IETF 124
Montreal
November 2025

Aaron Parecki

DPoP for Device Authorization Grant and JWT Authorization Grant

https://datatracker.ietf.org/doc/draft-parecki-oauth-dpop-device-flow/
https://datatracker.ietf.org/doc/draft-parecki-oauth-jwt-dpop-grant/

DPoP for Device Authorization Grant

Why?

- Clients using the Device Code Grant (RFC8628) are likely public clients
- DPoP + app attestation reduces risk of mass token sales
- This was always possible, but not actually written down anywhere

https://datatracker.ietf.org/doc/draft-parecki-oauth-dpop-device-flow/

DPoP for Device Authorization Grant

```
POST /device_authorization HTTP/1.1
Host: server.example.com
Content-Type: application/x-www-form-urlencoded
DPoP: eyJ0eXAiOiJkcG9wK2p3dCIsImFsZyI6IkVTMjU2IiwiandrI…

client_id=1406020730&scope=example_scope
```

Client includes DPoP proof at:

- Device Authorization Endpoint (before user authentication)
- Token Endpoint polling (before and after user authentication)

Primary new thing in this draft

https://datatracker.ietf.org/doc/draft-parecki-oauth-dpop-device-flow/

DPoP for JWT Authorization Grant

RFC7523 defines `urn:ietf:params:oauth:grant-type:jwt-bearer` and a way to present a JWT as an authorization grant to obtain an access token

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

grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-type%3Ajwt-bearer
&assertion=eyJhbGciOiJFUzI1NiIsImtpZCI6IjE2In0.
eyJpc3Mi[...omitted for brevity...].
J9l-ZhwP[...omitted for brevity...]
```

How the JWT was obtained is out of scope.

What if the JWT was obtained with a Token Exchange using DPoP?

https://datatracker.ietf.org/doc/draft-parecki-oauth-jwt-dpop-grant/

DPoP for JWT Authorization Grant

This draft defines `urn:ietf:params:oauth:grant-type:`**`jwt-dpop`**

```
POST /token.oauth2 HTTP/1.1
Host: as.example.com
Content-Type: application/x-www-form-urlencoded
DPoP: eyJ0eXAiOiJkcG9wK2p3dCIsImFsZyI6IkVTMjU2IiwiandrI...

grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-type%3Ajwt-bearer
&assertion=eyJhbGciOiJFUzI1NiIsImtpZCI6IjE2In0.
eyJpc3Mi[...omitted for brevity...].
J9l-ZhwP[...omitted for brevity...]
```

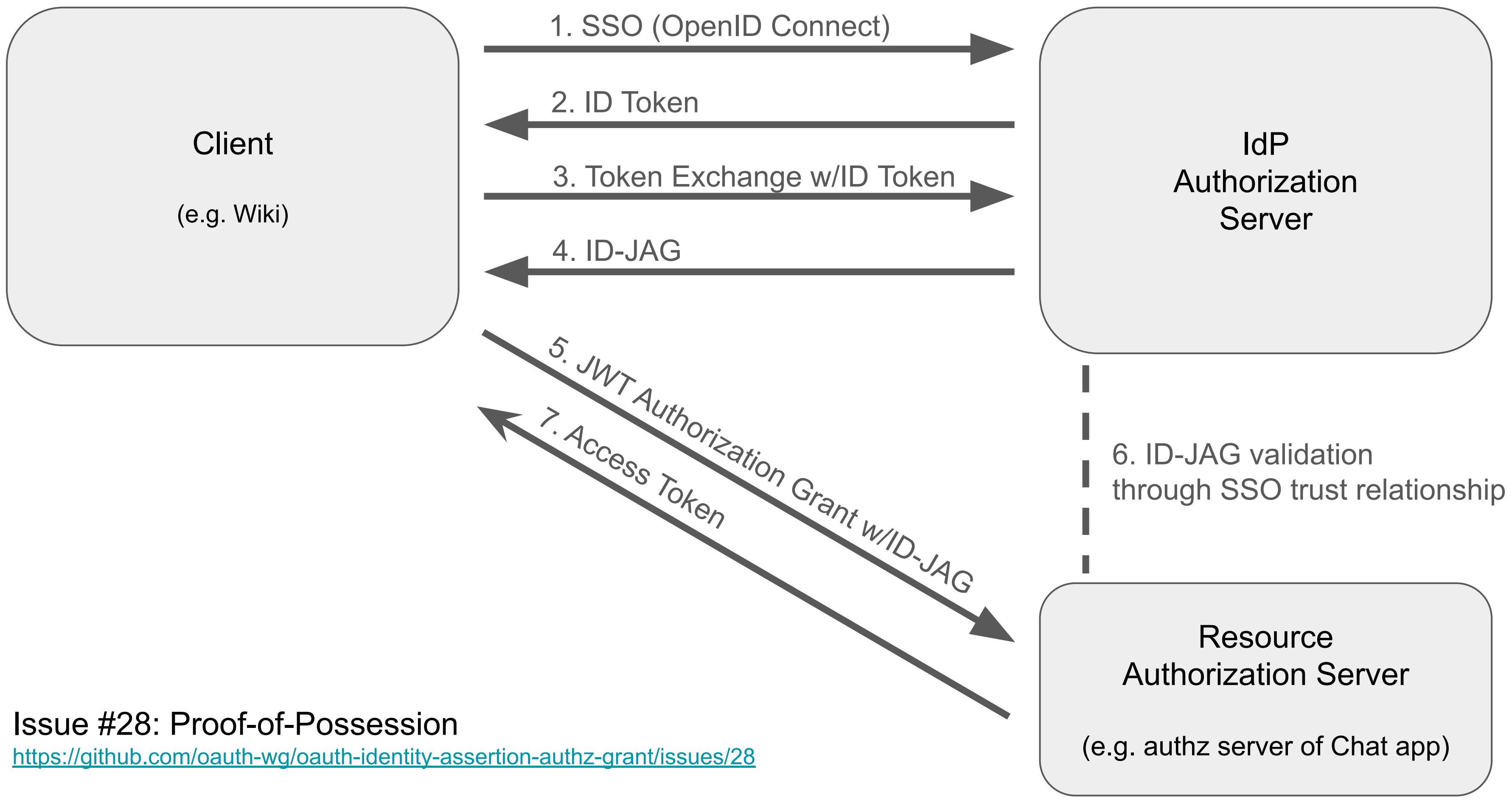
https://datatracker.ietf.org/doc/draft-parecki-oauth-jwt-dpop-grant/

Why?

End-to-end DPoP Binding for Identity Chaining

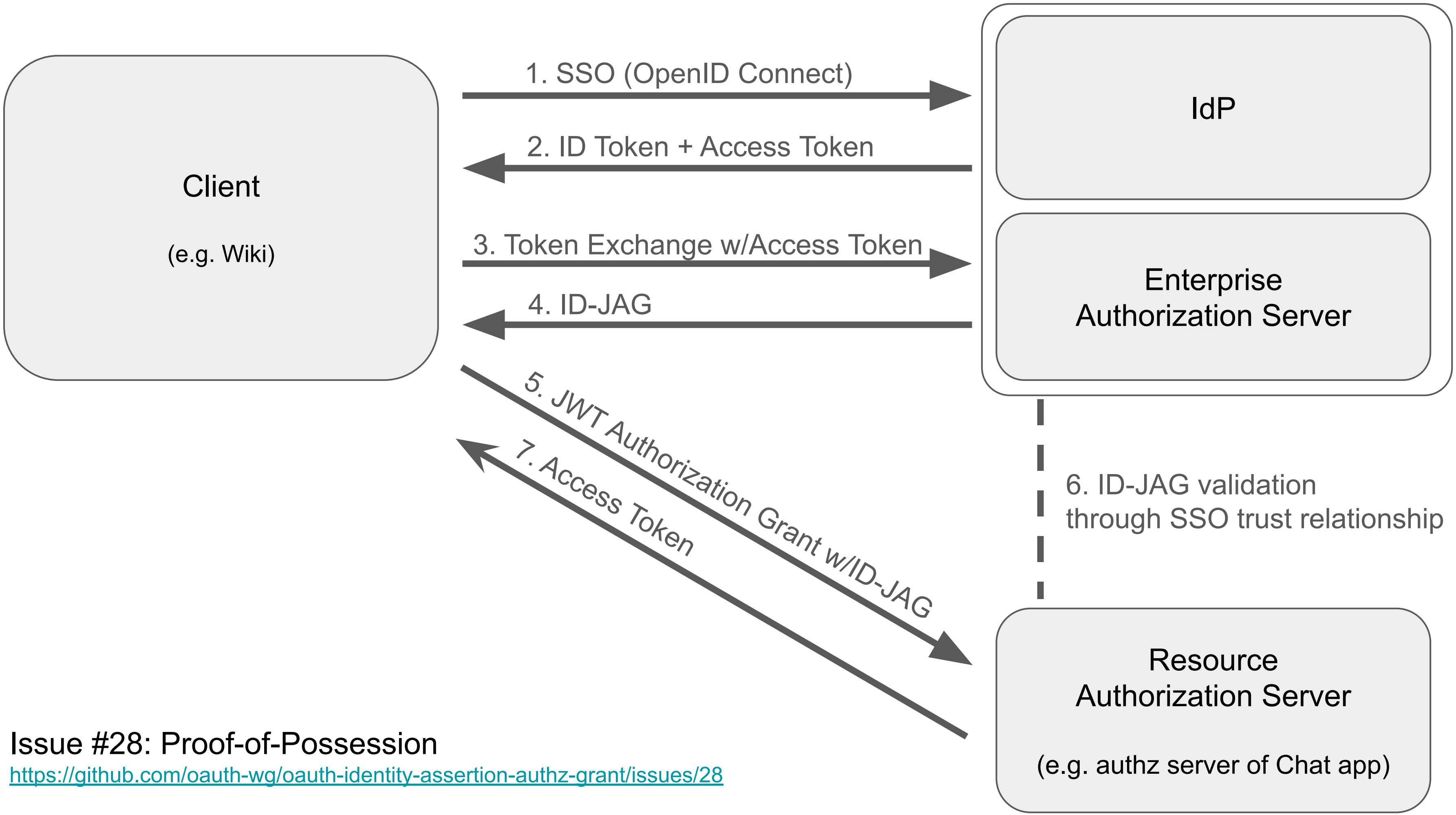
- [Out of scope] Obtain initial token
  - Covered by DPoP if initial token is Access Token
- [Token Exchange] Exchange initial token for JWT Assertion
  - Mostly covered by DPoP if you squint enough
