token Response
Header: Created (Code=2.01)
Content-Format: 19 (application/ace+cbor)
Max-Age: 3560
Payload:
{
  e'token_upload' : 1,
  / access_token / 1 : h'd08343a1...4819',
  / (full CWT elided for brevity;
    CWT contains the symmetric PoP key in the "cnf" claim) /
  / expires_in / 2 : 3600,
  / cnf / 8 : {
    / COSE_Key / 1 : {
      / kty / 1 : 4 / Symmetric /,
      / kid / 2 : h'3d027833fc6267ce',
      / k / -1 : h'73657373696f6e6b6579'
    }
  }
}
```

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

