DPoP:
Demonstrating Proof-of-Possession
[at the application layer]

Daniel Fett, John Bradley, Brian Campbell, Torsten Lodderstedt, Mike Jones

Problem Statement

- OAuth 2.0 Security BCP recommends use of sender-constrained tokens
- OAuth lacks suitable mechanism for SPAs
  - mTLS for OAuth 2.0 would cause UX issues in SPAs
  - Status of Token Binding is uncertain

Main Goal

Under the attacker model defined in [I-D.ietf-oauth-security-topics], the mechanism defined by this specification tries to ensure **token replay at a different endpoint is prevented**.

More precisely, if an adversary is able to get hold of an access token because it set up a counterfeit authorization server or resource server, the adversary is not able to replay the respective access token at another authorization or resource server.

Scope of the Proposal

- Define Proof of Possession mechanisms on application level that can be combined with any client type and client authentication method
- Closely follow Token Binding for OAuth design
- Signatures used for proof of possession and replay detection only
- Message integrity relies on TLS

Current Proposal

```
+--------+                               +---------------+
|        |                               |               |
|        |--(A)- Authorization Request ->|   Resource    |
|        |                               |     Owner     |
|        |<-(B)-- Authorization Grant ---|               |
|        |                               +---------------+
|        |
|        |                               +---------------+
|        |--(C)-- Token Request -------->|               |
| Client |        (DPop-Binding)         | Authorization |
|        |                               |     Server    |
|        |<-(D)-- PoP Access Token ------|               |
|        |                               +---------------+
|        |        PoP Refresh Token for public clients
|        |
|        |                               +---------------+
|        |--(E)-- PoP Access Token ----->|               |
|        |        (DPoP-Proof)           |    Resource   |
|        |                               |     Server    |
|        |<-(F)--- Protected Resource ---|               |
|        |                               +---------------+
|        |
|        | public client refresh token usage:
|        |                               +---------------+
|        |--(G)-- PoP Refresh Token ---->|               |
|        |        (DPoP-Proof)           | Authorization |
|        |                               |     Server    |
|        |<-(H)-- PoP Access Token ------|               |
|        |                               +---------------+
|        |
+--------+
```

DPoP JWT

```
{
    "typ": "dpop_binding+jwt",
    "alg": "ES512",
    "jwk": {
         "kty" : "EC",
         "kid" : "11",
         "crv" : "P-256",
         "x" : "usWxHK2PmfnHKwXPS54m0kTcGJ90UiglWiGahtagnv8",
         "y" : "3BttVivg+lSreASjpkttcsz+1rb7btKLv8EX4"
     }

}.{
    "jti": "HK2PmfnHKwXP",
    "http_method": "get",
    "http_uri": "https://server.example.com",
    "exp": "..."
}
```

To-dos

- Syntax clarifications (http_method? typ?)
- Thorough security review, completion of security considerations section
- Error codes
- ...