- [JWT Assertion Grant] Exchange JWT Assertion for Access Token
  - Gap (need new `...:grant-type:jwt-dpop`)

https://datatracker.ietf.org/doc/draft-parecki-oauth-jwt-dpop-grant/



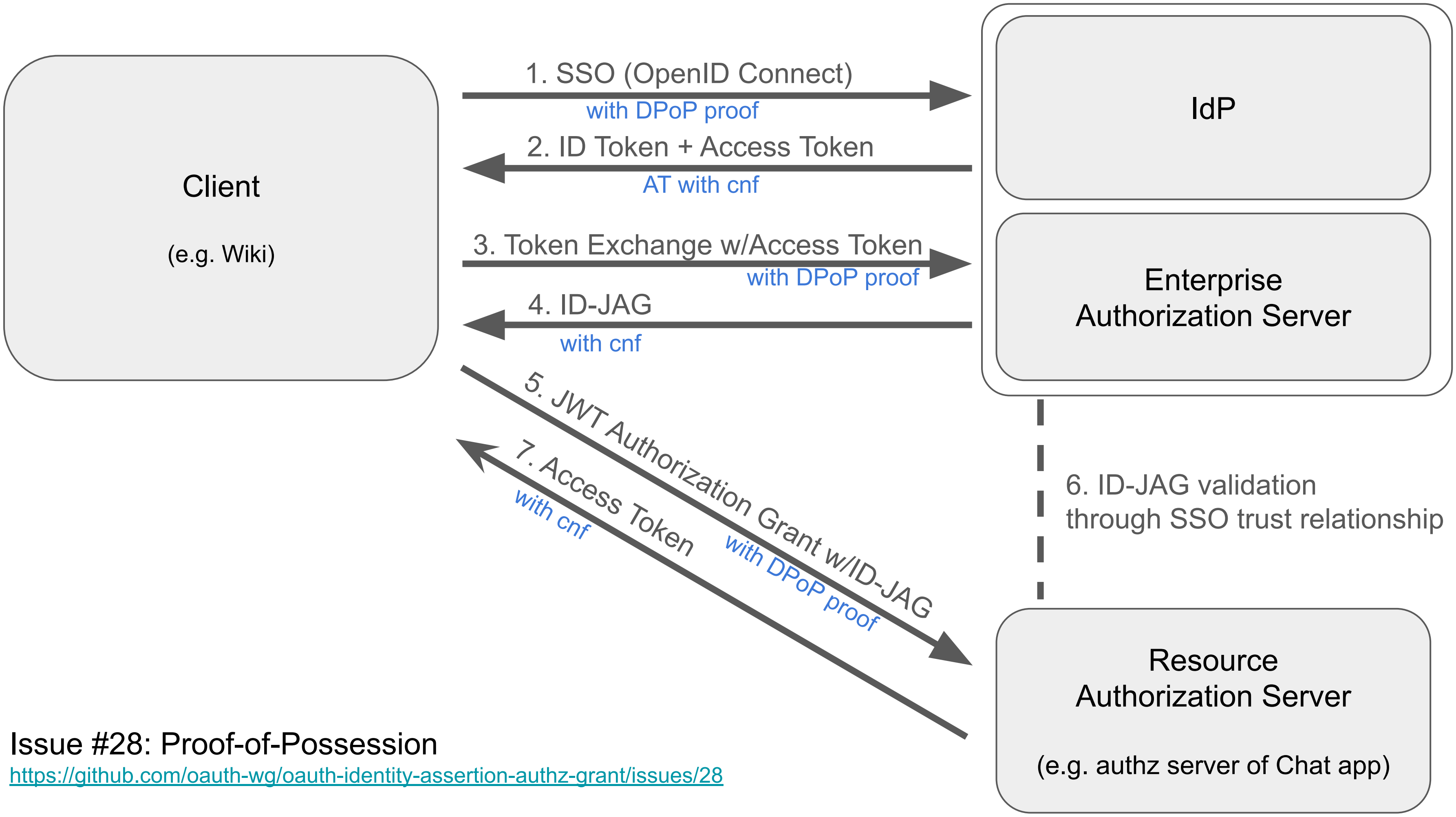
Issue #28: Proof-of-Possession

https://github.com/oauth-wg/oauth-identity-assertion-authz-grant/issues/28



Issue #28: Proof-of-Possession

https://github.com/oauth-wg/oauth-identity-assertion-authz-grant/issues/28



Issue #28: Proof-of-Possession

https://github.com/oauth-wg/oauth-identity-assertion-authz-grant/issues/28

Questions