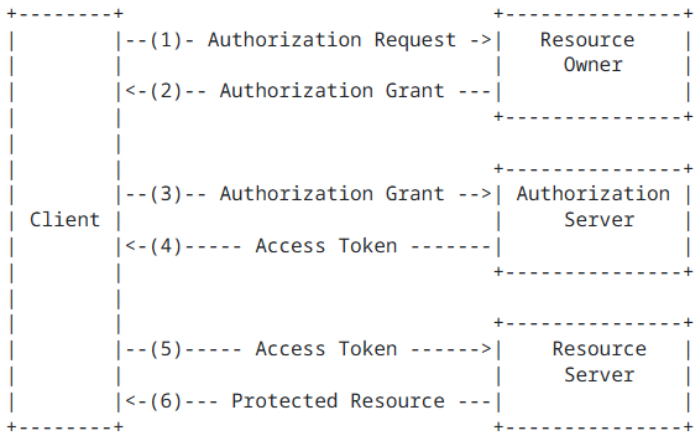
OAuth 2.0 Delegated Authorization

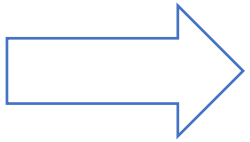
draft-li-oauth-delegated-authorization

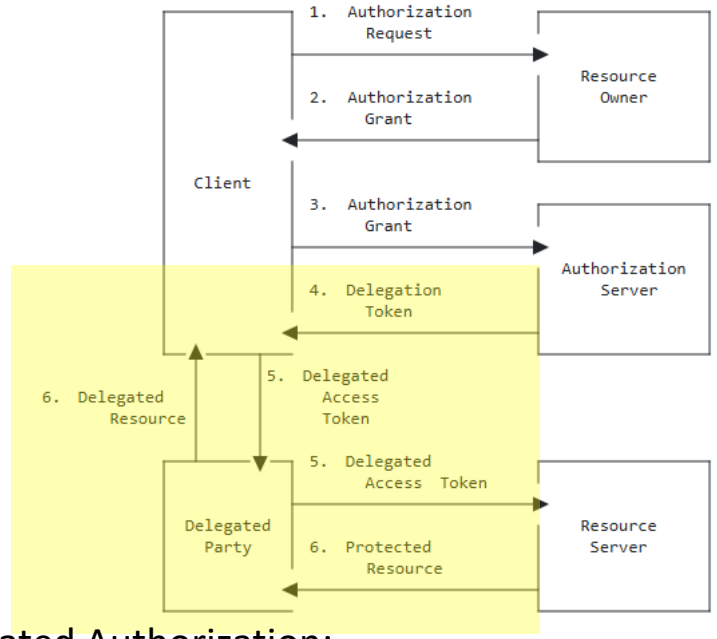
Ruochen Li, Haiguang Wang, Chunchi Peter Liu, Tieyan Li

Huawei

Delegated Authorization – Protocol Flow







OAuth 2.0:

- Client gets an **access token** from AS, and uses it to access RS

Problems:

- Down-scoping not possible…
  - without Token Exchange*
- Token generation relies on AS

