Token Revocation Notifications

draft-tiloca-ace-revoked-token-notification-00

Ludwig Seitz (ludwig.seitz@ri.se)

IETF 106 ACE WG meeting
November 19, 2019
Problem

• OAuth: token revocation by Client (RFC 7009)
• No revocation by Resource Owner or AS
  → Not a problem, tokens expire fast ...

... but not in ACE (e.g. clients with intermittent connectivity)

• AS: How do I tell my Client/RS?
Idea (by Jim Schaad)

• Create resource at AS for each Client/RS
• Client/RS can GET or GET-Observable
• Payload == list of revoked tokens
  – Actually IDs of revoked tokens
• What ID?
  – Not ‘cti’ → token opaque to client
  – Use hash of token (RFC 6920, section 3)
• Updated when new tokens revoked or revoked token expires
Example

Registration: POST

Payload:

```json
...
"trl" = "/trl/RS1"
}
```

GET Observe: 0
`coap://example.as.com/trl/RS1`

Access control

2.05 CONTENT Observe: 1

(Access Tokens t1 and t2 issued and successfully submitted to RS1)
Example ctd.

```
    (Access Token t1 is revoked)

    2.05 CONTENT Observe: 2
    Payload: [h(bstr.t1)]
    .
    .
    .

    (Access Token t2 is revoked)

    2.05 CONTENT Observe: 3
    Payload: [h(bstr.t1), h(bstr.t2)]
    .
    .
    .

    (Access Token t1 expires)

    2.05 CONTENT Observe: 4
    Payload: [h(bstr.t2)]
```