Off-Chain Message Signing with the Solana CLI

Off-chain message signing is a method of signing non-transaction messages with a Solana wallet. This feature can be used to authenticate users or provide proof of wallet ownership.

Sign Off-Chain Message

To sign an arbitrary off-chain message, run the following command:

solana sign-offchain-message < MESSAGE

> The message will be encoded and signed with CLI's default private key and signature printed to the output. If you want to sign it with another key, just use the-k/--keypair option:

solana sign-offchain-message -k < KEYPAIR

< MESSAGE

> By default, the messages constructed are version 0, the only version currently supported. When other versions become available, you can override the default value with the--version option:

solana sign-offchain-message -k < KEYPAIR

> --version < VERSION

< MESSAGE

> The message format is determined automatically based on the version and text of the message.

Version0 headers specify three message formats allowing for trade-offs between compatibility and composition of messages:

ID Encoding Maximum Length Hardware Wallet Support 0 Restricted ASCII *1212 Yes 1 UTF-8 1212 Blind sign only 2 UTF-8 65515 No* Those characters for whichisprint(3) returns true. That is,0x20..=0x7e .

Formats0 and1 are motivated by hardware wallet support where both RAM to store the payload and font character support are limited.

To sign an off-chain message with Ledger, ensure your Ledger is running latest firmware and Solana Ledger App version 1.3.0 or later. After Ledger is unlocked and Solana Ledger App is open, run:

solana sign-offchain-message -k usb://ledger < MESSAGE

> For more information on how to setup and work with the ledger device see thisink .

Please note that UTF-8 encoded messages requireAllow blind sign option enabled in Solana Ledger App. Also, due to the lack of UTF-8 support in Ledger devices, only the hash of the message will be displayed in such cases.

IfDisplay mode is set toExpert , Ledger will display technical information about the message to be signed.

Verify Off-Chain Message Signature

To verify the off-chain message signature, run the following command:

solana verify-offchain-signature < MESSAGE

< SIGNATURE

> The public key of the default CLI signer will be used. You can specify another key with the--signer option:

solana verify-offchain-signature --signer < PUBKEY

< MESSAGE

< SIGNATURE

> If the signed message has a version different from the default, you need to specify the matching version explicitly:

solana verify-offchain-signature --version < VERSION

< MESSAGE

< SIGNATURE

Protocol Specification

To ensure that off-chain messages are not valid transactions, they are encoded with a fixed prefix:\xffsolana offchain , where first byte is chosen such that it is implicitly illegal as the first byte in a transactionMessageHeader today. More details about the payload format and other considerations are available in theproposal . Previous Solana CLI: Offline Transaction Signing Next Solana CLI: Test Validator