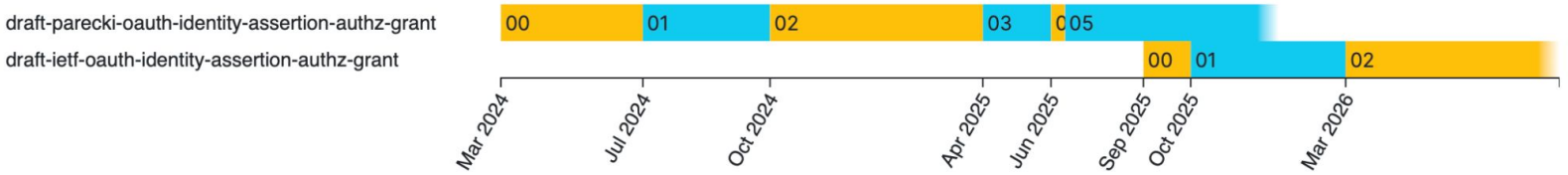
IETF 125
Shenzhen
March 2026
Aaron Parecki
Karl McGuinness
Brian Campbell
Identity Assertion Authorization Grant
https://datatracker.ietf.org/doc/draft-ietf-oauth-identity-assertion-authz-grant/
draft -02

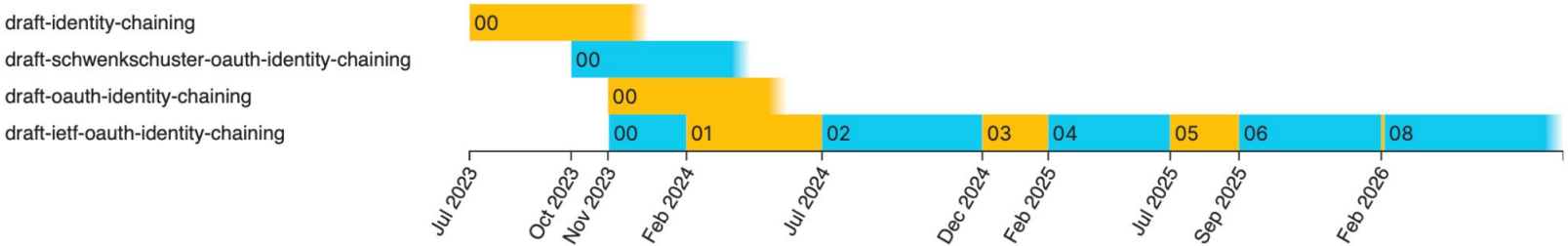
Identity Assertion Authorization Grant

https://datatracker.ietf.org/doc/draft-ietf-oauth-identity-assertion-authz-grant/

