Multi-signature Bitcoin with Casa Keymaster

Don’t Trust. Verify. Service Capabilities and Caveats.

by @vicariousdrama

640679 - 644340

Table of Contents

Introduction

Casa Keymaster is a managed service that has been available since 2018 to help you stay in control of your bitcoin, maximizing security. In essence, it's a multisig offering where you maintain full control of all but one key whether you're using their gold 2-of-3 plan, the platinum 3-of-5 plan, or their diamond 3-of-6 plan. The key they maintain is an emergency key to help get you back solid if you lose one, or in some cases multiple keys in your possession.

If you haven't yet read past articles by WizardofAus titled 'Not Your Keys, Not Your Bitcoin', and 'Level Up Your Bitcoin Security', you may want to read those first as they off excellent primers on the security of your coin. Multisig, a feature available in Bitcoin since 2012 takes this to the next level. To spend coins from addresses in a multisig wallet requires a specified number of cosigners to sign the transaction established at the time the wallet was setup.

Casa provides great documentation and YouTube videos about the benefits of their service. My intention is not to duplicate that content, or for this article to be an advertisement, but rather bring attention to how you can test and verify their offerings. This article examines this through use of the basic Gold 2-of-3 plan, which you can get free for a 30 day trial, and then decide where to go from there.

Within, you'll see ✔ indicators for a feature that was verified, and ⚠ to alert you to aspects you should be aware of should you choose to use Casa.

Change History

2020-08-19 – Initial Document
2023-02-19 – Add footers for page numbers, adjust table of contents and symbols

The Test Bed

For my testing I've done everything with only the Gold Plan. Where there are known differences as it relates to the service, I make mention of those below.

Android Phone - My starting hardware of choice is an android phone. The applications should be very similar in appearance and functionality between Android and iPhone. Through testing I encountered an issue where Casa personnel indicated that it was fixed on the iPhone version of their app, but overall there were no showstoppers.

Hardware Wallets - Although Casa supports Ledger Nano S, Ledger Nano X, Trezor One, Trezor Model T and Coldcard, unless explicitly called out, all my testing so far has been with Coldcards only with the intent to fully airgap signing transactions.

Emails - Most email interactions I transition to using email and the resultant website steps on my primary computer. However, if you only have a mobile device, and the appropriate hardware to interface hardware wallets with such device, that works as well.

Website Signup and Privacy Concerns

The first thing you'll be asked to do to make use of Casa Keymaster is to sign up for an account on the website. When signing up for the Gold plan to try 30 days free, in total you'll still need to provide

- Your name, or a name to be referred to as
- Email address
- Create a Password
- Specify answers to three security questions
- Credit Card number, expiration, and I believe zip code

It's important to note that the email address needs to be "real", and one for which you'll have ongoing access to in the future. The managed service is exceptionally email heavy in concert with the app. In discussions with key personnel from Casa, it was indicated that you could use a more private email address such as protonmail, and even pay with Bitcoin instead of a credit card.

Your password, and the answers to security questions can be memorable, or auto-generated. I usually treat security questions as another credential and dont use real answers. Some consideration should be given here regarding whether you want to auto-generate random values for security question answers and track them like passwords, of if you should use attributes that you'd easily remember in the future if the need arose.

If you think this will help keep things private however, then you should bear the following in mind

- For the service as a whole, interaction follows the pattern of: initiate on app -> receive email -> web pages to perform steps -> return to mobile app
- ⚠ Assorted pages or sites of Casa also reference zdassets.com, calendly.com, typeform.com, w3.org, googleapis.com, cloudflare.com, amazonaws.com. While reach is minimal you should be aware of this.
- ⚠ Setting up protonmail requires a phone (consider throwaway) or donation which may compound identity privacy concerns
- ⚠ Since Casa needs the xpubs for devices to facilitate creation of transactions and derivation keys, they can see all transactions associated with the wallet.

For the purposes of the testing outlined below, I didn't setup a different email account or use anything like Tor.

Bottom Line: If you need absolute privacy, then I'd recommend DIY following the Glacier Protocol and appropriate use of Tor and strict network controls. Consider multiple addresses, including PO Boxes, remailers, and agents in other locales to facilitate paperwork, acquisition of equipment, and storage. For 99.9% of users, the information exposed to Casa is reasonable.

Casa Keymaster App Basics

After downloading the Casa Keymaster app from the Apple AppStore or Google Play, you'll use your credentials you created previously to login.

