MFA App - Studio di Fattibilità

Scopo del progetto

Il progetto ha come scopo lo sviluppo di un'applicazione mobile cross-platform che implementi la multi-factor authentication sfruttando i parametri biometrici dell'utente per l'autorizzazione delle diverse attività supportate.

Obiettivi del prodotto

L'applicazione mobile dev'essere fruibile sia su un dispositivo Android che su un dispositivo iOS; deve supportare i protocolli di autorizzazione e autenticazione OAuth2.0 e OpenID, nei quali, facendo riferimento allo standard RFC 6479 (link), ricoprirà il ruolo di client.
Inoltre l'applicazione dovrà essere integrabile con qualsiasi provider OAuth e permettere l'autorizzazione delle attività del fruitore del servizio .

Tecnologie utilizzate

Le principali tecnologie previste per lo sviluppo del prodotto sono:

- OAuth 2.0: protocollo di autorizzazione utilizzato per delegare l'autorizzazione a sistemi terzi;
- OpenID Connect: layer di autenticazione basato su OAuth 2.0 che permette la delegazione dell'accesso a sistemi terzi;
- TypeScript: linguaggio di programmazione open source utilizzato per lo sviluppo della logica dell'applicazione;
- Ionic: framework open source sviluppato in TypeScript per lo sviluppo di applicazioni mobile ibride;
- Vue.js: framework frontend open source per lo sviluppo di interfacce utente e single-page applications basate sull'architettura MVVM.

Librerie utilizzabili

Di seguito vengono elencate una serie di librerie ritenute opportune per lo sviluppo dell'applicazione in fase di studio; per le soluzioni a pagamento, ove possibile, è anche indicata un'opzione open source con la rispettiva licenza.

Auth Connect: info
Package proprietario di Ionic che permette l'integrazione con provider OAuth e implementa i framework di autenticazione e autorizzazione OAuth e OpenID Connect.

Identity Vault: info
Package proprietario di Ionic che permette il riconoscimento dell'utente tramite gli strumenti hardware per il riconoscimento biometrico (impronta digitale e/o riconoscimento facciale/dell'iride) oltre che il salvataggio criptato di token di accesso.

AppAuth: github alternativa open source a 'Auth Connect' con licenza Apache 2.0
Package open source che implementa i framework di autenticazione OAuth 2.0 e OpenId Connect sviluppato in JavaScript.

Fingerprint-AIO: github alternativa open source a 'Identity Vault' con licenza MIT
Package open source che permette il riconoscimento biometrico su dispositivi Android e iOS.

Vuex: info licenza MIT
Package open source che implementa il pattern di gestione dello stato in applicazioni Vue.js.

Capacitor-secure-storage-plugin: github alternativa open source a ‘Identity Vault’ con licenza MIT
Package per il salvataggio criptato di dati sensibili sfruttando i sistemi platform specific dei dispositivi mobili.

Vuex-persists: github alternativa open source a ‘Identity Vault’ con licenza MIT
Package open source per il salvataggio di informazioni nella memoria locale del dispositivo, da affiancare ad una libreria di criptazione (e.g. crypt-js) per il salvataggio sicuro di dati sensibili.

uuid: github licenza MIT
Package open source per la generazione di codici univoci ed identificativi per dispositivi secondo lo standard RFC 4122 (link).