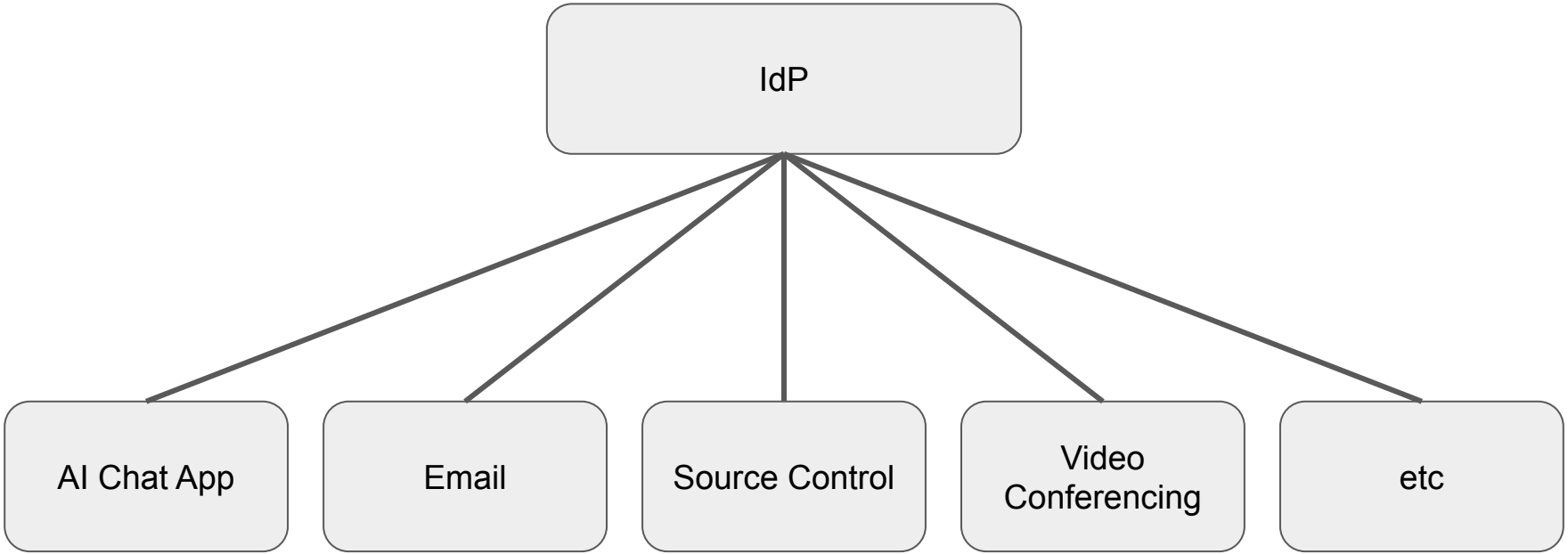


A profile of "OAuth Identity and Authorization Chaining Across Domains"

