mSIGNA™– Getting Started

Thank you for deciding to try mSIGNA™, the most powerful secure cryptocoin storage solution available. We think you will enjoy using mSIGNA™ as it is, but it is still a product under development – the best is yet to come! You have the opportunity to provide us with valuable feedback, suggestions, and bug reports. We are offering rewards for reporting issues and bugs to bugreport@ciphrex.com.

WARNING: This is beta software. It might have bugs. Use at your own risk.

IMPORTANT: Newer versions of mSIGNA™/CoinVault™ might not be able to read vault files created with older versions. Please make note of the schema version (in the About… box). It is recommended that you export your keychains and accounts to file before upgrading. You can import these files into newer versions. If you need to access older vault files, older versions of mSIGNA™/CoinVault™ are available at https://ciphrex.com/releases/

VERY IMPORTANT: ALWAYS MAKE BACKUPS OF KEYS AND ACCOUNTS BEFORE USING THEM – IF YOU LOSE YOUR KEYS THERE IS NO WAY TO RECOVER ANY BITCOINS THEY HOLD. It is also recommended that you test deposit addresses with relatively small deposits first.

Introduction

mSIGNA™ is a powerful account management and secure storage tool for blockchain-based cryptocurrencies, such as Bitcoin and Litecoin. It features decentralized offline key generation, offline signing, watch-only shared wallets, fast multidevice synchronization, full support for BIP32 (hierarchical deterministic wallets), and general m-of-n multisignature transactions.

It has many applications, from secure cold storage for individuals to enterprise-wide accounts that can be deployed and monitored across entire organizations.

Core Concepts

Vaults

Vaults are files with extension .vault containing accounts, keychains, and transaction history. They can be opened directly in mSIGNA™ and constitute the basic document type that mSIGNA™ can create and edit.

Keychains

Keychains are collections of private and/or public keys generated deterministically from a master seed using BIP32. They can be imported and exported to and from mSIGNA™ as files with extensions .priv and .pub respectively. Every keychain can be given an arbitrary name and has a hash that is uniquely determined by the master seed and remains fixed.

Accounts

Accounts are logically grouped collections of deposit addresses generated deterministically from a set of keychains and an m-of-n policy. The account balance consists of all the transaction outputs spendable using the aforementioned keychains subject to the m-of-n policy. Each distinct account contains a separate set of addresses that always remain part of that account.

Addresses are generated by using keychain sequences/trees in parallel. Public keys are sorted lexicographically in the redeemscript. Accounts also have a starting timestamp that indicates how far back in the blockchain we should look when scanning for transactions.

Shared accounts, a.k.a. watch-only accounts, are accounts that have been stripped of all private keys. They can only be used to monitor transactions, not to spend.

First Steps…

1. Create a new vault file.

   From the File menu, select “New Vault…” – or alternately, click on the toolbar button. You will be prompted to pick a name for your vault file. Create a new folder for your vault files, make sure to use the file extension “.vault” and then save.

2. Create an account by either *using the wizard* or *manually*.

   USING THE WIZARD (easy)

   From the Accounts menu, select “Account Wizard…” – or alternately, click on the button in the toolbar. You will be asked for an account name and an account policy. If you just want a simple account, leave the policy as 1 of 1.

   NOTE: mSIGNA™ always uses pay-to-script-hash addresses, which begin with the character 3 in Bitcoin, even for 1 of 1 accounts.

   For multisignature accounts: on the left select the minimum number of signatures required to sign transactions from the account. On the right select the total number of keychains to use for the account. An account will automatically be created for you along with a new set of keychains.

   MANUALLY (advanced)

   From the Keychains menu, select “New Keychain…” – or alternately, click on the toobar button. You will be prompted to name the keychain. Pick whatever name you want.

   Repeat step 2 to create multiple keychains if desired.

   Right-click on any keychain in the Keychains tab and select “Export Private Keychain…” to make backups of the keychain. Select “Export Public Keychain…” to export a file you can share with other people or devices that you wish to make part of the account.

   Using the same menu, select “Import keychain…” to import public or private keychains from file.

Versions below 0.8.0

In the Keychains tab, click on one or more of the keychains just created to select them. Then from the Keychains menu, select "Create Account…" – or alternately, click on the toolbar icon (hover over toolbar icons to get a tip). You will be prompted to name the account. The second line will display the list of selected keychains. The third line contains a dropdown list where you can select the minimum number of signatures that the account policy requires. For instance, if you had selected three keychains and chose two minimum signatures, this would create an account with a 2-of-3 signing policy. In order to send payments from the account, at least two of the selected keychains would be needed.

