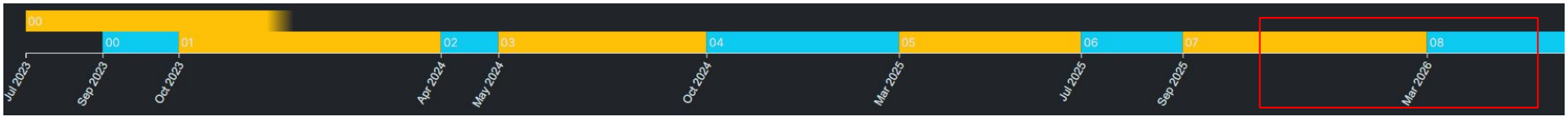
# OAuth 2.0 Attestation-Based Client Authentication

- Updates since IETF 124
- Discussion points
- Q&A

*Tobias Looker, Paul Bastian, Christian Bormann*

# Changes since IETF 124



# Changes since IETF 124

## Incorporating feedback from IETF 124 & some cleanup

- 08

- remove concatenated Serialization for Client Attestations
- update all examples (removal of iss and nbf)
- remove iss from Client Attestation JWT and Client Attestation PoP JWT
- add small security consideration sub-section for MAC-based deployments
- remove public clients reference and clarify this draft targets confidential clients
- clarify this may be a client authentication mechanism but also may be not
- add examples for RS usage and non client authentication
- add note on protocols providing a challenge on previous responses
- add structured-type to iana header field registration requests
- moving Authorization Server metadata into it's own top level section
- editorial fixes

# Changes since IETF 124

## Restructuring & combined mode (DPoP)

- 09 (editor's copy)

- restructure draft
- rephrase introduction text
- add challenge request/response to graphic
- Add combined DPoP mode

# Current State of the draft

- Added most missing sections
- Focused on improving readability (restructure, improve clarity of introduction etc.)
- We proposed one bigger update that was also discussed several times before: the combined DPoP presentation

# DPoP Combined mode

As previously discussed there are complexities created when client attestation and dpop are used together that warrant an optimisation for implementations that wish for the DPoP key and Client Attestation PoP key to be the same.

PR #146 merged in editor's copy

- We tried to incorporate all feedback from previous discussions
- Restructured overall draft to make it easier to describe both modes
- **Please review!**

# Client Attestation + DPoP Without Optimization

```
POST /token HTTP/1.1
Host: as.example.com
Content-Type: application/x-www-form-urlencoded
OAuth-Client-Attestation: eyJhbGciOiJSUzI1NiIsImtpZCI6IjIyIn0.eyJpc3Mi[...omitted for brevity...].
cC4hiUPo[...omitted for brevity...]
OAuth-Client-Attestation-PoP: eyJzI1NiIsImtphbGciOimtpZCI6IjIyIn0.
IjIyIn0[...omitted for brevity...].
iOiJSUzI1[...omitted for brevity...]
DPoP:
eyJ0eXAiOiJkcG9wK2p3dCIsImp3ayI6eyJhbGciOiJFUzI1NiIsImNydiI6IlAtMjU2Iiwia3R5IjoiRUMiLCJ4IjoiaThReW03NFRNUHVLQXV
KUGlZczFSZlVsYTVjemNxelVobEpmRHNMdzd0NCIsInkiOiJGQjlUY2ZmeVZDSEpFQjJjejc4NTE2MUE0SmxlTkh2cG44bXhHRldZMlNjIn0sIm
FsZyI6IkVTMjU2In0.eyJqdGkiOiIzNTc2ODI5Ny1kZWM1LTQ2ZjYtODVlNS1iNzU4MjE2YWI1ZmYiLCJodG0iOiJQT1NUIiwiaHR1IjoiaHR0c
HM6Ly9hcy5leGFtcGxlL3Rva2VuIiwiaWF0IjoxNzAwODEyODAwLCJub25jZSI6ImV5SjdTX3pHLmV5SkgwLVouSFg0dy03diJ9.5VuDrkd8RhM
Raps_AzJBs2p-_UXXWT4dVHITBHiQxe31GeDq81otnIh3HBQN8_XjS1diHPq1tti1pn55eZdI5g


grant_type=authorization_code&
code=n0esc3NRze7LTCu7iYzS6a5acc3f0ogp4&
```

1. Client Attestation

2. Client Attestation PoP

3. DPoP proof for access_token

# Client Attestation + DPoP With Optimization

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

grant_type=authorization_code&
code=n0esc3NRze7LTCu7iYzS6a5acc3f0ogp4&
```

Client Attestation

DPoP proof fulfills the role of the Client Attestation PoP and for access_token

# DPoP Combined mode: AS Support

Support signaled via new auth method (in *token_endpoint_auth_methods_supported*)

- ***attest_jwt_client_auth_dpop*:** signals support for combined mode
- ***attest_jwt_client_auth*:** “normal” mode

# Path Forward

- We hope to close all remaining issues in the coming weeks
- Looking for reviews & WGLC after that

Currently:

- 17 open issues
- ~6 clear todos / ready for PR
- We have some open questions

# Open Questions / Issues

#56, #114: Bind to other OAuth artefacts?

#61: Relationship to DCR? Should this explicitly be mentioned?

#107: Should we provide more guidance for other use-cases?

#170: Does Client metadata make sense here?

# Questions?