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-08

Marco Tiloca, RISE
Göran Selander, Ericsson

IETF 126 Meeting – Vienna – July 20th, 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
- **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 -07 to -08

- **Warning: unintended instances of remnant text to be fixed! (Sections 3.2, 3.3.2, and 9)**
  - CURRENT: *“token_upload” parameter with value 0 or 2*
  - SHOULD BE: *“token_upload” parameter with value 0*

- **Fixes in IANA considerations**
  - Added references to IANA registries
  - Added updates to OAuth parameters “ecdh_info” and “kdc_dh_creds” recently added to the registry
    - The new SDC workflow extends their usage to the as-rs request and rs-as response

- **Section 5.2 – Rephrasing requested by Dave Robin at IETF 125**
  - Disentangle the inclusion and the value of “rs_cnf” in the access token request
    - C indicates that it wants the RS’ authentication credential by value, or by reference, or neither
  - New wording: if C includes “rs_cnf” and C does not have the RS’ authentication credential, then:
    - “rs_cnf” MUST NOT specify null (give me nothing)
    - “rs_cnf” SHOULD NOT specify false (give me a reference)

Updates from version -07 to -08

- **Section 3.1.1 – On using the SDC workflow and RFC 9770**
  - RFC 9770: the AS notifies about revoked access tokens, referred by token hashes
  - In the SDC workflow, C can ask the AS to have the access token (2), a token hash (1), or neither (0), through appropriate values of “token_upload” in the access token request
  - Practical guideline: not really useful to have token_upload = 0 if interested in using RFC 9770

- **Sections 3.3.1 and 3.3.2 – Strong decoupling of “to_rs” and “from_rs” in the SDC workflow**
  - “to_rs”: C provides the AS with information to relay to the RS when uploading the access token
  - “from_rs”: the AS provides C with information from the RS after successfully uploading the access token
  - New: the use of “from_rs” is totally unaffected by the use or non-use of “to_rs”
    - C might not have anything to relay to the RS → No “to_rs” in the access token request
    - Yet, the RS might reply to the AS with information to relay to C

Updates from version -07 to -08

- **Section 3.1.2 – Access token response when using the SDC workflow**
  - What if the access token is issued to a group-audience, i.e., for multiple RSs?
  - New: the AS stops uploading an access token to any remaining RS in the group-audience, as soon as the token upload fails at one of those RSs. It follows that …
  - The access token response indicates that the upload of an access token was successful if and only if the token upload was successful at each RS in the group-audience

- **New Section 9 "EDHOC EAD Item for Transporting a Session Identifier"**
  - In the EDHOC and OSCORE profile of ACE defined in *draft-ietf-ace-edhoc-oscore-profile* …
  - … C uploads the access token to the RS while running an EDHOC session
    - Within an EDHOC EAD item ACE-OAuth Access Token, specifying the access token by value
  - When using the SDC workflow and all goes fine, C might never get the access token
  - New: defined EDHOC EAD item Session ID, specifying the access token by reference
    - The EAD item conveys the token series ID that the AS provides to C in the access token response
  - Beyond the SDC workflow, also useful as an optimization, if C wants to re-run EDHOC with the RS

SDC workflow: 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 the RS
  - The AS issues T_NEW (same token series as T_OLD) and tries to upload it to the RS
  - The upload fails, specifically because the RS has deleted T_OLD to be superseded
  - … Then what?

- **Until version -07:**
  - The AS replies to C, specifying T_NEW and “token_upload” = 1 (failed upload)
  - C tries to upload T_NEW at the RS, using the corresponding secure comm. association
  - The RS deleted T_OLD and 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

From IETF 125: we can do better than this!

Updates from version -07 to -08

- **TL;DR: in this particular situation, the AS creates a new token series "on the fly"**

- **Updated Section 3.1.2; new Sections 3.7.1, 3.7.2, and 3.7.2.1**
  - The error response from the RS to the AS uses a new ACE error code "missing_old_token"
  - The AS receives that particular error response from the RS and:
    - Declares the upload of T_NEW failed
    - Invalidates T_NEW and terminates the token series of T_NEW
  - The AS starts a new token series "on the fly", with its first token T_NEXT where:
    - "scope" is the same as in T_NEW
    - Anything else is aligned with the old access token request that started the terminated token series of T_NEW
  - The AS replies to C with an access token response specifying:
    - The access token T_NEXT and "token_upload" = 2 (failed upload, with this outcome)
  - The AS can't upload T_NEXT to the RS – What if C would want to provide additional info?

Related errata on 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

- **Fix sentences in Sections 3.2, 3.3.2, and 9**
  - *… "token_upload" parameter with value 0 ~~or 2~~ …*
- **Add example of message exchange in the SDC workflow**
  - With the AS using the "updated_rights" parameter
- **Add guidelines for using the “anchor_cnf” parameter with group-audiences**
  - See also https://github.com/ace-wg/ace-workflow-and-params/issues/2
- **Extend “Security Considerations” section**
- **Add “Operational Considerations” section**
- **Comments and reviews are welcome!**

Thank you!

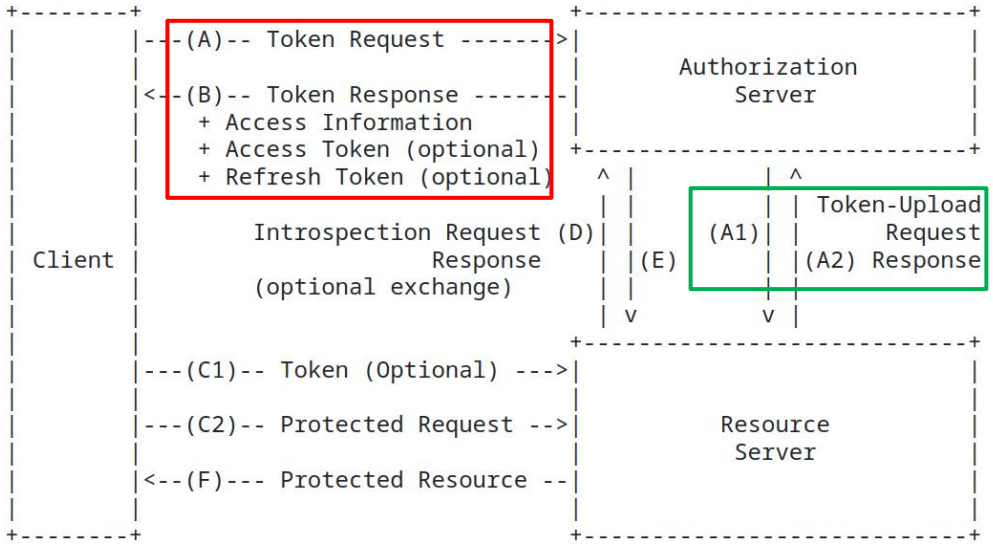
Comments/questions?

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 the 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 the 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