

OAuth 2.0 Attestation-Based Client Authentication

A nighttime photograph of a city skyline reflected in a river. The sky is dark, and the city lights are bright. A large Ferris wheel is illuminated with blue lights on the right side. The river in the foreground shows clear reflections of the buildings and lights.

Tobias Looker, Paul Bastian

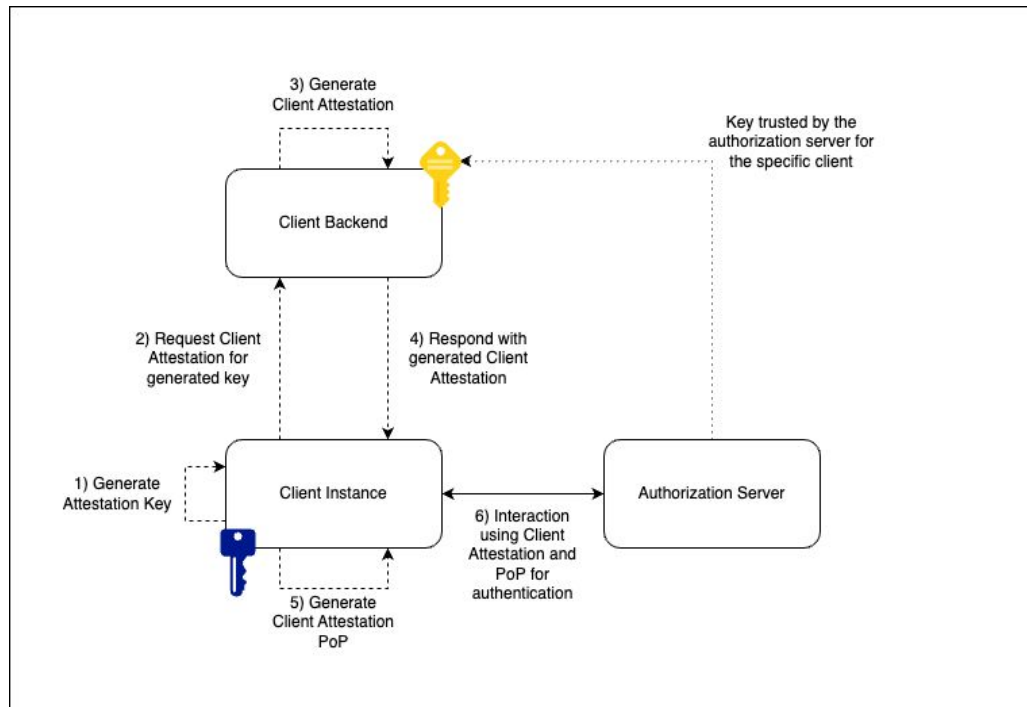


Motivation

- Environments that *public* clients are operating/deployed in increasingly have primitives that can be used for client authentication examples such as:
 - [App Attest on iOS](#) for Native iOS applications
 - [Play Integrity](#) on Android for Native Android applications
- The question is how to appropriately use these capabilities to allow clients to authenticate with an authorization server?

