OAuth 2.0 Attestation-Based Client Authentication

- Refresher
- Updates since IETF 120
- Discussion points
- Q&A

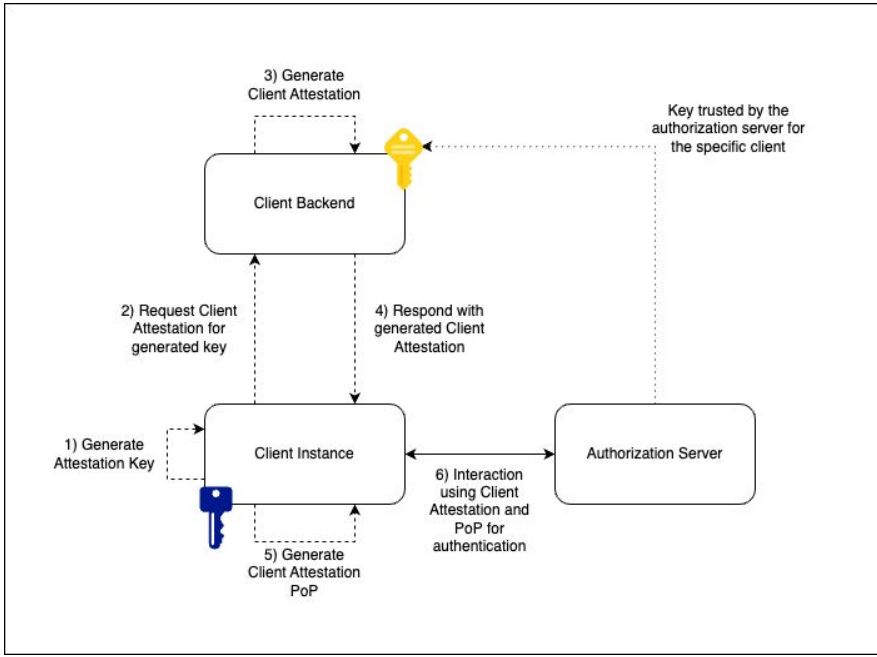
Tobias Looker, Paul Bastian, Christian Bormann

A Refresher - Motivation

- Backend vs frontend channel authentication
  - Classical OAuth Security model requires client authentication through a backend channel, which also causes the transaction to be conducted through the backend channel
  - In the context of OpenID4VCI and the Issuer-Holder-Verifier model, this creates significant privacy issues, as the backend gets to see all credentials/tokens
  - Establish **a mechanism for backend-attested client authentication through a front-end channel**
- Establish a mechanism to enable technologically independent attestations that give AS assurances about the security level of the Client

Architecture overview

- Client Backend attests a Client Instance with a Client Instance Key and provides a key-bound Client Attestation JWT
- Client Backend may perform any number of security checks before issuing a key-bound Client Attestation JWT to the client instance, however, steps 2 and 4 are out of scope
- Client Instance generates a Proof of Possession and utilize both to authenticate towards AS
- Avoids the client instance from having to register with the AS via DCR
    - May still work in conjunction with DCR



Changes since IETF 120

Changes: -04

- remove key attestation example
- restructured JWT Claims for better readability
- added JOSE typ values for Client Attestation and Client Attestation PoP
- add RATS relation
- add concatenated representation without headers
- add PAR endpoint example
- fix PoP examples to include jti and nonce
- add iana http field name registration

Key Attestation vs Client Attestation

- Lesson learned: Client attestation and Key attestation are different things and should be treated differently depending on use-case / context
- Client Attestation:
  - An attestation to establish trust in an unknown client. Can contain details about the client system, trust ecosystem etc.
- Key Attestation:
  - An attestation to establish trust in a key, especially details about key storage etc.

- We decided to remove the key attestation parts from the specification - can still be used within a client attestation depending on ecosystem specific payload, but not defined in the spec

Discussion to nonce fetching

- Section 7.1 on Replay Attack Detection recommends nonce over jti
- However, explicit nonce fetching mechanism is not described yet
  - Consider reusing DPoP mechanism, yet DPoP integration is thought to be optional
  - Require independent mechanism
- Thoughts so far:
  - As we move to header syntax, request nonce via headers
  - DPoP mechanism may result in nonce being too old and AS requesting new DPoP proof with fresh nonce
    - This may be very costly in the context of this draft when using hardware-backed crypto(external or remote HSM)
    - Otherwise requesting a new nonce with HTTP 400 result
  - Enable new mechanism for the Client to explicitly request a new nonce, i.e. new header OAuth-Client-Attestation-Nonce
    - Especially useful for Client Authentication at PAR endpoint without prior interaction

DPoP Optimization

```
POST /token HTTP/1.1
Host: as.example.com
Content-Type: application/x-www-form-urlencoded
DPoP:
eyJ0eXAiOiJkcG9wK2p3dCIsImp3ayI6eyJhbGciOiJFUzI1NiIsImNydiI6IlAtMjU2Iiwia3R5IjoiRUMiLCJ4IjoiaThReW03NFRNUHVLQXV
KUGlZczFSZlVsYTVjemNxelVobEpmRHNMdzd0NCIsInkiOiJGQjlUY2ZmeVZDSEpFQjJjejc4NTE2MUE0SmxlTkh2cG44bXhHRldZMlNjIn0sIm
FsZyI6IkVTMjU2In0.eyJqdGkiOiIzNTc2ODI5Ny1kZWM1LTQ2ZjYtODVlNS1iNzU4MjE2YWI1ZmYiLCJodG0iOiJQT1NUIiwiaHR1IjoiaHR0c
HM6Ly9hcy5leGFtcGxlL3Rva2VuIiwiaWF0IjoxNzAwODEyODAwLCJub25jZSI6ImV5SjdTX3pHLmV5SkgwLVouSFg0dy03diJ9.5VuDrkd8RhM
Raps_AzJBs2p-_UXXWT4dVHITBHiQxe31GeDq81otnIh3HBQN8_XjS1diHPq1tti1pn55eZdI5g
OAuth-Client-Attestation: eyJhbGciOiJSUzI1NiIsImtpZCI6IjIyIn0.eyJpc3Mi[...omitted for brevity...].
cC4hiUPo[...omitted for brevity...]

grant_type=authorization_code&
code=n0esc3NRze7LTCu7iYzS6a5acc3f0ogp4&
```

Client Attestation PoP via DPoP syntax

Client Attestation via new header

Questions?