Authentication and Authorization for Constrained Environments (ACE)

draft-ietf-ace-oauth-authz-02

Ludwig Seitz (ludwig@sics.se)

IETF ACE WG meeting, IETF 96
20. July, 2016

Major changes from -01 to -02

- Separation of Framework and Profiles
- OAuth Endpoints
- Proof-of-possession Key Distribution
- Key Confirmation
- Client Tokens
- IANA
- Deployment Scenarios

Separation of Framework and Profiles

- This draft is the ACE framework
  - Defines OAuth endpoints
    - Note: “endpoint” defined differently in OAuth and CoAP
- ACE Profiles specify
  - Communication protocol
  - Communication security
  - Mutual authentication
  - Proof-of-Possession method for access tokens (could coincide with client authentication)
  - *Optionally: New methods of token transfer*

First example: draft-seitz-ace-oscoap-profile

OAuth Endpoints

- /token
  - Hosted by AS
  - Used by client to request access tokens
  - Informs client about the profile to use
- /introspect
  - Hosted by AS
  - Used by RS to get information about access tokens
  - Can provide information for the client → *client-token*
- /authz-info
  - Hosted by RS
  - Used by client to submit access tokens

Proof-of-possession Key Distribution

- /token endpoint (like in plain OAuth 2.0)
- Additional response parameters:
  - profile : Specifies ACE profile between client and RS
  - token_type : here always “pop”
  - alg : Proof-of-possession method, specified by profiles
  - cnf : Proof-of-possession key (See next slide)
- Client can also use these to indicate preferences in the request
- Duplicates some work from draft-ietf-oauth-pop-key-distribution
  - Status of this draft unclear

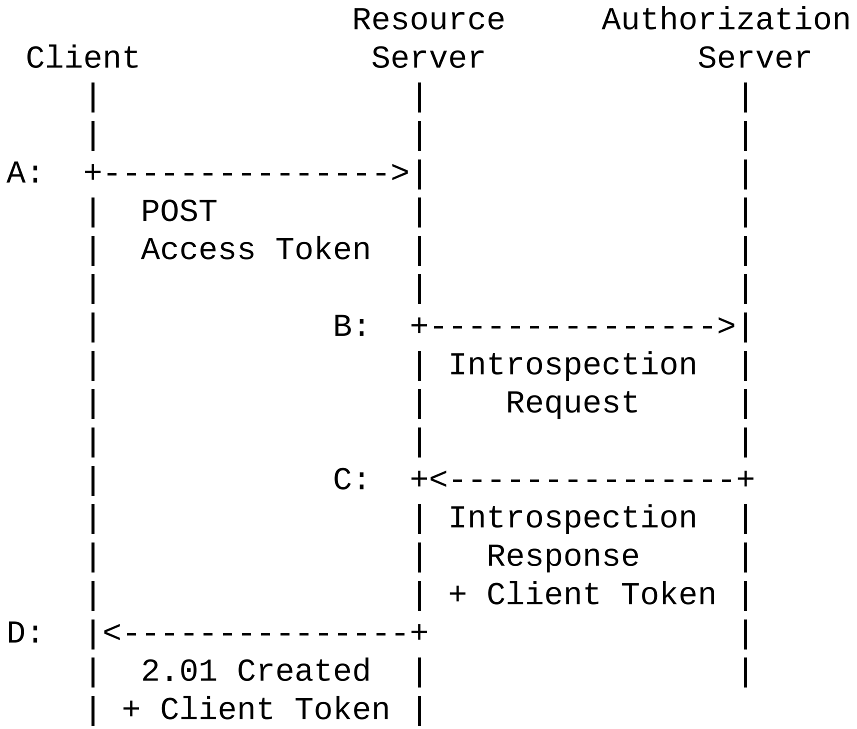
Key Confirmation

- Uses 'cnf' claim/parameter
  - Analogous to RFC 7800, but for CBOR/COSE
  - Either holds a COSE_Key or a key-identifier
- Defined for use in:
  - Access Token
  - Client Token
  - Access Token request
  - Access Token response
  - Introspection response

Client Tokens

Scenario:

- Client with limited connectivity and long-lived token
- Client Token informs client about RS's key (and possibly about other access token metadata)
- New concept, please review for usefulness!



```
                  Resource     Authorization
 Client            Server           Server
    |                |                |
    |                |                |
A:  +--------------->|                |
    |  POST          |                |
    |  Access Token  |                |
    |                |                |
    |           B:   +--------------->|
    |                | Introspection  |
    |                |    Request     |
    |                |                |
    |           C:   +<---------------+
    |                | Introspection  |
    |                |   Response     |
    |                | + Client Token |
D:  |<---------------+                |
    |  2.01 Created  |                |
    | + Client Token |
```

IANA

- Registering new parameters/claims for OAuth
- Registering CBOR abbreviation for existing parameters
- Please double-check!

Deployment Scenarios

- Moved to appendix
- Non-normative examples of how the framework could be used
- May be replaced by profiles

Next Steps

- Address Renzo's review comments
- More feedback on Client Tokens
- Complete the client information
- CoAP-DTLS profile
- Planned implementation work
  - SEI group at CMU
  - SICS

Thank you!

Questions/comments?