JS-Capacitor Passkey Kit Architecture Doc

written for the Abstract Submission of SCF 37

Table of Contents

1. Introduction 2

2. Overview 2

2.1. JS-Smart Wallet API 4

2.2. Capacitor native passkey plugin 4

2.3. Demo App 4

3. Summary 5

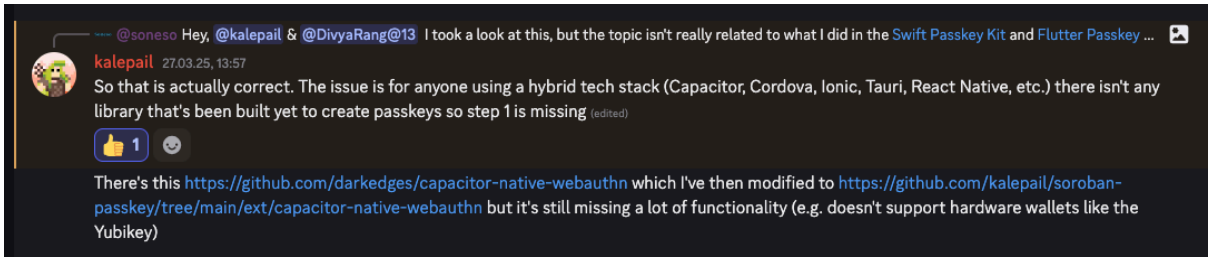
1. Introduction

This document is about the development of the open-source JS-Capacitor Passkey Kit for Soroban. The new kit will help developers to use native passkey functionality on different types of devices such as Apple, Android, web and hardware like Yubikey for developing Soroban smart wallets.

Currently there is no working passkey solution for the Java Script hybrid tech stack like Capacitor, Cordova, Ionic allowing JS developers to access passkey functionality on mobile devices or other hardware to be able to build Soroban smart wallets for those platforms.

The ts-passkey-kit for Soroban smart wallets can only be used in browsers but cannot be used for example for registration and authentication (extract public key, sign, etc.) on mobile devices. This problem has often been discussed in the Stellar Dev Discord passkey channel. See for example this conversation:

https://discord.com/channels/897514728459468821/1250851135561142423/1354801613218250784

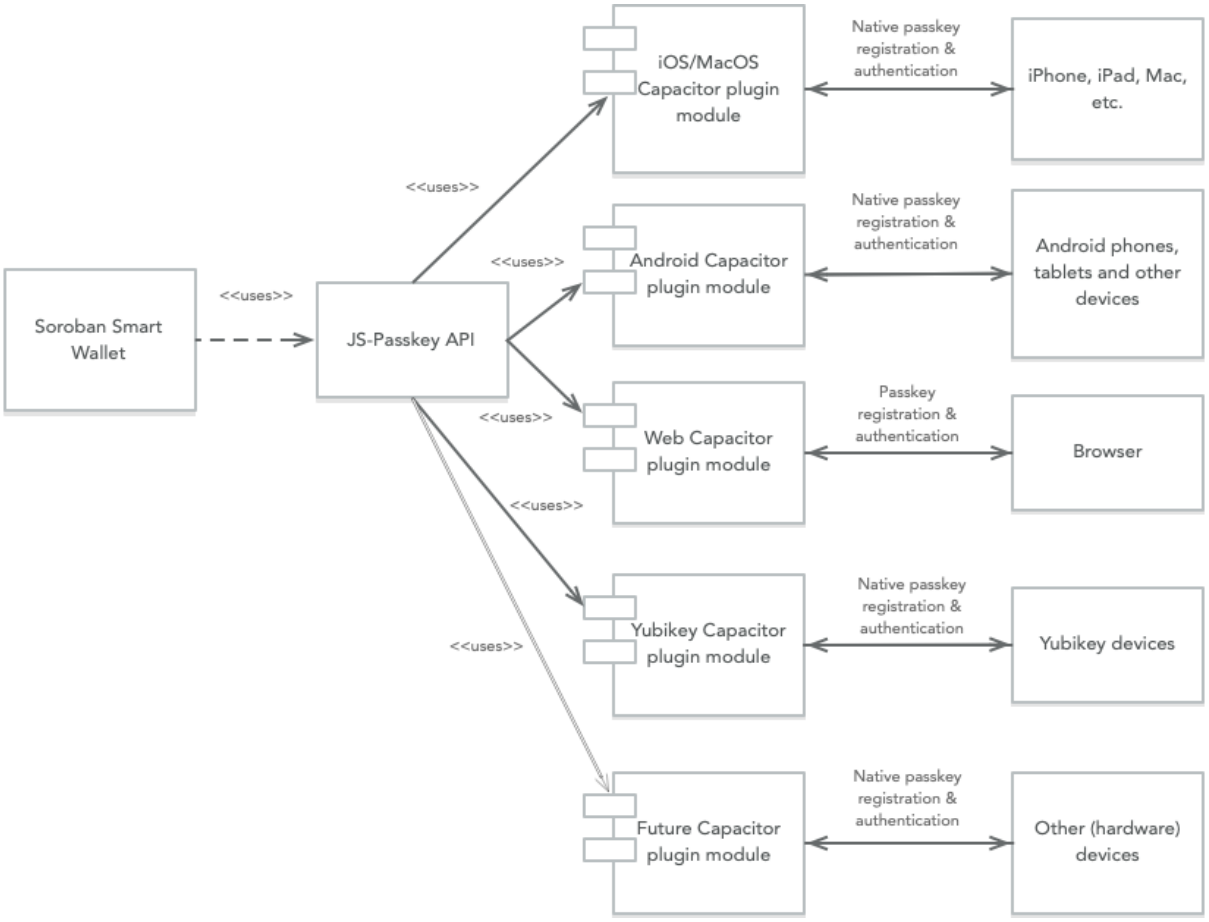


Our solution is to implement an open-source JS-Capacitor Passkey Kit for Soroban smart wallets, that can be used alone or in conjunction with the ts-passkey-kit to build Soroban smart wallets not only for browsers but also for mobile devices or by using hardware like Yubikey.