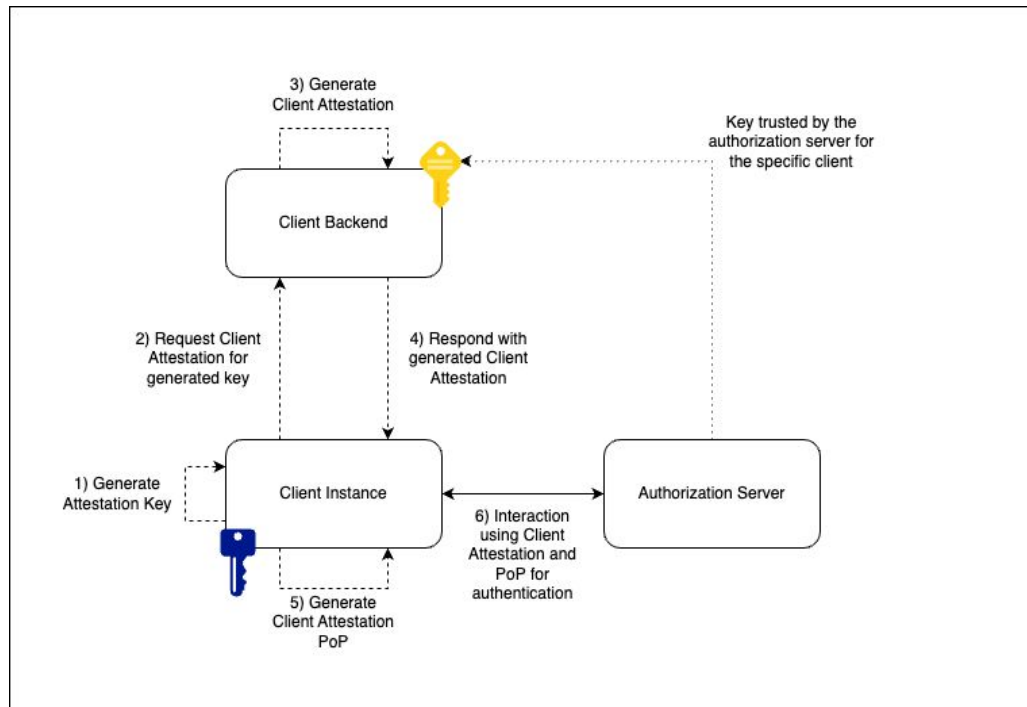
Proposed Solution

- Extends the established framework of RFC7521 for a new form of client authentication
- Client instance obtains an attestation from client backend
- Client backend may perform any number of security checks before issuing a key-bound attestation JWT to the client instance
- Client instance authenticates towards Authorization server during a token or PAR request
- **Note** - how the client communicates with the client backend in steps 2&4 are out of scope

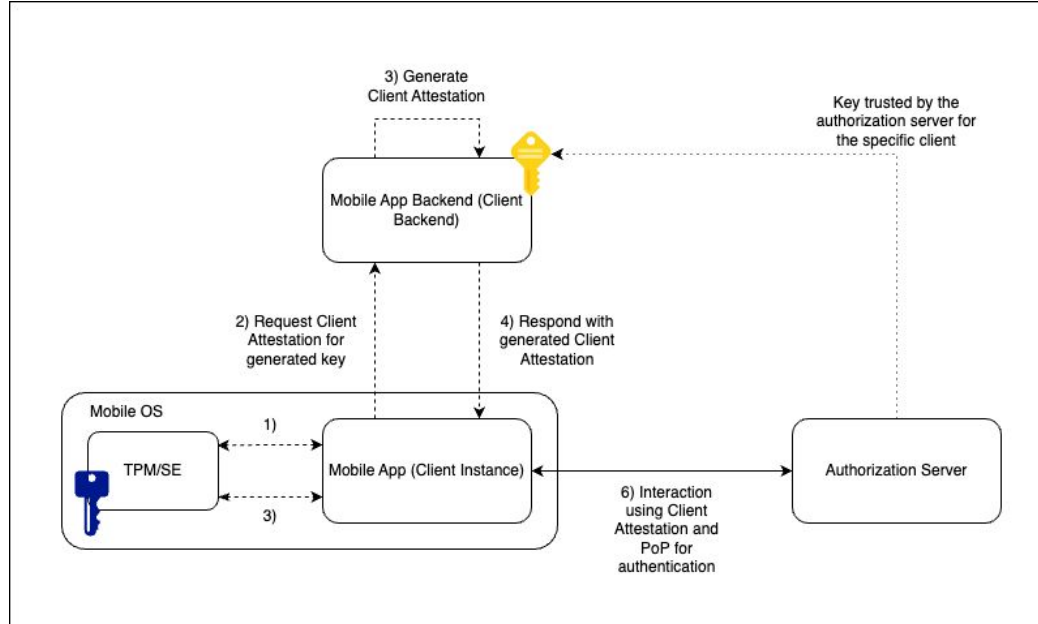


Key Callouts

- Proof of possession enabled client authentication method
- Can be used to authenticate the key used to bind to an access token via DPOp
- Direct mode of authentication between the client instance and the authorization server rather than a backend for front end pattern
- Avoids the client instance from having to register with the AS via DCR



Native App Example





Example - Token Request

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

grant_type=authorization_code&
code=n0esc3NRze7LTCu7iYzS6a5acc3f0ogp4&
client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3A
client-assertion-type%3Ajwt-client-attestation&
client_assertion=eyJhbGciOiJSUzI1NiIsImtpZCI6IjIyIn0.
eyJpc3MiOiIjIyIn0.eyJpc3MiOiIjIyIn0.eyJpc3MiOiIjIyIn0.
cC4hiUPo[...omitted for brevity...]~eyJzI1NiIsImtpZCI6IjIyIn0.
IjIyIn0[...omitted for brevity...].
i0iJSUzI1[...omitted for brevity...]
```




Example - Token Request

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

```
grant_type=authorization_code&
code=n0esc3NRze7LTCu7iYzS6a5acc3f0ogp4&
client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3A
client-assertion-type%3Ajwt-client-attestation&
client_assertion=eyJhbGciOiJIUzI1NiIsImtpZCI6IjIyIn0.
eyJpc3MiOiIiLCJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiIsImtpZCI6IjIyIn0.
cC4hiUPo[...omitted for brevity...]~eyJzI1NiIsImtpZCI6IjIyIn0.
IjIyIn0[...omitted for brevity...]
i0iJSUzI1[...omitted for brevity...]
```

New assertion type



Example - Token Request

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

