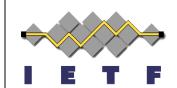
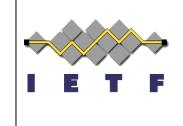
# OAuth 2.0 Demonstrating Proof-of-Possession at the Application Layer (DPoP)



#### draft-ietf-oauth-dpop

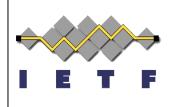
Michael B. Jones OAuth Virtual Interim Meeting October 27, 2021

#### **The Goal**



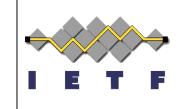
 Simple application-level proof-of-possession mechanism for OAuth 2.0

## **Recent Updates**



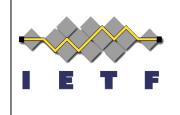
- Current draft is <u>draft-ietf-oauth-dpop-04</u>
  - Added server-contributed nonces
    - Thanks for the good discussions leading up to that!
  - Mentioned that that RFC 7235 allows multiple authentication schemes in WWW-Authenticate
  - Added some IANA registrations

# End-to-End Proof Under Discussion



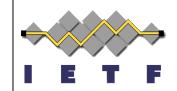
- DPoP key currently first sent with token request
- Also possible to send with authorization request
  - Would provide end-to-end DPoP binding from authorization request to token request to resource request
- Related issues:
  - #71: Tie keys back to the authorization endpoint for E2E PoP protection
  - #85: Describe and prevent double-code-usage attack
- PR #86 proposes a DPoP PKCE method to do this
  - Under discussion whether to do this with PKCE
  - or whether to do it with a new dpop\_jkt request parameter
- Let's discuss

#### **Next Steps**



- Decide how to achieve end-to-end binding
- Triage open issues (see next slide)
- Publish -05
- Initiate Working Group Last Call (WGLC)?

## **Open Issues**



- Currently 8 open issues filed:
  - https://github.com/danielfett/draft-dpop/issues
- Also, PR comments by Filip Skokan:
  - https://github.com/danielfett/draft-dpop/pull/81#pullreq uestreview-761774711
  - https://github.com/danielfett/draft-dpop/pull/81#issuec omment-928145557
- And mailing list comments by Neil Madden:
  - https://mailarchive.ietf.org/arch/msg/oauth/VIIc3XQ0p\_ 4eVFfrtN8B8-TqyZY/
- We could triage some of these together now, time permitting