Use the OAuth 2.0 authorization code flow with the PKCE extension

Require the OAuth 2.0 state parameter

Recommend exact matching of redirect URIs, and require the hostname of the redirect match the hostname of the URL the app was served from

Do not return access tokens in the front channel
First-Party Applications

- It is strongly RECOMMENDED that applications use the Authorization Code flow instead of the Password grant.
- Can prompt the user for multi-factor authentication.
- Can take advantage of single-sign-on sessions.
- Can use a third-party IdP.
Apps Served from the Same Domain as the API

- OAuth and OIDC provide little benefit
- Use session authentication instead
Authorization Code Flow

• MUST use PKCE

• MUST use the "state" parameter

• SHOULD require exact match of redirect_uri, but MAY require only the hostname match

• SHOULD use a unique redirect_uri per authorization server

• MUST be considered public clients, and SHOULD NOT be issued a secret
Implicit Flow

- MUST NOT be used by browser-based apps
- Cannot be protected with PKCE
- Already cannot be used for mobile apps following RFC 8252