Passkey

Passkey provides a secure and user-friendly alternative for submitting transactions to Sui. Built on the WebAuthn standard , passkey lets users authenticate and sign transactions using:

Passkey simplifies authentication by removing the need to manage seed phrases or private keys manually. Instead, they rely on device-based authentication and cloud synchronization, allowing seamless, phishing-resistant access across multiple devices.

By supporting the passkey signature scheme, Sui improves security and accessibility, making it easier for users to manage their accounts with hardened security. Passkey-based wallets are also tied to the origin, meaning they can't be phished or used on a different site, which makes it a more secure authentication option.

Refer to the Typescript SDK support on how to add passkey support to your application. For product specification, refer to SIP-9 .

Passkey support is available in beta in Sui Devnet and Testnet. The Mainnet release is yet to be scheduled.

Sign transactions seamlessly

Users can sign transactions in Sui using passkey, where the passkey private key stays securely stored within the authenticator, reducing the risk of key extraction attacks.

Authenticate across devices

Users can approve transactions on their mobile phones by scanning a QR code from a desktop browser. Cloud-synchronized passkey (such as those stored in Apple iCloud or Google Password Manager) lets users authenticate across multiple devices without manual key transfers.

Use hardware security keys

Users can sign transactions with external security keys, such as YubiKeys, to add an extra layer of protection against phishing and unauthorized access.

Authenticate with platform-based security

Users can sign transactions directly on devices with built-in authenticators (such as Face ID on iPhones or Windows Hello on Windows PCs). This approach lets users sign transactions natively without needing an external security key.

Recover access and secure accounts with cloud-synced passkey

Cloud-synced passkey helps users recover access if they lose a device.

Passkey functionality varies by authenticator

Some security keys do not support biometric authentication, requiring users to enter a PIN instead. Also, because WebAuthn does not provide access to private keys, users must store their passkey securely or enable cloud synchronization for recovery.

Cloud synchronization introduces potential risks

Cloud-synced passkey improves accessibility but also create risks if a cloud provider is compromised or if a user loses access to their cloud account. Users who prefer full self-custody can rely on hardware-based passkey that does not use cloud synchronization.

Passkey cannot be exported

Users cannot transfer a passkey between different authenticators. For example, a passkey created on a security key cannot move to another device unless it syncs through a cloud provider. To avoid losing access, users should set up authentication on multiple devices.

Benefits of using passkey

Sign transactions seamlessly

Users can sign transactions in Sui using passkey, where the passkey private key stays securely stored within the authenticator, reducing the risk of key extraction attacks.

Authenticate across devices

Users can approve transactions on their mobile phones by scanning a QR code from a desktop browser. Cloud-synchronized passkey (such as those stored in Apple iCloud or Google Password Manager) lets users authenticate across multiple devices without manual key transfers.

Use hardware security keys

Users can sign transactions with external security keys, such as YubiKeys, to add an extra layer of protection against phishing and unauthorized access.

Authenticate with platform-based security

Users can sign transactions directly on devices with built-in authenticators (such as Face ID on iPhones or Windows Hello on Windows PCs). This approach lets users sign transactions natively without needing an external security key.

Recover access and secure accounts with cloud-synced passkey

Cloud-synced passkey helps users recover access if they lose a device.

Passkey functionality varies by authenticator

Some security keys do not support biometric authentication, requiring users to enter a PIN instead. Also, because WebAuthn does not provide access to private keys, users must store their passkey securely or enable cloud synchronization for recovery.

Cloud synchronization introduces potential risks

Cloud-synced passkey improves accessibility but also create risks if a cloud provider is compromised or if a user loses access to their cloud account. Users who prefer full self-custody can rely on hardware-based passkey that does not use cloud synchronization.

Passkey cannot be exported

Users cannot transfer a passkey between different authenticators. For example, a passkey created on a security key cannot move to another device unless it syncs through a cloud provider. To avoid losing access, users should set up authentication on multiple devices.

Limitations of passkey

Passkey functionality varies by authenticator

Some security keys do not support biometric authentication, requiring users to enter a PIN instead. Also, because WebAuthn does not provide access to private keys, users must store their passkey securely or enable cloud synchronization for recovery.

Cloud synchronization introduces potential risks

Cloud-synced passkey improves accessibility but also create risks if a cloud provider is compromised or if a user loses access to their cloud account. Users who prefer full self-custody can rely on hardware-based passkey that does not use cloud synchronization.

Passkey cannot be exported

Users cannot transfer a passkey between different authenticators. For example, a passkey created on a security key cannot move to another device unless it syncs through a cloud provider. To avoid losing access, users should set up authentication on multiple devices.