Without the Gold plan, you will only see Single Key mode, and the wallet acts like any other typical Bitcoin wallet with a few extra benefits. The app saves your private key in an encrypted format to your Google Drive or Apple iCloud allowing you to restore if you delete the app. Furthermore, there is a health check function, and ability to check the backup. I verified that sending some bitcoin to the displayed address did indeed show up in that account.

With the Gold plan, you now have access to a Basic Multisig wallet in addition to Single Key mode. I setup this wallet using my phone and a Coldcard. The process for doing this entails initiating the action on the phone to add the new hardware wallet, and receiving an email with a link to follow. On the page you can choose whether using a Ledger, Trezor, or Coldcard as the instructions will differ. I opted for Coldcard, and it walked me through how to export the XPubs from the Coldcard and then upload that file back to the website. When that completed, the app on my phone showed the hardware device added.

Sidenote: The Coldcard I used during setup actually had a flaw where the cancel (X) button would not work. Hardware wallets can and do go bad, and this emphasizes another benefit of multisig solutions. Had this been a singlesig setup where I didn't have the seed phrase I could have lost funds associated with the wallet.

✔ Funding Single Key from external bitcoin
✔ Setup Basic Multisig with phone+coldcard
✔ Funding Basic Multisig from external bitcoin
✔ Send from Basic Multisig to Single Key (now there are 2 UTXOs)
✔ Send from Single Key to Basic Multisig choosing UTXO to use
✔ Send from Single Key to External address
✔ Verified receipt of Sovereign Recovery instructions

⚠ Control over fees is somewhat limited within the app. Regardless of Single Key or Basic Multisig, the options are tied to an option for Choosing Transaction Speed. The default is "Normal" targeting within 30 minutes. Additional options include Fast (10 minute), Slow (~1 hour), and Cheapest (~24 hours). The sats/byte are displayed for each, but no control is offered to adjust to specific fee values.

⚠ All transactions are broadcast through Casa servers. This gets back to the privacy considerations above. At this time there is no option to broadcast transactions through your own node or export to do so. When I asked Casa about

this, the response indicated this is one of those power user features they'd like to add, but would only serve a small portion of the user base and hasn't been prioritized yet. A detailed rationale was given regarding different failure scenarios that need to be covered.

⚠ The minimum size of a transaction is .0001 BTC, or 10000 sats. When I asked Casa about this, the rationale was that it avoids issues with very small transactions being dropped out of node memory. They can always raise it as bitcoin goes up in price and people are sending smaller amounts.

⚠ There is currently no support for multiple outputs or control over change addresses in transactions. Transactions can only have one output, and automatically set the change address.

⚠ There is currently no support for displaying amount of Bitcoin in Satoshis, or forcing to 8 decimal places. When I reached out to Casa regarding this, they indicated its on their roadmap to add in the future.

Performing Health checks

Periodic health checks are a good way to verify everything is good. Just like regular dental, medical and vision checks, you should check that your hardware wallets are functioning as intended. The Casa app helps facilitate this for the keys you are controlling with it, and keeps a log of when a device was last checked as well as when a backup was most recently performed.

For Single Key, this is accessed by tapping the Single Key balance, and then choosing 'Perform Health Check'. You can also check the backup.

✔ Single Key Health Check
✔ Verified app shows when a health check was last performed
✔ Perform Check Backup

For Basic Multisig, each device can be checked individually. The process for performing a health check on a hardware wallet is as follows.

- Initiate health check on device in the app
- Receive an email
- Follow link, and follow steps to sign the message
- Upload result to the webpage

✔ Hardware Wallet Health Check

⚠ You can save health check results and resubmit them. I brought this to Casa's attention and they indicated that this is because the health check link is valid for a period of time. So the link in the email is only good for a certain period.

✔ Verified older Health Check result is not accepted for newer health check

⚠ Submitting signed messages that have been altered do not result in UI feedback. If you upload a signed message that has been tampered with in response to the Health Check, the website UI will not show that an error has occurred. This is an edge case though and only possible through direct modification, malware in browser extensions, or other MITM attack.

✔ Verified app only acknowledges successfully completed health checks

Signing Transactions

After preparing a multisig transaction in the app, you'll need to sign it. When you Begin Signing the Transaction, For Basic Multisig, the default set up you choose from 2 of

- Phone
- Hardware Wallet
- Casa Recovery Key

✔ Verified ability to sign with Phone

For setups where you don't use the phone, and instead 2 hardware wallets, the options are

- Hardware Wallet
- Casa Recovery Key

For the Hardware wallet, this initiates an email, where you follow a link and walk through the steps for signing. You choose the type of device you're signing with. For Coldcard, download the PSBT file, transfer to device, choose Ready to Sign, verify the amounts of destination and change address are as expected and choose OK. The updated PSBT is created, and can be uploaded in response after clicking Next on the webpage. A confirmation page indicates if it worked or failed. These steps are repeated for as many signers are needed for hardware devices.