Versions 0.8.0 and above

Click "New Account" button on toolbar. Check the keychains you wish to use to sign for the account, then select the minimum signatures required. The creation time defaults to your system clock – it is used to determine how far back in the blockchain to scan. Make sure the creation time precedes the first transaction made to the account.

You'll see the new account appear in the Accounts tab. Right-click the account to get a popup menu. Select "Export Account…" to backup the account to file – this backup will include any private keys you have. To export the public watch-only account, select "Export Shared Account…" instead. You'll be able to import this file on another device where you can view all activity with signing functionality completely disabled.

3. Connect to network.

By default, mSIGNA™ will attempt to connect to a bitcoin node running on localhost (i.e. a local running instance of Bitcoin-Qt). If you have Bitcoin-Qt running on your computer, leave this setting alone. If you would prefer to connect to a remote bitcoin node, you can change the IP address and port under Network->Settings…(File->Preferences … on Mac).

NOTE: mSIGNA™ only connects via the peer-to-peer protocol and does not require any special RPC access to other nodes.

At the bottom right of the main window, you should see two numbers followed by an icon. The two numbers tell you the blockchain synchronization state. The top number is how many blocks are stored in your vault file, the bottom number is how many blocks were in the blockchain the last time you synchronized. If you have not connected to the network before, it should read 0/0 and the icon should display a red X.

Make sure the bitcoin node to which you're connecting (i.e. Bitcoin-Qt) is synchronized, then select "Connect to <host>" from the Network menu – or click the "Connect" button from the toolbar. If the connection is successful, you should see the bottom number rise, then you should see the top number rise until they are the same. While this happens, the icon will contain a rotating arrow in an orange circle. Once the vault is synched, the icon will turn green.

4. Fund the account

Select the Accounts tab. In it you should see the account you just created. Make sure the account is selected. Click on the "Receive" toolbar button. You will be asked to give the payment a label and specify an amount – these are optional. Click the "New Invoice" button. At the bottom of the dialog you will see Script Details. On the right you'll get a QR code. Copy the "Address" from there and send a payment to it from another wallet. If successful, you should see the account balance credited the deposited amount.

5. View your transaction

Make sure the account is selected in the Accounts tab. Then select the Transactions tab. In it you should see the deposit you just made. Right-click on the transaction and select "View at blockchain.info" to open up a browser and view the transaction details.

6. Unlock keychains (versions 0.1.1 and up)

In the Keychains tab, you must right-click the keychains you want to use to sign transactions and click "Unlock keychain…" from pop-up menu. Once unlocked, the keychains can be used to sign repeatedly within a session. When the program is closed and reopened, the keychains will again need to be unlocked. This is a security feature

Versions 0.7.0 and above

You will have the option to set a keychain passphrase. This will encrypt the keychain – the decrypted keychain will only be kept in memory while the keychain is unlocked. When exporting the keychain or account to file, only the encrypted keychain will be saved.

VERY IMPORTANT: IF YOU FORGET YOUR PASSPHRASE, TOO BAD! You might want to write down the passphrase and save it in a different location from where you store the encrypted keychain backups.

7. Send your first payment

Select the Accounts tab. Make sure the account from which you want to send is selected. Click the "Send" toolbar button. You will be asked to specify a fee, an address, an amount, and a label (For). A fee is generally required by the bitcoin network for transactions involving outputs smaller than 0.01 BTC, so if you're sending very small amounts it is recommended to use a fee of at least 0.0005 BTC. A higher fee tends to result in faster confirmation times, but exact confirmation time cannot be predicted.

Once you've entered the transaction information, click "Save Unsigned".

The unsigned transaction will appear at the top of the Transactions tab. Right-click it and select "Signatures…" to open the signature dialog. At the top you'll see the unsigned transaction hash as well as the number of signatures that are still required. Right-click a keychain and select "Add signature…" to sign for that keychain. NOTE: You can only sign for keychains for which you have the private master key.

From the same popup menu, you can select "Export Transaction To File…" and "Import Transaction From File…". Use these commands to share unsigned or partially signed transactions as files with other people or other devices. Any added signatures get merged into the transaction when you import it.

Once the minimum signatures required by your m-of-n policy have been added you'll have the option to send the transaction to the network by right-clicking it and selecting "Send Transaction".

Congratulations!

Again, thank you for deciding to try mSIGNA™.