OAuth Profile for Open Public Clients

Neil Jenkins

https://www.ietf.org/archive/id/
draft-jenkins-oauth-public-00.html

The problem

The solution

Profile overview

1. The OAuth 2.0 Authorization Server Metadata (RFC8414) is fetched.

2. The client registers with the authorization server to get a client id using the OAuth 2.0 Dynamic Client Registration Protocol (RFC7591).

3. The client authorizes using the Authorization Code Grant flow (RFC6749, Section 4.1) with PKCE (RFC7636), Issuer Identification (RFC9207) and Resource Indicators (RFC8707)

4. The client gets an access token and refresh token (RFC6749, Section 5).

Presumptions

This OAuth flow presumes you have an email address that is used to identify the user, along with:

- The set of services that may be available for this email address (e.g., JMAP/IMAP/SMTP/POP/CardDAV/CalDAV);
- The Application Server endpoint to connect to in order to access them; (e.g. a JMAP session endpoint https://api.example.com/jmap/session, or an IMAP endpoint imaps://imap.example.com:993).
- The authorization server issuer identifier, needed to do OAuth, e.g. https://auth.example.com.

Open questions

- Autodiscovery
- Scopes

Call for adoption