```
grant_type=authorization_code&
code=n0esc3NRze7LTCu7iYzS6a5acc3f0ogp4&
client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3A
client-assertion-type%3Ajwt-client-attestation&
client_assertion=eyJhbGciOiJIUzI1NiIsImtpZCI6IjIyIn0.
eyJpc3MiOiIiLCJ1IjIyIn0.
cC4hiUPo[...omitted for brevity...]~eyJzIjIyIn0.
IjIyIn0[...omitted for brevity...]
i0iJSUzI1[...omitted for brevity...]
```

Two JWTs concatenated via a '~' character

- Client Attestation
- Client Attestation PoP



Example - Client Assertion

Client Attestation

```
eyJhbGciOiAiRVMyNTYiLCJraWQiOiAiMTEifQ.eyJpc3MiOiJodHRwczovL2NsaWVudC5leGFtcGxlLmNvbSIsInN1YiI6Imh0dHBzOi8vY2xpZW50LmV4YW1wbGUuY29tIiwibmJmIjoxMzAwODE1NzgwLCJleHAiOjEzMDA4MTkzODAsImNuZiI6eyJqd2si0nsia3R5IjoirUMiLCJ1c2UiOiJzaWciLCJjcniOiJQLTI1NiIsIngiOiIxOHdITGVJZ1c5d1Z0NlZEMVR4Z3BxeTJM3pZa01mNko4bWpWQWlidmhNIiwieSI6Ii1WNGRTNFVhTE1nUF80Zlk0ajhpcjdjbDFUWGxGZEFnY3g1NW83VGtjU0EifX19.Sf1KxwRJSMeKKF2QT4fwpMeJf36P0k6yJV_adQssw5c~eyJhbGciOiJFUzI1NiJ9.eyJpc3MiOiJodHRwczovL2NsaWVudC5leGFtcGxlLmNvbSIsImF1ZCI6Imh0dHBzOi8vYXMuZXhhbXBsZS5jb20iLCJuYmYiOiJzMDA4MTU3ODAsImV4cCI6MTMwMDgxOTM4MH0.coB_mtdXwvi9RxSMzbIey8GVVQLv9qQrBUqmc1qj9BS
```

Client Attestation PoP

Note signatures are invalid



Example - Client Attestation

```
{
  "alg": "ES256",
  "kid": "11"
}
.
{
  "iss": "https://client.example.com",
  "sub": "https://client.example.com",
  "nbf": 1300815780,
  "exp": 1300819380,
  ... //other claims
  "cnf": {
    "jwk": {
      "kty": "EC",
      "crv": "P-256",
      "x": "18wHLeIgW9wVN6VD1Txgpqy2LszYkMf6J8njVAibvhM",
      "y": "-V4dS4UaLMgP_4fY4j8ir7c11TX1FdAgcx55o7TkcSA"
    }
  }
}
```



Example - Client Attestation

```
{
  "alg": "ES256",
  "kid": "11"
}
.
{
  "iss": "https://client.example.com",
  "sub": "https://client.example.com",
  "nbf": 1300815780,
  "exp": 1300819380,
  ... //other claims
  "cnf": {
    "jwk": {
      "kty": "EC",
      "crv": "P-256",
      "x": "18wHLeIgW9wVN6VD1Txgpqy2LszYkMf6J8njVAibvhM",
      "y": "-V4dS4UaLMgP_4fY4j8ir7c11TX1FdAgcx55o7TkcSA"
    }
  }
}
```

Key used to verify the Client Attestation PoP





Use Cases

- Potentially applicable to any OAuth 2.0 Flow that uses Client Authentication
- Concrete applications include:
 - eIDAS 2.0 usage of OpenID for Verifiable Credentials
 - Software workload authorization - enabling ephemeral software workload instances to authenticate with authorization servers without having to register with the authorization server first



Why not other approaches

- **Private key JWT Based Client Authentication**
 - Is a bearer based authentication mechanism so vulnerable to certain modes of token thief
 - A client instance would likely have to obtain a new attestation from a client backend for every AS interaction involving client authentication
- **Backend for Front Style Client Authentication**
 - Confidentiality and privacy issues for certain use-cases such as verifiable credential issuance where requests/responses would proxy through the client backend



Questions?



Links

Current Editors Copy ->

<https://vcstuff.github.io/draft-looker-oauth-attestation-based-client-auth/draft-looker-oauth-attestation-based-client-auth.html>

Git Repository -> <https://github.com/vcstuff/draft-looker-oauth-jwt-cwt-status-list>