

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-05

Marco Tiloca, RISE
Göran Selander, Ericsson

IETF 123 Meeting – Madrid – July 24th, 2025

Recap

Set of updates to RFC 9200 (and more)

- › **Define a new 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
- › **Define additional OAuth parameters to use in ACE**
 - Enabling the new workflow, also with dynamic update of access rights
 - Effectively enabling the issue of an access token for a group-audience
- › **Extended semantics of the “ace_profile” parameter**
- › **C and the AS can coordinate on exchanging authentication credentials by value or reference**
- › **Define a new ACE error code for failed proof-of-possession verification at the AS** **NEW**
- › **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 in v -05

› Editorial improvements, including:

- The CoAP definition of “endpoint” from RFC 7252, which is not used here
- s/“Named Information Hash Algorithm” registry/“Named Information Hash Algorithm Registry”

› Revised order of some sections

- Section “Updated Requirements on Profiles of ACE” moved later, as last contribution

› Fixes in the IANA considerations

- Distinguish between “registry” and “registry group”
- All considerations about the “OAuth Parameters” registry in a single section
- All considerations about the “OAuth Parameters CBOR Mappings” registry in a single section

› Updated references

- *draft-ietf-ace-revoked-token-notification* → RFC 9770
- More recent reference to SHA-256, i.e., FIPS PUB 180-4 (August 2015)

Updates in v -05

Error handling at the AS and new ACE error code

› C-to-AS access token request to the /token endpoint

- The optional parameter “req_cnf” typically conveys the public key of C, to use as PoP key
- The AS must achieve proof of possession of C’s private key (Section 3.1 of RFC 9201), e.g.:
 - › It is achieved already (e.g., previous interactions or out-of-band means)
 - › It is achieved through an evidence in the present request (e.g., see request parameters in [1])

› If the AS does not achieve proof of possession, it must reject the request

› Defined new ACE error code “failed_pop_verification”

- Used in the payload of an error response, with response code equivalent to the CoAP code 4.00
- Requested IANA registrations (“OAuth Extensions Error” and “OAuth Error Code CBOR Mappings”)
- Note: the OAuth error “invalid_dpop_proof” is different and specific for DPoP (see RFC 9449)

Updates in v -05

Revised definition of the parameters "to_rs" and "from_rs"

› Parameters defined in version -03

- Used between C and the AS, when using the new SDC workflow
- In fact, for some profiles of ACE, they enable the use of the new SDC workflow

› “to_rs” – For the C-to-AS access token request

- Must be accompanied by the parameter “token_upload”
- Only used when requesting the first access token in a token series
- Value: information that the AS has to upload to the RS on behalf of C, when uploading the access token

› “from_rs” – For the AS-to-C access token response

- Must be accompanied by the parameter “token_upload” with value 0 (successful token upload)
- Only used when the parameter “to_rs” was present in the access token request
- Value: information that the AS provides to C on behalf of the RS, after a successful token upload

› C and the RS would exchange the same information directly, if using the original workflow

- The semantics of the parameter values depends on the profile of ACE used

Updates in v -05

Revised definition of the parameters "to_rs" and "from_rs" (continued)

› The original design was not general enough

- Strong bias from the OSCORE profile of ACE (RFC 9203) as main beneficiary
- Not considering applications at large and media types used between C and the RS in the original workflow

› Revised semantics of "to_rs"

- Presence → C wants to relay information to the RS and to have information from the RS relayed back
- Value → Information from C to relay to the RS
 - › CBOR simple value null (0xf6) → no actual information to relay
 - › (tagged) CBOR byte string → information to relay to the RS
 - The value of the CBOR byte string is the binary representation of a CBOR data item STRUCT
 - STRUCT wraps the same information that C would send to the RS in the original workflow
 - If not tagged: the POST request from the AS to /authz-info will have the same Content-Format that is employed in the profile of ACE used
 - If tagged: the POST request from the AS to /authz-info will have the Content-Format that is indicated by the tag number, as per Appendix B of RFC 9277 (e.g., use the DTLS profile (RFC 9202) together with an application profile of RFC 9594 ...)