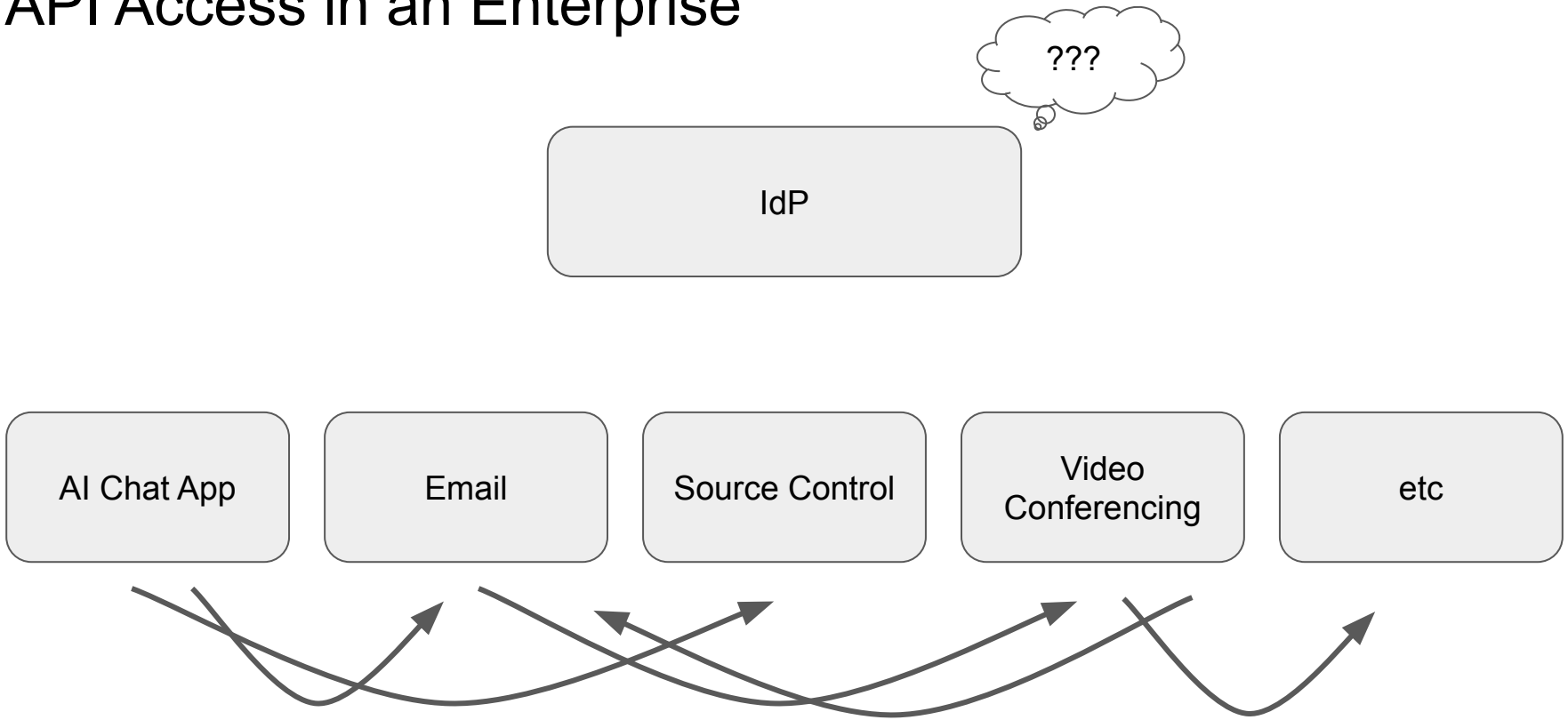
https://datatracker.ietf.org/doc/draft-ietf-oauth-identity-chaining/

