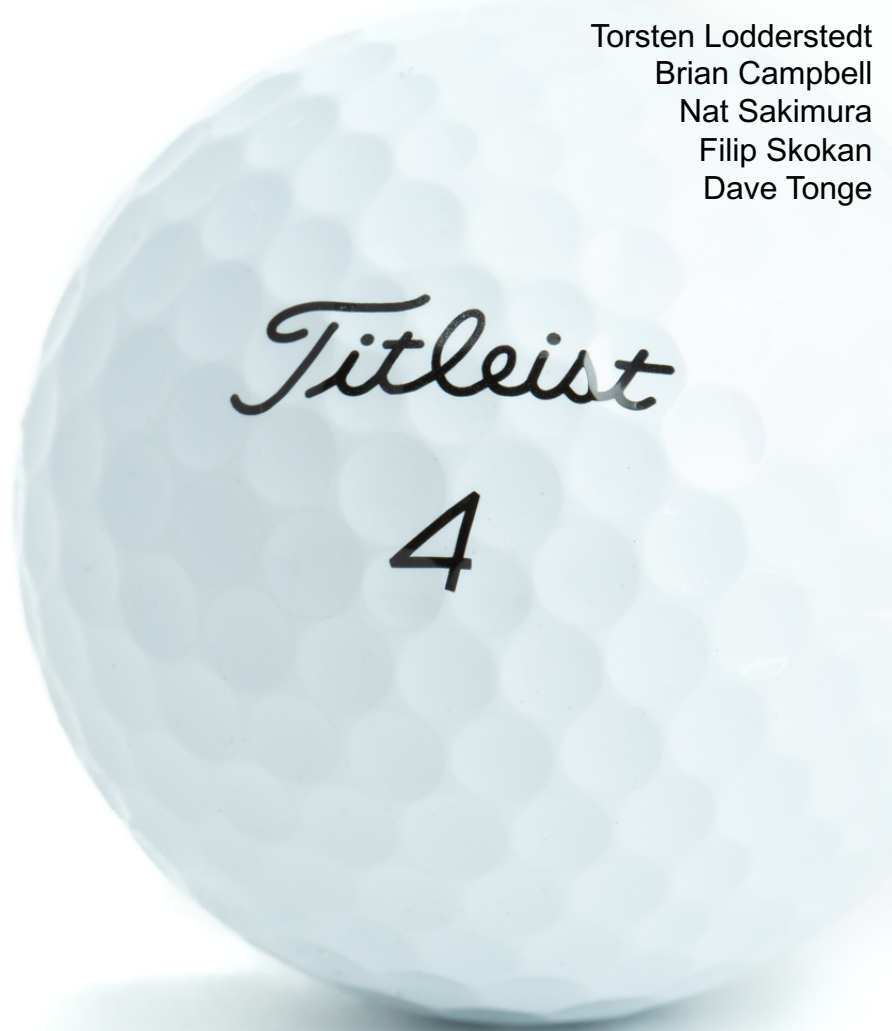


OAUTH WG
~~IETF 108, Madrid~~
Virtual Interim
August 10, 2020

Torsten Lodderstedt
Brian Campbell
Nat Sakimura
Filip Skokan
Dave Tonge

OAuth 2.0 **P**ushed **A**uthorization **R**equests

PAR

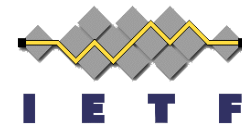


draft-ietf-oauth-par

PAR, what is it good for?

- Introduces the pushed authorization request endpoint, which:
 - allows a client to push the payload of an OAuth 2.0 authorization request to the AS via a direct request
 - using the same client authentication as at token endpoint (and others)
 - provides client with a request URI that is used as reference to the data in a subsequent authorization request via the browser
- Allows for large authorization requests
 - e.g. in `authorization_details` or `claims` parameters, scope run amok, JWT encoded state, etc.
- Direct client->AS TLS provides integrity & confidentiality protection
- Client authentication and authorization prior to the start of user interaction for confidential clients

