# OAuth 2.0 Token Exchange

## An STS for the REST of Us

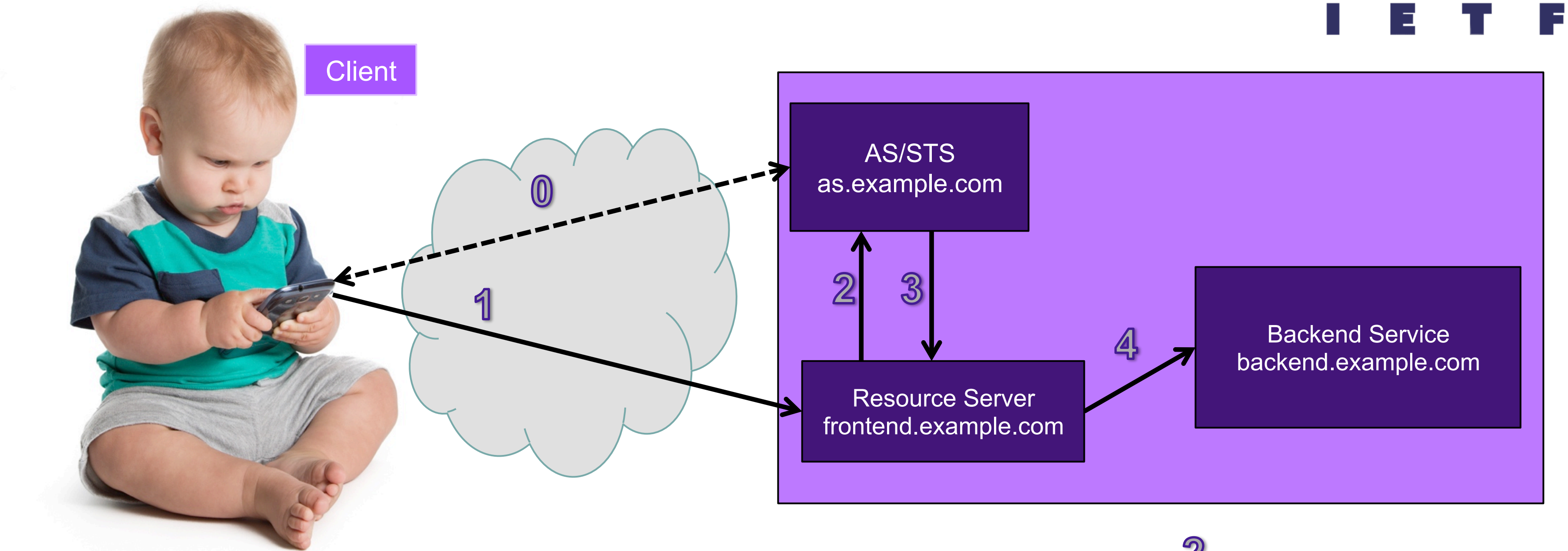
Brian Campbell
et al.

IETF 96
Berlin
July 2016

current: https://tools.ietf.org/html/draft-ietf-oauth-token-exchange-05

# Just One Example

(a quick illustration in the very unlikely event of some folks not having read the draft)



1

```
GET /resource HTTP/1.1
Host: frontend.example.com
Authorization: Bearer accVkjcJyb4BWCxGsndESCJQbdFMogUC5PbRDqceLTC
```

2

```
POST /as/token.oauth2 HTTP/1.1
Host: as.example.com
Authorization: Basic cnMwODpsb25nLXNlY3VyZS1yYW5kb20tc2VjcmV0
Content-Type: application/x-www-form-urlencoded

grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-type%3Atoken-exchange
&resource=https%3A%2F%2Fbackend.example.com%2Fapi%20
&subject_token=accVkjcJyb4BWCxGsndESCJQbdFMogUC5PbRDqceLTC
&subject_token_type=
 urn%3Aietf%3Aparams%3Aoauth%3Atoken-type%3Aaccess_token
```