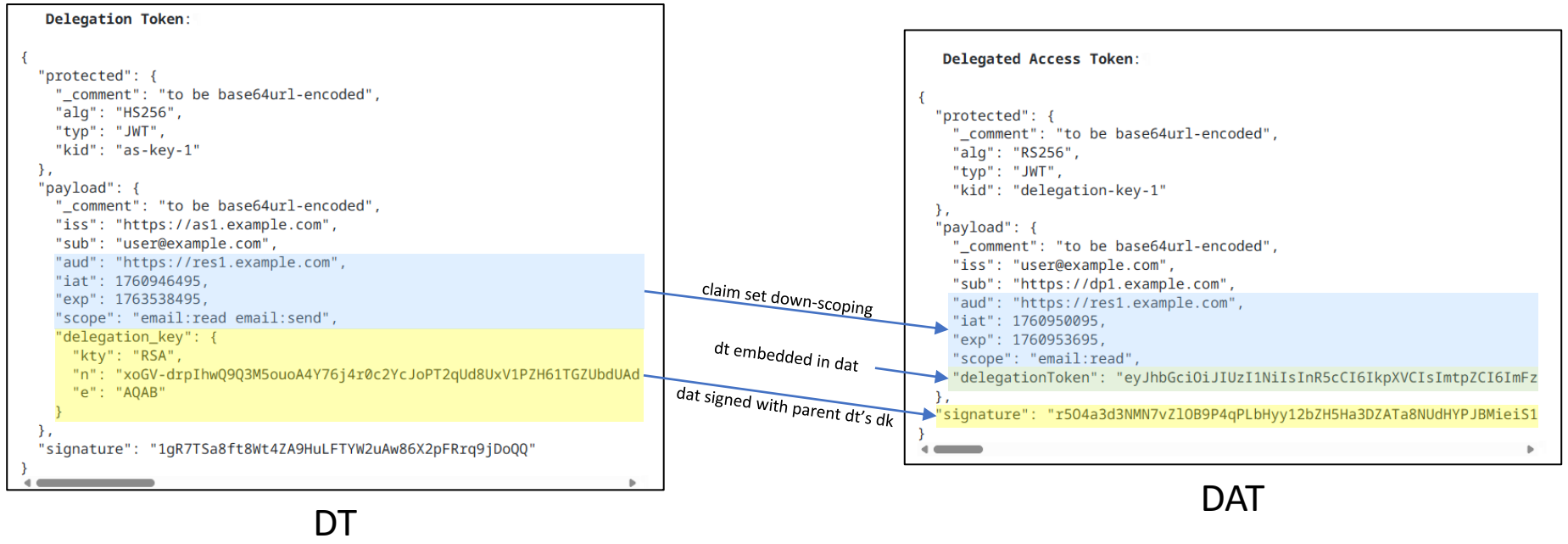
Delegated Authorization:

- Client gets a **delegation token (dt)** from AS
- Client issues a **delegated access token (dat)**
- Client uses the **dat** to delegate auth to **Delegated Party (DP)**
- Client uses the **dat** to access RS via **DP**

Key points:

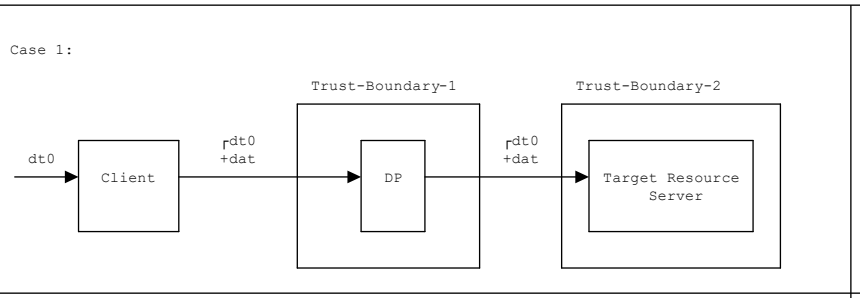
- Digital-signature-linked token chain similar to PKI certs
  - only DATs are accepted by RS, DTs alone not accepted
- RO requests one token from AS, client performs down-scoping
- DATs generated locally

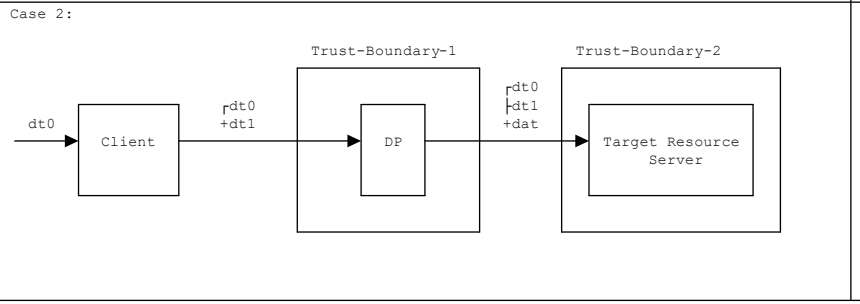
Delegated Authorization – Token Format (JWT)