Updates in v -05

Revised definition of the parameters "to_rs" and "from_rs" (continued)

› Revised semantics of "from_rs"

- Value → Information from the RS to relay to C
- Empty CBOR byte string (0x40), if no payload in the successful response from the RS
- (tagged) CBOR byte string
 - › The value of the CBOR byte string is the payload of the successful response from the RS
 - › Tagged if the response specifies a Content-Format; the tag number is as per Appendix B of RFC 9277

› Processing at the AS

- If "to_rs" is not null
 - › Complete STRUCT by adding the issued access token
 - › Use STRUCT as payload of the POST request to /authz-info
 - Content-Format as per the ACE profile used or per the tag number of "from_rs" (if tagged)
- Build "from_rs" using the payload of the successful response from the RS
 - › Tag "from_rs" to indicate the Content-Format of the response, if one is indicated therein

Updates in v -05

› Use of “to_rs” and “from_rs” in the OSCORE profile (RFC 9203)

- Still as intended and consistent with the latest general semantics
- Effectively enabling the alternative workflow in this profile
- C and the RS can exchange (N1, ID1) and (N2, ID2) through the AS

› In “to_rs”, the CBOR byte string wraps a CBOR map with:

- The nonce N1 generated by C, as a CBOR byte string
- The Recipient ID ID1 generated by C, as a CBOR byte string

› In “from_rs”, the CBOR byte string wraps a CBOR map with:

- The nonce N2 generated by the RS, as a CBOR byte string
- The Recipient ID ID2 generated by the RS, as a CBOR byte string

› The AS builds:

- The POST request to /authz-info at the RS, using N1 and ID1 from “to_rs”, plus the issued access token
- The information in “from_rs”, using N2 and ID2 from the response from the RS

```
Access token request
Header: POST (Code=0.02)
Uri-Host: "as.example.com"
Uri-Path: "token"
Content-Format: 19 (application/ace+cbor)
Payload:
{
  / audience / 5 : "tempSensor4711",
  / scope / 9 : "read",
  e'token_upload' : 0,
  e'to_rs' : h'a2182848018a278f7faab55a182b421645'
}

Access token response
Header: Created (Code=2.01)
Content-Format: 19 (application/ace+cbor)
Max-Age: 3560
Payload:
{
  e'token_upload' : 0,
  e'from_rs' : h'a2182a4825a8991cd700ac01182c420000',
  / ace_profile / 38 : / coap_oscore / 2,
  / expires_in / 2 : 3600,
  / cnf / 8 : {
    / osc / 4 : {
      / id / 0 : h'01',
      / ms / 2 : h'f9af838368e353e78888e1426bd94e6f'
    }
  }
}
```

Next steps

› Add examples of message exchanges

- C and the AS coordinating on exchanging credentials by value or reference
 - › Using the new error code “unknown_credential_referenced”
 - › Using the “rs_cnf” parameter in the access token request

› On the new ACE workflow

- Detailed handling of an uploaded access token on the RS side
- New parameter “updated_rights” → Prevent ambiguities when dynamically updating access rights (*)

› 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

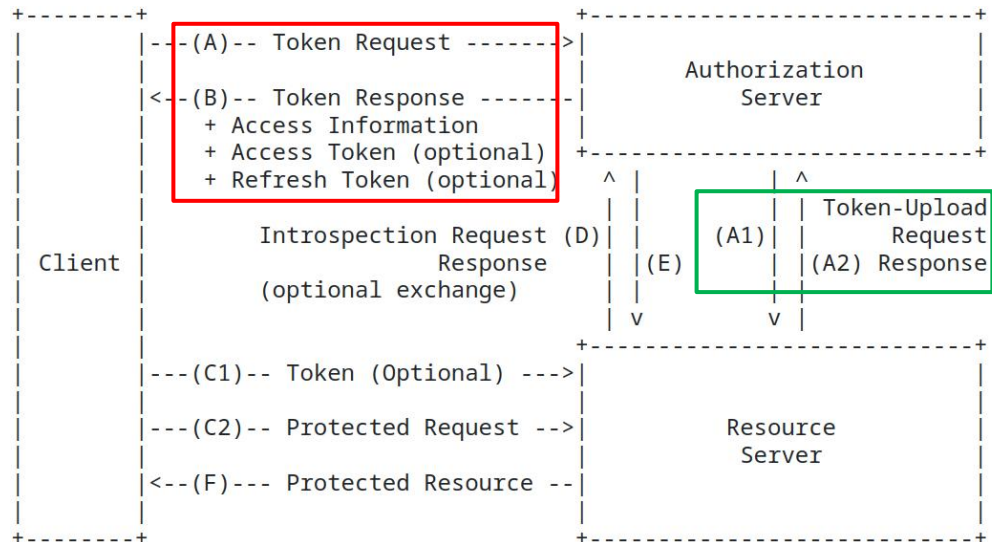
› (A1) The AS uploads the access token to RS, on behalf of C

- 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

