OAuth 2.0 Token Exchange


Brian Campbell et al.

IETF 99
Prague
July 2017
Attempt to Provide Context
(one example of the many use cases of a token exchange framework)

GET /resource HTTP/1.1
Host: frontend.example.com
Authorization: Bearer accVjcyb4BWGxGsdESCJQbdPMoUC5PbDqc6LTc

HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-cache, no-store

```
{
  "access_token": "eyJhbGciOiIjFUZ1NiIsImltZCI6IjI1l3JlciJ9.eyJhbGciOiIjFQIi
  odHRwczovL2JhY2tlbmQuZlhhXbsS5jb20iLCJpIjoiMjB0b3JpOGFwc3Yy
  4YWlwbGUyY29tIiwzXhjiowxQwOF3NTkzLCJpYXQiOjE0NDE5MTo1MeMn
  N1y1Ii6mJQGV4YWlwbGUyY29tIiwic2NjIjpmFwaSjEQ-MXqygYPMoNhce
  Pw8Qbun32q_pDyCFA-Saob16gYAdyPbaALFuAOypFr4X7WaePEnHV_LGnxL6T
  z0yC7h1SQR",
  "issued_token_type": 
  "urn:ietf:params:oauth:token-type:access_token",
  "token_type": "Bearer",
  "expires_in": 60
}
```

POST /as/token.oauth2 HTTP/1.1
Host: as.example.com
Authorization: Basic cnMWQDpsb25lLXN1Y3Vv245yWkb20tc2VjcmV0
Content-Type: application/x-www-form-urlencoded

```
grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-type%3Atoken-exchange
&resource=https%3A%2F%2Fbackend.example.com%2Fpapi%20
&subject_token=accVjcyb4BWGxGsdESCJQbdPMoUC5PbDqc6LTc
&subject_token_type=urn%3Aietf%3Aparams%3Aoauth%3Atoken-type%3Atoken
```

GET /api HTTP/1.1
Host: backend.example.com
Authorization: Bearer eyJhbGciOiIjFUZ1NiIsImltZCI6IjI1l3JlciJ9.eyJhbGciOiIjFQIi
odHRwczovL2JhY2tlbmQuZlhhXbsS5jb20iLCJpIjoiMjB0b3JpOGFwc3Yy
4YWlwbGUyY29tIiwzXhjiowxQwOF3NTkzLCJpYXQiOjE0NDE5MTo1MeMn
N1y1Ii6mJQGV4YWlwbGUyY29tIiwic2NjIjpmFwaSjEQ-MXqygYPMoNhce
Pw8Qbun32q_pDyCFA-Saob16gYAdyPbaALFuAOypFr4X7WaePEnHV_LGnxL6T
z0yC7h1SQR
Current Status

- Draft -09 published July 3rd with relatively minor changes addressing actionable and meaningful WGLC feedback
  - Changed "security tokens obtained could be used in a number of contexts" to "security tokens obtained may be used in a number of contexts"
  - Clarified that the validity of the subject or actor token have no impact on the validity of the issued token after the exchange has occurred
  - Changed use of “invalid_target” error code to a SHOULD (from MAY)
  - Clarified text about non-identity claims within the "act" claim being meaningless
  - Added brief Privacy Considerations section
Next Steps

* *humbly request* Transition to "Waiting for Writeup"

from IETF 93