Web3Auth tKey JS SDK

'tKey' is an abbreviation for Threshold Key, which is responsible for the management of wallet shares produced using threshold cryptography. The tKey SDK manages wallets by generating shares via Shamir's Secret Sharing scheme.

In a typical 2 out of 3 (2/3) setup, the user is provided with three shares: ShareA, ShareB, and ShareC.

- ShareA
- is managed and divided across Web3Auth's Auth Network and can be accessed through an OAuth login provider owned by the user, like their
- Google account.
- ShareB
- is stored on the user's device. The method of storage is specific to the device and system. For instance, on mobile devices, the share
- could be stored in device storage that's secured with biometrics.
- ShareC
- serves as a recovery share. It's an extra share that the user can keep on a separate device, download, or base on user input with
- sufficient entropy. This could include a password, security questions, or a hardware device, among other options.

Like existing 2FA systems, users must prove ownership of at least 2 out of 3 (2/3) shares to retrieve their private key.

caution Although you can create as many shares as you want, we recommend you create no more than a total of 6 shares, including your device shares and recovery shares. This is because the more shares you create, it increases the size of the tKey state, which can cause performance issues in the frontend and can slow down the login process. Ideally, you should create 2 recovery shares and ask the user for their trusted devices and only store the device share on them.

Requirementsâ

Webâ

- This is a frontend SDK and can only run in a browser environment
- Basic knowledge of JavaScipt
- Supports all major JavaScript Frameworks, Libraries and Bundlers

React Nativeâ

- React Native Release 0.71 and above (for Bare React Native Workflow)
- Expo SDK 48 and above (for Expo Managed Workflow)
- iOS Platform Target Version 14 and above
- Android Target SDK Version 31 and above

note The minimumpricing plan to use this SDK in a production environment is theGrowth Plan , since custom verifier setup is a needed feature for Core Kit SDKs. You can use this SDK with all features enabled in the development environment for free. warning Web3Auth SDKs are not compatible with "Expo Go" app. They are compatible only with Custom Dev Client and EAS builds. Please refer to the troubleshooting section for more on this.

Please runnpx expo prebuild to generate native code based on the version of expo a project has installed, before moving forward.

Understanding the tKey Flowâ

The tKey SDK depends upon the Service Provider, Storage Layer and Modules to work as an off chain multi sig infrastructure working within your app.

Service Providerâ

TheService Provider helps with the authentication and identification of the user using their social logins and giving the an easy way of account retreival.

Storage Layerâ

TheStorage Layer refers to the Metadata Storage, which is used to store the metadata information of the shares generated by the tKey SDK.

Modulesâ

Modules are the various functionalities that can be added to the tKey SDK, tkey enhance the storage and usage of different shares generated in a way it is most suitable for your project.

We have 3 types of modules available right now:

- Storage Modules
- : Storage Modules are used to store the tKey shares in the user's device
- storage.
- Recovery Modules
- : Recovery Modules are used to recover the tKey shares in the case user
- doesn't have access to their device/storage or needs additional security.
- Additional Modules
- : These modules provide extra capability to the tKey SDK, like importing
- user's existing private keys or seedphrases.

Thresholdâ

The threshold is the minimum number of shares required to reconstruct the private key. By default, the number is set to2 which means that at least two shares are required to reconstruct the private key. This is done to ensure that the private key is not compromised even if one of the shares is compromised.

tKey Modesâ

Apart from this, the tKey SDK internally has multiple modes of operation, which are as follows:

Read modeâ

This happens when atleast 1 share is available to the tKey SDK. In this mode, the tKey SDK can only read the metadata information of the share currently available to it, alongside the public data of the other shares.

Write modeâ

This happens when 2 or more shares are available to the tKey SDK. Please note that the threshold set by the dApp might change this number required. Basically once the key threshold is reached, the tKey SDK can write the metadata information of the shares and modify them according to the need of the user.

Resourcesâ

- Example Applications
- : Explore our example applications and try the SDK yourself.
- Troubleshooting
- : Find quick solutions to common issues faced by developers.
- Source Code
- : Web3Auth is open sourced. You can find the source code on our GitHub repository.
- Community Support Portal
- : Join our community to get support from our team and other developers.

Helper SDKsâ

Provider packagesâ

For making RPC calls within your dApp, Web3Auth exposes respective providers for different chains. This provider can be used to interact with the connected chain using exposed functions within the provider. Currently Web3Auth supports providers for both EVM and Solana chains. For other chains, one can easily get the private key from the Web3Auth SDK.

tip Checkout theProviders SDK Reference to learn more.

- For EVM based Chains@web3auth/ethereum-provider
- For Solana Blockchain@web3auth/solana-provider

Plugin packagesâ

Plugins extend the functionality of Web3Auth, helping you to add more features to your application. These features can be used to extend the UI functionalities, making your Web3Auth instance more interoperable, adding wallet features and a lot more!

Currently, we support UI plugins for wallet operations, helping you with flows to add funds, manage transactions, provide

wallet UI and much more. This helps you avoid making wallet flows within your application. Additionally, for interoperability with multiple applications, these packages give you the advantage of using the same key from Web3Auth across multiple applications.

tip Checkout thePlugins SDK Reference to learn more.

- EVM Wallet UI Plugin@web3auth/torus-wallet-connector-plugin
- Solana Wallet UI Plugin@web3auth/solana-wallet-connector-plugin Edit this page Previous Usage Next Install