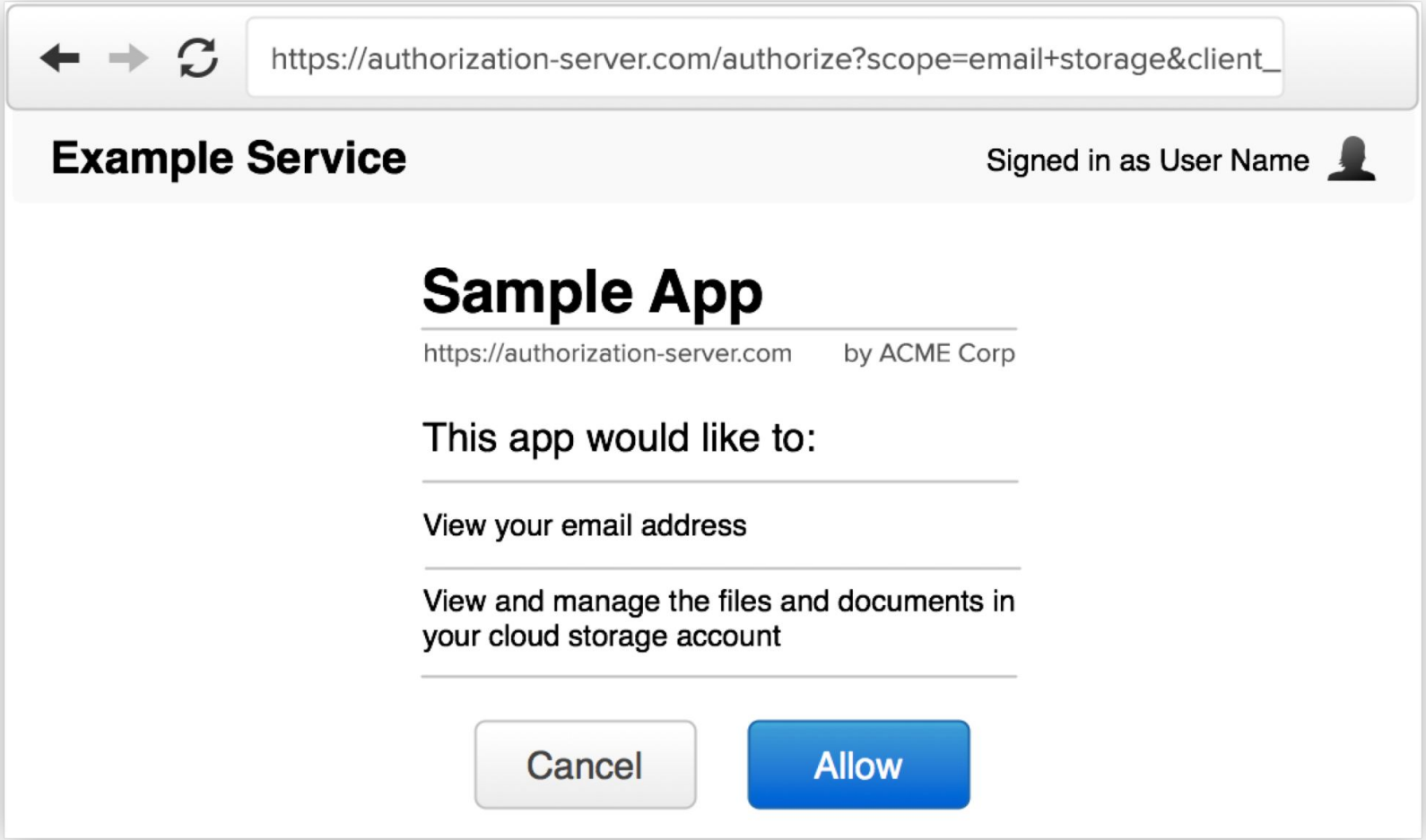


Single Sign-on in an Enterprise



API Access in an Enterprise




https://authorization-server.com/authorize?scope=email+storage&client_
Example Service
Signed in as User Name
Sample App
https://authorization-server.com
by ACME Corp
This app would like to:
View your email address
View and manage the files and documents in your cloud storage account
Cancel
Allow

