PKCE - Funksjonalitet

Skrevet ned etter workshop vedrørende innloggingen til FixrateApp.

Klient (app)

1. Logger inn med fingeravtrykk
2. Genererer en “code-verifier” (RANDOM STRING)
3. Lager en “code-challenge” (Hasher code-verifier)
4. Hvis biometrisk innlogging = true → Lag key-value pairs.
5. Lag et objekt som inneholder code-challenge og spesifiser hvilken hash-algoritme som ble brukt for å lage den.
6. Motta “authorization code” fra server.
7. Spørr server om en access token ved å sende tilbake authorization code og code-verifier.
8. Mottar enten access-token fra server eller feilmelding.
9. Lagre access-token i SecureStore

Server (autentisering)

1. Mottar data fra klienten
2. Generer “authorization code”. Og knytt denne til code-challengen som ble mottatt.
3. Lagre “authorization code” og “code challenge” i databasen.
4. Returner “authorization code” til klient (app).
5. Valider code-verifier fra forespørselen. Siden vi lagret auth-code og code-challenge i steg 3 kan server hashe mottatt code-verifier for å se at det er riktig bruker. Server finner data i databasen ved å bruke authorization code. Da får vi tidligere code-challenge og hash-funksjon. Server hasher mottatt code-verifier og sammenligner den med den lagrede code-challenge.
6. Hvis server godkjenner steg 5 så sendes det en access-token tilbake. Hvis det ikke stemmer, send error tilbake.