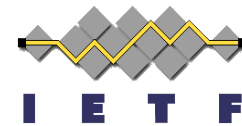
How to PAR: Client->AS Request



```
POST /as/par HTTP/1.1
Host: as.example.com
Content-Type: application/x-www-form-urlencoded
Authorization: Basic czZCaGRSa3F0Mzo3RmpmcDBaQnIxS3REUmJuZlZkbUl3
```

```
response_type=code&
state=uiXjmb1aIb3EASVhtQD-3SRLWWvROUoBoYB7yjzeic5CwU7fPM305frN_&
client_id=s6BhdRkqt3&
redirect_uri=https%3A%2F%2Fclient.example.org%2Fcb&
code_challenge=K2-ltc83acc4h0c9w6ESC_rEMTJ3bww-uCHaoeK1t8U&
code_challenge_method=S256&
scope=account-information
```

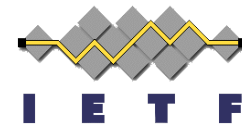
How to PAR: AS->Client Response



HTTP/1.1 201 Created
Content-Type: application/json
Cache-Control: no-cache, no-store

```
{  
  "request_uri":  
    "urn:ietf:params:oauth:request_uri:bwc4JK-ESC0w8acc191e-Y1LTC2",  
  "expires_in": 60  
}
```


How to PAR: Authorization Request via Browser



`https://as.example.com/as/authz?client_id=s6BhdRkqt3&request_uri=urn%3Aietf%3Aparams3Aoauth%3Arequest_uri%3Abwc4JK-ESC0w8acc191e-Y1LTC2`

History



- Conceptualized in Nat's mind long ago
- Half-hearted subsection in FAPI for a while
- I-D discussed at IETF 105 & 106
- Adopted by the WG at the end of 2019

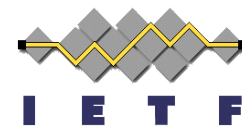


IETF #105 Montreal



IETF #106 Singapore

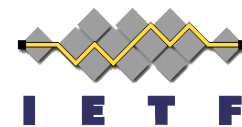
Consensus, PAR for the Course



- -02 published July 10th with updates based on consensus around items discussed in previous interim and on the list
 - Added “require_pushed_authorization_requests” client and AS metadata in support of policy for only accepting pushed authorization requests
 - Updated to comply with JAR draft -21, which requires client_id in the authorization request in addition to the request_uri
 - Added note regarding “require_signed_request_object” metadata that was added to JAR draft -25
 - Clarified timing of request validation
 - Added some guidance/options on the request URI structure
 - “urn:ietf:params:oauth:request_uri:<reference-value>” based on the seminal work of RFC 6755
 - UUID as a URN per RFC 4122
 - Update Resource Indicators reference to the somewhat recently published RFC 8707
 - Add the key used in the request object example so that a reader could validate or recreate the request object signature
- Note that JAR draft -22 relaxed language that said a request_uri MUST refer to a JWT so PAR didn’t need an exception/explanation

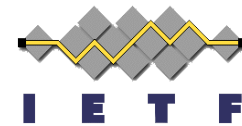
Bogey on the -02nd Hole

(minor though)



- -03 published July 31st
 - Editorial updates
 - Explicitly state the PAR endpoint URL MUST use the "https" scheme
 - Better explain one-time use recommendation of the request_uri
 - Added text about motivations behind PAR - integrity, confidentiality and early client auth
 - Drop the section on special error responses for request objects
 - Add some discussion of browser form posting an authorization request vs the benefits of PAR for any application
 - Clarify authorization request examples to say that the client directs the user-agent to make the HTTP GET request (vs. making the request itself)

and Running Code



- Numerous implementations
 - Connect2id
 - node-oidc-provider
 - Authlete
 - ID-Porten
 - yes[®]
 - Santander's Digital Trust Protocol
 - PingFederate[®]
- Used/referenced by other SDOs
 - FAPI 2.0 baseline profile
 - Australian CDR initiative

Next Steps: Progress PAR to WGLC?

IETF #103
Bangkok Marriott
Marquis Queen's
Park



Gratuitous closing slide featuring the city of
the next likely-canceled in-person meeting