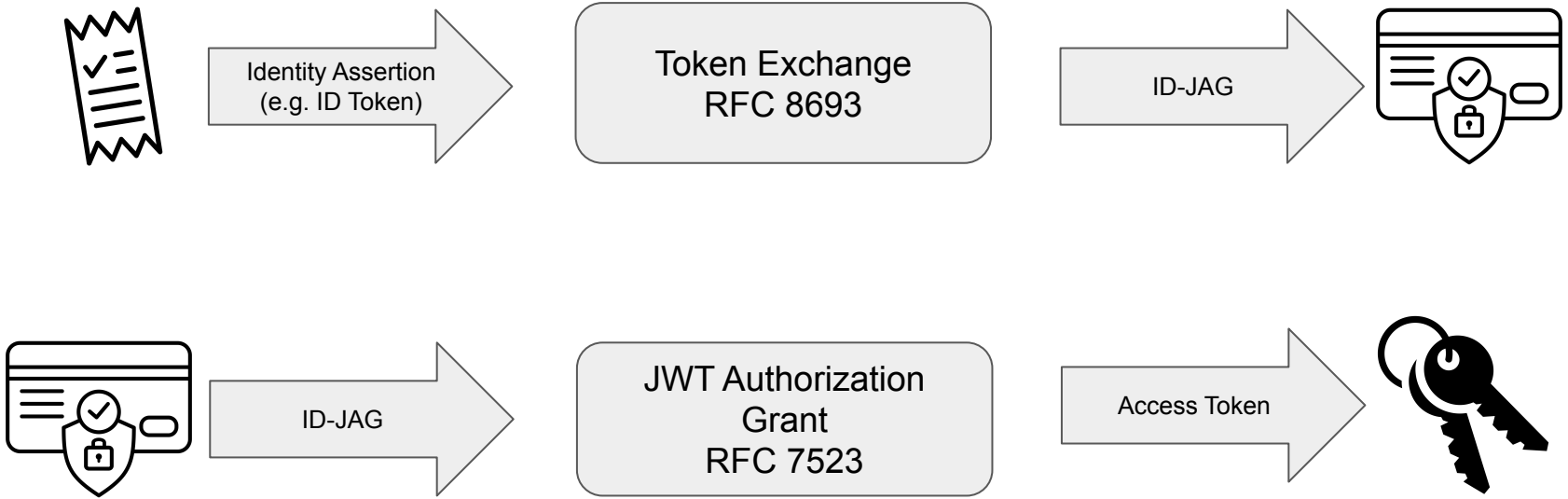
Identity Assertion Authorization Grant

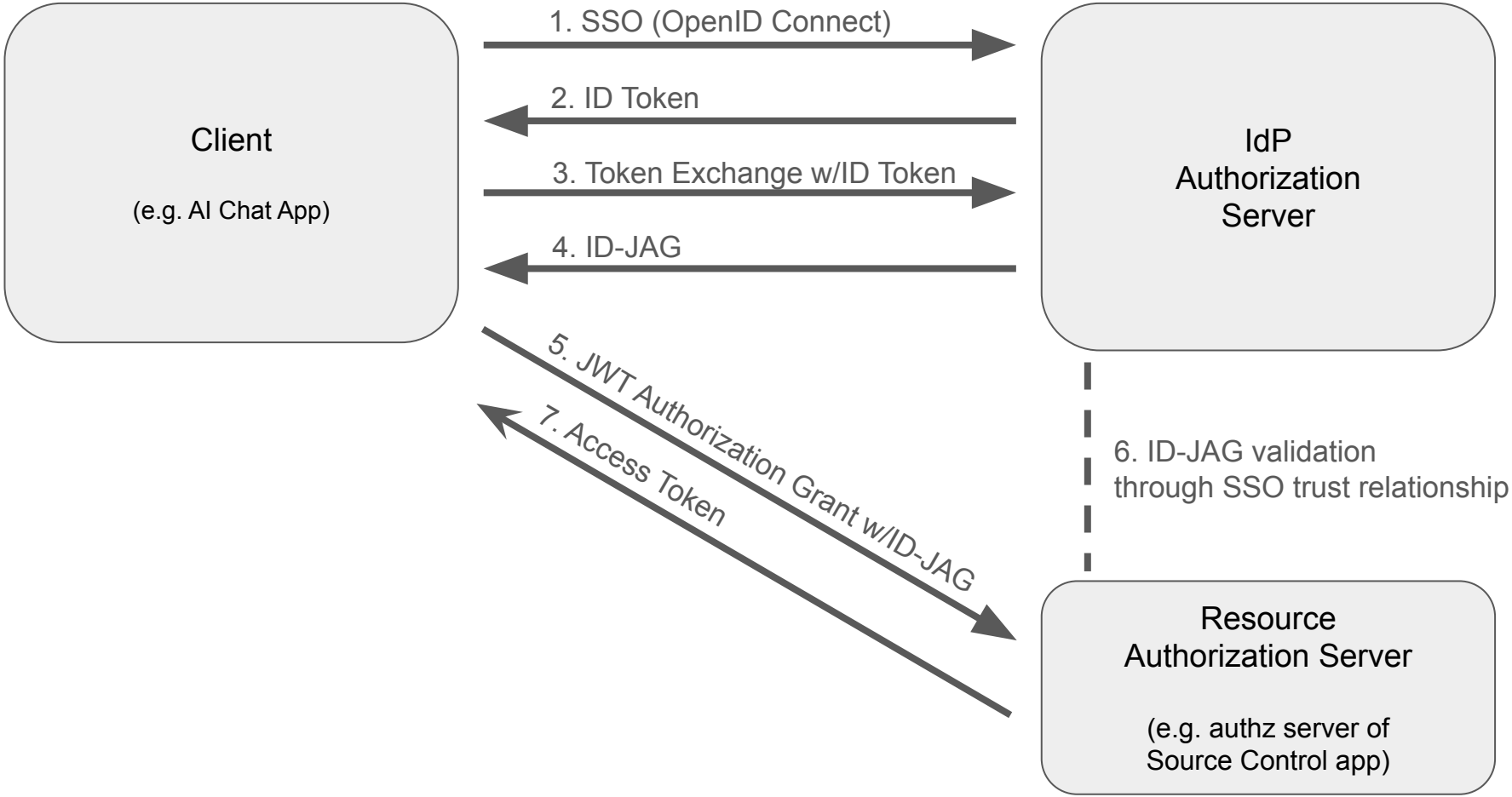
https://datatracker.ietf.org/doc/draft-ietf-oauth-identity-assertion-authz-grant/

Goals:

