Proposed New OAuth 2.0 Client Assertion

Omer Levi Hevroni
IETF meeting
April 2018
Why new standard?

- Login screen is required for authentication
- Apps don’t always need/want login screen
- Login screen affects the app look and feel
- Another solution is required
- We need to authenticate the device
  - Device level authorization
  - Any device can register
High level overview

- The app uses JWS to authenticate
- JWS payload is one time password (OTP)
- Similar to JWT client assertion
  - Main difference is the payload
  - Time is tricky on mobile devices
- Client registration is not part of the draft
Authentication request

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

grant_type=token_id_token&
client_assertion_type=urn%3Aietf%3Aparams%3Aoath%3A
client_assertion-type=3Ajwt-otp&
client_assertion=eyJhbGciOiJSUzI1NiIsImtpZCI6IjIyIn0.
eyJpc3Mi[...omitted for brevity...].
cC4hiUPo[...omitted for brevity...]
JWS Payload
Next steps

- Early version of the standard is on GitHub
- Looking for feedback
- First draft: Q2 2018
Questions?

@omerlh
Resources

- Blog post describing the flow
- Talk describing the flow
- GitHub repo with the proposed standard
- Reach out to me if you have any question