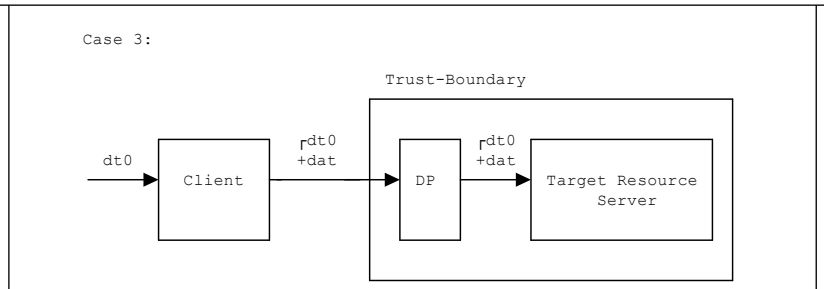


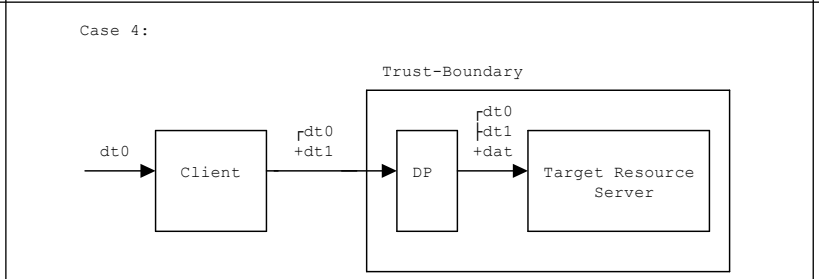
- Support authorization code grant, etc.
- Rich Authorization Request (in addition to scope)
- Delegated Authorization header, DP metadata
- RS local verification of DAT & token introspection
- DT supports encrypted tokens (JWE). DAT supports sign-then-encrypt tokens

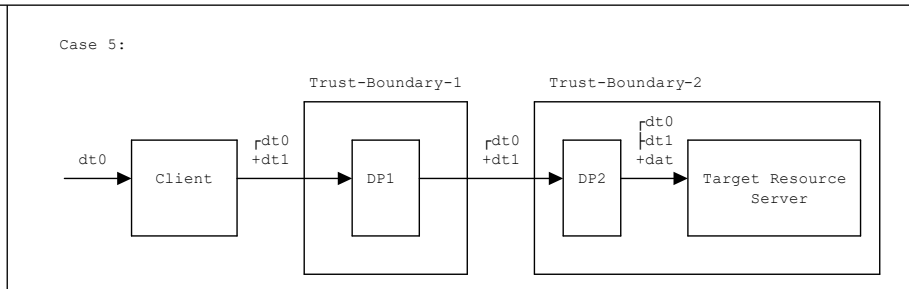
Delegated Authorization – Use Scenarios

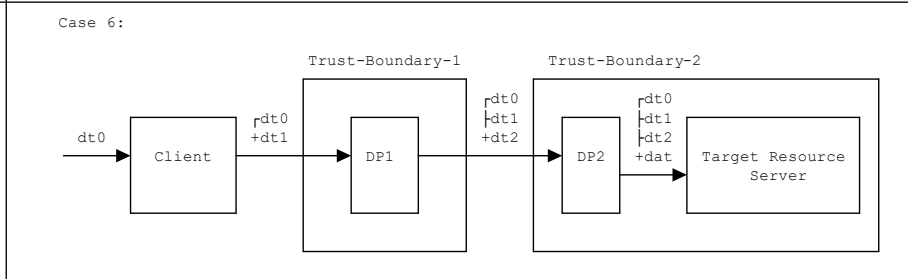












Cases 1, 3:

- DT → DAT
- Client to issue DAT

Cases 2, 4, 5, 6 (yet to be added to the draft):

- DT → … → DT → DAT
- Client/DPs to issue DT/DAT

Comparison with RFC8693 Token Exchange

Token Exchange / Transaction Token	Delegated Authorization
Creating output tokens involves an external service (STS)	Creating subordinate tokens does not involve external services
Output token not tightly linked with input token	Subordinate token directly linked to the superior delegation token
Token exchange normally happens within the trust domain of the target resource	Delegation can happen at any node along the invocation chain, including the original OAuth client and intermediate third party services
Input tokens are valid access tokens	Delegation tokens are NEVER used as access tokens. Only delegated access tokens are accepted as access tokens.

Future Work

- Define token format for DT, DAT
- Multiple layers of delegation (multiple DPs in the middle)
- Multiple DTs in a request (DP to access multiple backend RSes)

Comments / Feedbacks?