- Extend single sign-on to API access between apps
- Reduce user friction
- Enable enterprise control of data sharing between apps

Building Blocks




Client
(e.g. AI Chat App)
1. SSO (OpenID Connect)
2. ID Token
3. Token Exchange w/ID Token
4. ID-JAG
5. JWT Authorization Grant w/ID-JAG
7. Access Token
IdP
Authorization
Server
6. ID-JAG validation
through SSO trust relationship
Resource
Authorization Server
(e.g. authz server of
Source Control app)

ID-JAG (Identity Assertion JWT Authorization Grant)

```
{
  "typ": "oauth-id-jag+jwt"
}
.
{
  "jti": "9e43f81b64a33f20116179",
  "iss": "https://acme.idp.example",
  "sub": "U019488227",
  "aud": "https://acme.chat.example/",
  "client_id": "f53f191f9311af35",
  "exp": 1311281970,
  "iat": 1311280970,
  "scope": "chat.read chat.history"
}
.
signature
```

What’s new since IETF 124?

There are a handful of new in-progress implementations, some open source and some closed source.

MCP now references this as an MCP Authorization Extension
https://modelcontextprotocol.io/specification/2025-11-25/basic/authorization#mcp-authorization-extensions

Changes in version -02

Based on most common implementer feedback

- DPoP
- RAR
- Refresh token as subject token input
- Support for multi-tenant systems

Changes in version -02

- Added an example describing how to do DPoP with the flow (relies on draft-parecki-oauth-jwt-dpop-grant as presented at IETF 124)

The client generates a key pair and includes a DPoP proof JWT in the `DPoP` header of the Token Exchange request:

```
POST /oauth2/token HTTP/1.1
Host: acme.idp.example
Content-Type: application/x-www-form-urlencoded
DPoP: eyJ0eXAiOiJkcG9wK2p3dCIsImFsZyI6IkVTMjU2IiwiandrIjp7Imt0eSI6IkVDI...

grant_type=urn:ietf:params:oauth:grant-type:token-exchange
&requested_token_type=urn:ietf:params:oauth:token-type:id-jag
&audience=https://acme.chat.example/
&resource=https://api.chat.example/
&scope=chat.read+chat.history
&subject_token=eyJraWQiOiJzMTZ0cVNtODhwREo4VGZCXzdrSEtQ...
&subject_token_type=urn:ietf:params:oauth:token-type:id_token
```

Changes in version -02

- Added example of including a RAR object in the Token Exchange and ID-JAG

```
POST /oauth2/token HTTP/1.1
Host: acme.idp.example
Content-Type: application/x-www-form-urlencoded

grant_type=urn:ietf:params:oauth:grant-type:token-exchange
&requested_token_type=urn:ietf:params:oauth:token-type:id-jag
&audience=https://acme.chat.example/
&authorization_details=[{"type":"chat_read","actions":["read"],"locations":["https://api.
&subject_token=eyJraWQiOiJzMTEoOVNtOBhMRE4.MSI6NzI.eZtQ...
&subject_token_type=urn:ietf:params:oauth:token-type:id_token
&client_assertion_type=urn:ietf:params:oauth:client-assertion-type:jwt-bearer
&client_assertion=eyJhbGciOiJSUzI1NiIsImtpZCI6IjIyIn0...
```

```
{
  "typ": "oauth-id-jag+jwt"
}
.
{
  "jti": "9e43f81b64a33f20116179",
  "iss": "https://acme.idp.example/",
  "sub": "U019488227",
  "aud": "https://acme.chat.example/",
  "client_id": "f53f191f9311af35",
  "exp": 1311281970,
  "iat": 1311280970,
  "authorization_details": [
    {
      "type": "chat_read",
      "actions": ["read"],
      "locations": ["https://api.chat.example/channels"]
    },
    {
      "type": "chat_history",
      "actions": ["read"],
      "datatypes": ["message"]
    }
  ],
  "auth_time": 1311280970
}
.
signature
```

Changes in version -02

- Added refresh token as optional subject token input, enables uses when SSO relationship is SAML rather than OpenID Connect

