OAuth Profile for Open Public Clients

Neil Jenkins

https://www.ietf.org/archive/id/
draft-jenkins-oauth-public-01.html

Passwords are a *problem*

- No 2FA, passkeys, SSO, etc.
- Can't (easily) detect if a new device has connected.
- Can't revoke access to just one device.
- No granular access.

OAuth is a solution

Profile overview

Step 0: Autoconfig

← Gets OAuth issuer

RFC8414

Step 1: Fetch the OAuth metadata

← Gets other OAuth endpoints

← Gets supported scopes

RFC7591

Step 2: Dynamic client registration

→ Client sends JSON file with name, version, redirect_uri endpoints etc.

← Gets a client id

RFC6749

Step 3: Authorization Code Grant flow

→ Client opens browser at auth endpoint

← Gets an auth code on success

RFC6749

Step 4: Swap for access/refresh tokens

→ Client sends auth code + PKCE verifier

← Gets access/refresh tokens

RFC7628

Step 5: Use access token to authenticate

→Authorization: Bearer {token} for HTTP

→ SASL OAUTHBEARER for IMAP etc.

Call for adoption