

Transaction Authentication

Transaction authentication features on Sui provide security against unauthorized access to on-chain data.

Sui adheres to widely accepted wallet specifications in the cryptocurrency industry, including BIP-32 (and its variation, SLIP-0010), BIP-44, and BIP-39, to facilitate key management for users. At present, Sui supports pure Ed25519, ECDSA Secp256k1, ECDSA Secp256r1, and multisig for signed transactions.

Go to [Keys and Addresses](#) .

Cryptographic agility is core to Sui. The system supports multiple cryptography algorithms and primitives and can switch between them rapidly. With Sui, you can choose the right cryptography solution for your system and implement the latest algorithms as they become available.

Go to [Signatures](#) .

Sui supports multi-signature (multisig) transactions, which require multiple keys for authorization rather than a single, one-key signature.

Go to [Multisig](#) .

Sui supports offline signing, which is signing transactions using a device not connected to a Sui network, or in a wallet implemented in a different programming language without relying on the Sui key store.

Go to [Offline Signing](#) .

In Sui, an intent is a compact struct that serves as the domain separator for a message that a signature commits to. The data that the signature commits to is an intent message. All signatures in Sui must commit to an intent message, instead of the message itself.

Go to [Intent Signing](#) .

Keys and Addresses

Sui adheres to widely accepted wallet specifications in the cryptocurrency industry, including BIP-32 (and its variation, SLIP-0010), BIP-44, and BIP-39, to facilitate key management for users. At present, Sui supports pure Ed25519, ECDSA Secp256k1, ECDSA Secp256r1, and multisig for signed transactions.

Go to [Keys and Addresses](#) .

Cryptographic agility is core to Sui. The system supports multiple cryptography algorithms and primitives and can switch between them rapidly. With Sui, you can choose the right cryptography solution for your system and implement the latest algorithms as they become available.

Go to [Signatures](#) .

Sui supports multi-signature (multisig) transactions, which require multiple keys for authorization rather than a single, one-key signature.

Go to [Multisig](#) .

Sui supports offline signing, which is signing transactions using a device not connected to a Sui network, or in a wallet implemented in a different programming language without relying on the Sui key store.

Go to [Offline Signing](#) .

In Sui, an intent is a compact struct that serves as the domain separator for a message that a signature commits to. The data that the signature commits to is an intent message. All signatures in Sui must commit to an intent message, instead of the message itself.

Go to [Intent Signing](#) .

Signatures

Cryptographic agility is core to Sui. The system supports multiple cryptography algorithms and primitives and can switch between

them rapidly. With Sui, you can choose the right cryptography solution for your system and implement the latest algorithms as they become available.

Go to [Signatures](#) .

Sui supports multi-signature (multisig) transactions, which require multiple keys for authorization rather than a single, one-key signature.

Go to [Multisig](#) .

Sui supports offline signing, which is signing transactions using a device not connected to a Sui network, or in a wallet implemented in a different programming language without relying on the Sui key store.

Go to [Offline Signing](#) .

In Sui, an intent is a compact struct that serves as the domain separator for a message that a signature commits to. The data that the signature commits to is an intent message. All signatures in Sui must commit to an intent message, instead of the message itself.

Go to [Intent Signing](#) .

Multisig

Sui supports multi-signature (multisig) transactions, which require multiple keys for authorization rather than a single, one-key signature.

Go to [Multisig](#) .

Sui supports offline signing, which is signing transactions using a device not connected to a Sui network, or in a wallet implemented in a different programming language without relying on the Sui key store.

Go to [Offline Signing](#) .

In Sui, an intent is a compact struct that serves as the domain separator for a message that a signature commits to. The data that the signature commits to is an intent message. All signatures in Sui must commit to an intent message, instead of the message itself.

Go to [Intent Signing](#) .

Offline Signing

Sui supports offline signing, which is signing transactions using a device not connected to a Sui network, or in a wallet implemented in a different programming language without relying on the Sui key store.

Go to [Offline Signing](#) .

In Sui, an intent is a compact struct that serves as the domain separator for a message that a signature commits to. The data that the signature commits to is an intent message. All signatures in Sui must commit to an intent message, instead of the message itself.

Go to [Intent Signing](#) .

Intent Signing

In Sui, an intent is a compact struct that serves as the domain separator for a message that a signature commits to. The data that the signature commits to is an intent message. All signatures in Sui must commit to an intent message, instead of the message itself.

Go to [Intent Signing](#) .