3

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

{
 "access_token":"eyJhbGciOiJFUzI1NiIsImtpZCI6IjllciJ9.eyJhdWQiOiJo
   dHRwczovL2JhY2tlbmQuZXhhbXBsZS5jb20iLCJpc3MiOiJodHRwczovL2FzLmV
   4YW1wbGUuY29tIiwiZXhwIjoxNDQxOTE3NTkzLCJpYXQiOjE0NDE5MTc1MzMsIn
   N1YiI6ImJjQGV4YW1wbGUuY29tIiwic2NwIjpbImFwaSJdfQ.MXgnpvPMo0nhce
   PwnQbunD2gw_pDyCFA-Saobl6gyLAdyPbaALFuAOyFc4XTWaPEnHV_LGmXklSTp
   z0yC7hlSQ",
 "issued_token_type":
     "urn:ietf:params:oauth:token-type:access_token",
 "token_type":"Bearer",
 "expires_in":60
}
```

4

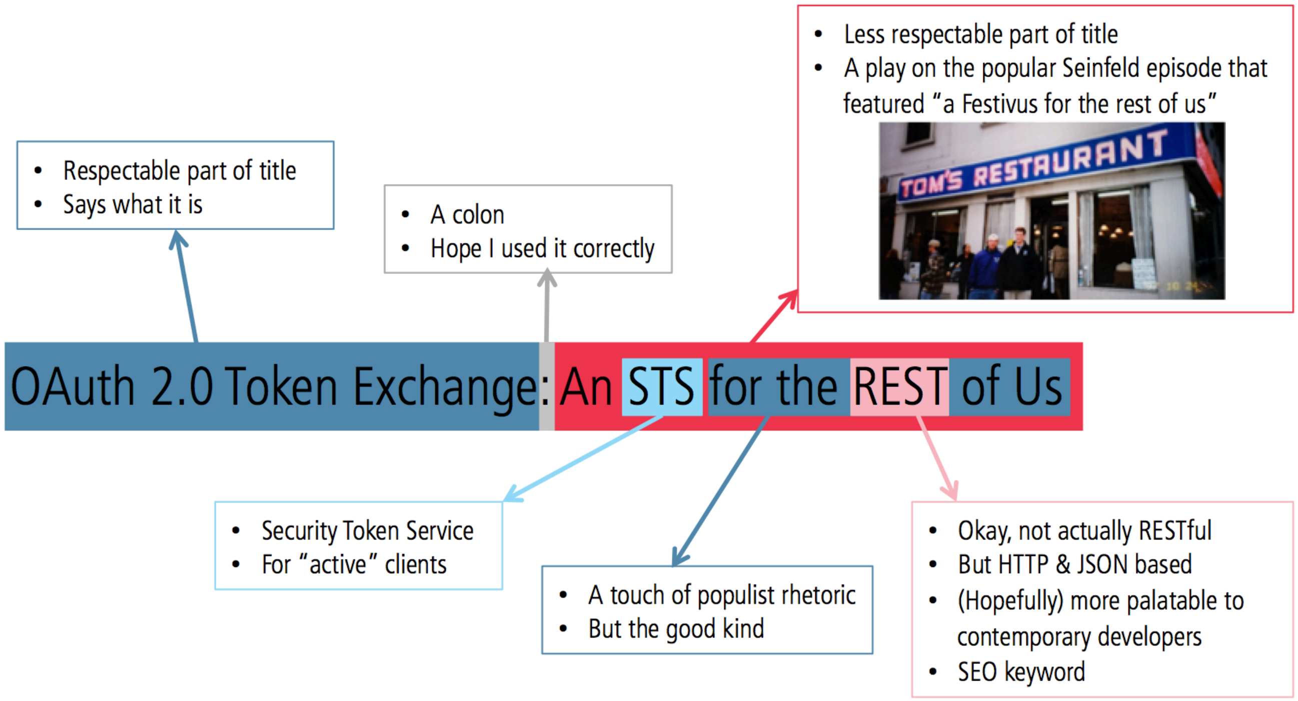
```
GET /api HTTP/1.1
Host: backend.example.com
Authorization: Bearer eyJhbGciOiJFUzI1NiIsImtpZCI6IjllciJ9.eyJhdWQ
   iOiJodHRwczovL2JhY2tlbmQuZXhhbXBsZS5jb20iLCJpc3MiOiJodHRwczovL2
   FzLmV4YW1wbGUuY29tIiwiZXhwIjoxNDQxOTE3NTkzLCJpYXQiOjE0NDE5MTc1M
   zMsInN1YiI6ImJjQGV4YW1wbGUuY29tIiwic2NwIjpbImFwaSJdfQ.MXgnpvPMo
   0nhcePwnQbunD2gw_pDyCFA-Saobl6gyLAdyPbaALFuAOyFc4XTWaPEnHV_LGmX
   klSTpz0yC7hlSQ
```

# Current Status

- Draft -05 published July 8 (yes, the cut-off) with relatively minor changes
  - Added "cid” JWT claim that can express the client identifier of the client that requested the token.
  - Token introspection response parameter registration for "act" and "may_act”
  - refresh_token now OPTIONAL (was NOT RECOMMENDED)
  - Attempt to better clarify the distinction between JWT and access token URIs.
  - Remove some of the ‘Open Issues’
    - No short names
    - No supplementary info/claims

# Moving Forward

- I believe it's getting close…
- Open Issues
  - Facilitating proof-of-possession cases
    - In & out, token binding, use-case diversity
- Other stuff
  - ID Tokens
    - URI
    - Scope & "id_token" response parameter
  - The title…



OAuth 2.0 Token Exchange: An STS for the REST of Us

- Respectable part of title
- Says what it is

- A colon
- Hope I used it correctly

- Less respectable part of title
- A play on the popular Seinfeld episode that featured "a Festivus for the rest of us"

- Security Token Service
- For "active" clients

- A touch of populist rhetoric
- But the good kind

- Okay, not actually RESTful
- But HTTP & JSON based
- (Hopefully) more palatable to contemporary developers
- SEO keyword