4.3.1.1. Example: Token Exchange using Refresh Token

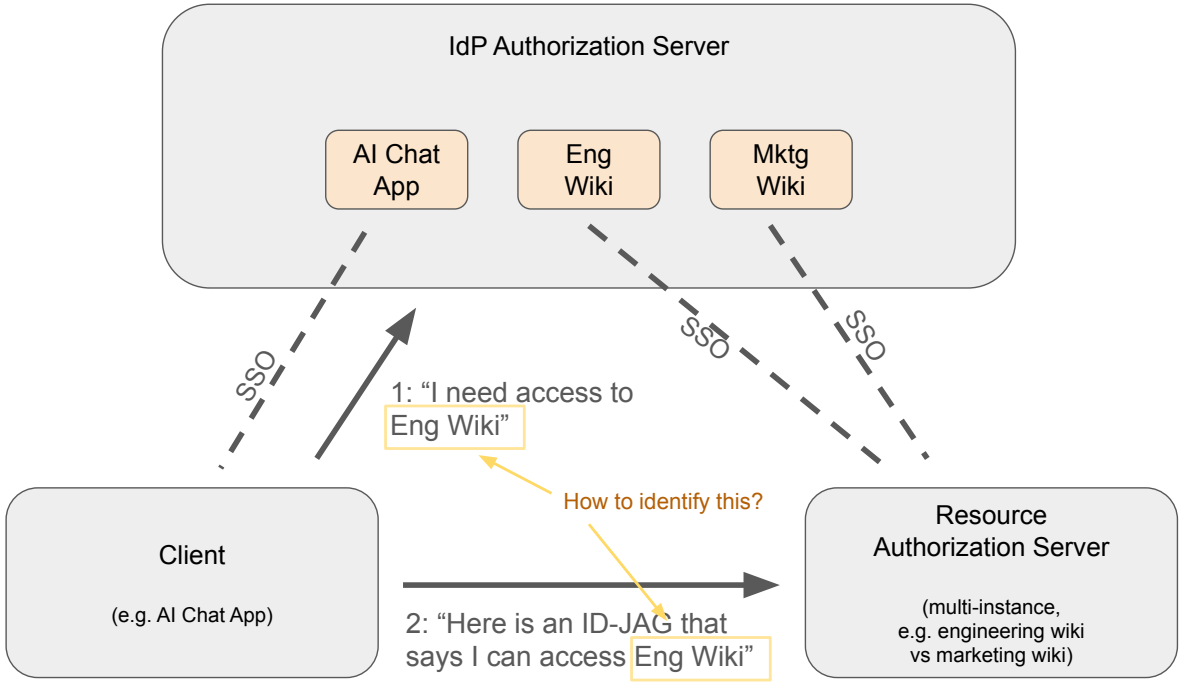
This non-normative example shows using a Refresh Token as the `subject_token` (when supported by the IdP Authorization Server) to obtain an ID-JAG without acquiring a new Identity Assertion:

```
POST /oauth2/token HTTP/1.1
Host: acme.idp.example
Content-Type: application/x-www-form-urlencoded

grant_type=urn:ietf:params:oauth:grant-type:token-exchange
&requested_token_type=urn:ietf:params:oauth:token-type:id-jag
&audience=https://acme.chat.example/
&resource=https://api.chat.example/
&scope=chat.read+chat.history
&subject_token=tGzv3JOkF0XG5Qx2TlKWIA
&subject_token_type=urn:ietf:params:oauth:token-type:refresh_token
&client_assertion_type=urn:ietf:params:oauth:client-assertion-type:jwt-bearer
&client_assertion=eyJhbGciOiJSUzI1NiIsImtpZCI6IjIyIn0...
```

Changes in version -02

- Added `aud_tenant` and `aud_sub` to clear up ambiguity for multi-tenant systems



Changes in version -02

Based on most common implementer feedback

- DPoP
- RAR
- Refresh token as subject token input
- Support for multi-tenant systems

Remaining issues are questions or editorial, not expecting major changes