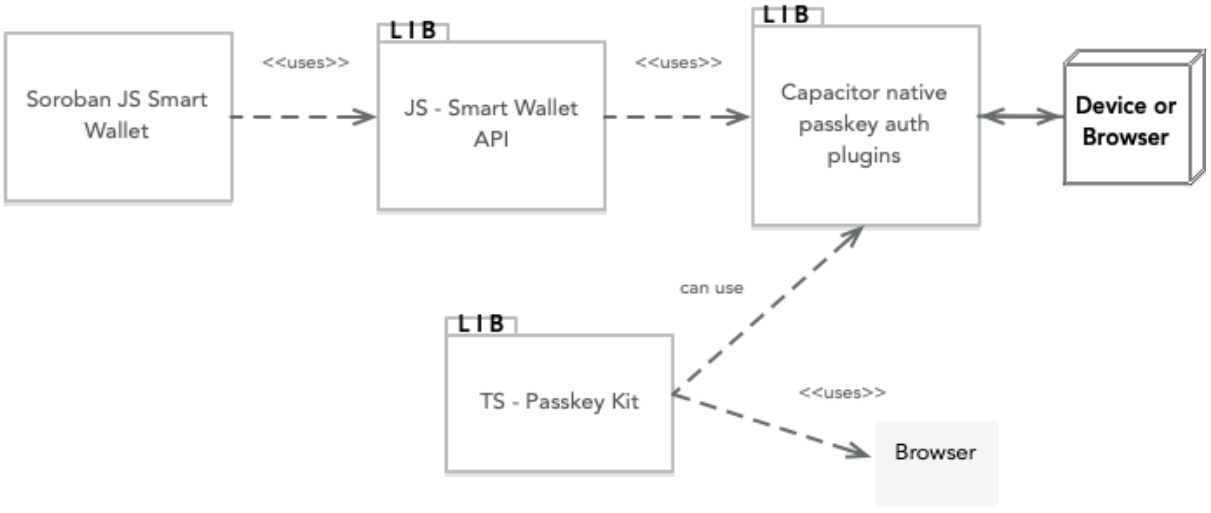
This document is intended for the abstract submission for SCF 37 and contains an overview of the necessary steps and components required for the solution described above. A more detailed breakdown will be provided in the subsequent step for the SCF 37 build submission.

2. Overview

The JS-Capacitor Passkey kit will provide a JS API for the creation and management of smart wallets. Depending on the underlying system, the corresponding capacitor plugin will be used to provide native passkey functionality such as passkey registration and authentication.



The functionality will be split into two separate libraries, so that the capacitor plugins can also be used by other packages such as the ts-passkey-kit.



2.1. JS-Smart Wallet API

Like the TS-Passkey Kit, this library will provide the necessary Soroban smart wallet functionality via its interfaces. This includes creation of wallets, connection to smart wallets, creation of keys that can be used as Secp256r1 signer for smart wallets, adding, updating, removing of Secp256r1, Ed25519 and policy signers, signing auth entries with passkeys, keypairs and policies, etc.

With the help of the capacitor native plugin lib, this libraries logic will abstract the creation of new native passkey and the signing of transactions by using them.

2.2. Capacitor native passkey plugin

This library will provide a set of specific modules that will access the native passkey functionality of the device used. Each module must be implemented individually and separately for the corresponding platform, using its programming language and frameworks. E.g. iOS in Swift, Android in Kotlin, etc.

In the first step, the library will provide modules for iOS/MacOS, Android, Browsers and Yubikey. Other modules can easily be added later.

2.3. Demo App

An important part of our submission will be the creation of demo app that will demonstrate the functionality on the different platforms and provide implementation examples for smart wallet developers.

Such a demo app is provided by the current TS-Passkey Kit for browsers here: https://passkey-kit-demo.pages.dev/

With the demo app, the user will be able register, sign in, reset, add funds, get balance, add Ed25519 signers, execute Ed25519 transfers, add Secp256r1 signers, execute Secp256r1 signer transfers, add policy signers, execute policy transfers, and multisig transfers. The app will work on iOS, MacOS, Android, Browser and with Yubikey devices and will be tested on testnet and on mainnet.

3. Summary

Currently there is no working passkey solution allowing JS developers to access passkey functionality on mobile devices and other hardware such as Yubikey to be able to build Soroban smart wallets for those platforms.

The open-source JS-Capacitor Passkey Kit will solve this problem and give JS developers the possibility to access the native passkey functionality of different platforms such as Apple, Android, Browser, Yubikey. In addition, the solution will provide a demo app that will help developers easily understand how the functionality can be used on the different platforms to be able to build smart wallets that not only work in browsers but also for example on mobile devices or with hardware like Yubikey.