✔ Verified acceptance of signed transaction
✔ Verified non-members of the keyset cannot sign
✔ Verified ability to cancel pending transactions

For setups using 2 hardware wallets, Casa detects which device is associated with the Home Device vs the Safe Device and indicates which device signed it in the app.

✔ Verified app identified Home Device properly
✔ Verified app identified Safe Device properly

In the event that you don't have one of your devices (due to it being lost, destroyed, compromised, etc), the Casa Recovery key can be used. For Gold level accounts, you need to answer your security questions and once complete, starts a 7 day countdown before the key will be used to sign it. An email is sent on each day and the request can be cancelled at any time. The 7 days are to give the user time to notice if someone has tried to maliciously request the recovery key. Per

Casa, at the Diamond and Platinum level, they sign within 48 hours and that process involves a video verification call to ensure the client is not under duress.

✔ Verified Casa Recovery Key 7 Day wait for Gold plan
✔ Verified Casa wasn't easily coerced into shortening period for my testing

⚠ Use of Casa Recovery Key entails not only the 7 day countdown, but up to one additional day after that before the signing occurs. Plan on an 8 day period of time for this to occur. During that 8 days, fees can change dramatically, and a caveat to multisig transactions is that the fee is set at the beginning and cannot be altered.

Changing Keysets

On occasion, you may find that one of your devices no longer functions, or is lost. Herein lies a benefit of multisig, and in particular the seedless concepts around Casa's service offering. With 2-of-3 Gold plan, you can lose one device, and still be able to recover. Likewise for the Platinum 3-of-5 plan, up to 2 devices could be lost. Similarly, for the Basic Multisig, this process is followed for changing from the basic Phone + Hardware wallet to Dual Hardware wallet setup.

Whenever a new keyset is created on the Casa account, the derivation path is incremented, and the Casa service walks you through the steps to establishing the new set and transfer funds from the old set to the new wallet.

The process for this is to mark a key as compromised. The app then shows this as unlinked, and to Continue Basic Multisig Setup. You then follow steps as before with a new device.

✔ Verified ability to mark a device as compromised
✔ Verified ability to add a new device
✔ Verified receipt of updated sovereign recovery instructions
✔ Verified ability to change to 2 hardware wallet setup
✔ Verified ability to change to using Ledger Nano S
✔ Verified ability to change to reuse previously used device back to Coldcard

⚠ At time of writing, you can re-add a compromised device by reuploading the same public.txt in the case of Coldcard as was done originally. When I reached out to Casa about this they indicated it appears to be a Coldcard specific issue and such action is blocked for Trezor and Ledger. Their dev team is looking into it.

Once a new keyset is created, the app will walk you through the steps to transfer funds from your old wallet to the new one.

✔ Verified ability to transfer funds to new wallet, signing with device marked as compromised / being replaced

✔ Verified ability to transfer funds to new wallet, signing with Casa Recovery Key

⚠ At time of writing, the Android app may not be overly clear on which device you should be using to sign the transactions. You need to sign with devices that *currently* have access to the old addresses, not the replacement device.

⚠ At time of writing, when starting the Funds transfer, the amount shown will be less than that depicted on the Assets tab. This is explained in the next screen as the fees, as precalculated. There is no option to set the fee threshold. When signing with Coldcard, 2 addresses, in addition to the network fee will be shown. From the app there is no way to verify that the two addresses are both on the new account. This can only be done by setting up a watch wallet in Electrum or other client using the sovereign recovery information. There is work being done within Casa to address this going forward.

Setting up a Watch Wallet

In light of the serious concern in the previous section, I feel compelled to point out that setting up a watch wallet in Electrum is fairly straightforward. Hector of Casa actually prepared a great article titled Creating Watch Only Wallets.

You'll need the public keys which can be exported from the devices, or you can look up from the Casa app. If you are starting with the xpubs, and know the derivation path, then you can use the guidance written by Jameson Lopp on How to Check the Coldcard Ypub which references Ian Colemans BIP 39 tool to get the BIP 32 extended public key from the XPub and derivation path, and then Jameson Lopp's xpub-converter to convert to Ypub.

✔ Verified ability to setup Watch Wallet following the articles
✔ Verified addresses match new wallet being funded

I strongly encourage anyone using Casa to setup a watch wallet, and integrate Electrum with their own full node and instance of Electrum running for monitoring and verification purposes. This should be done anytime you change keysets.

Sovereign Recovery

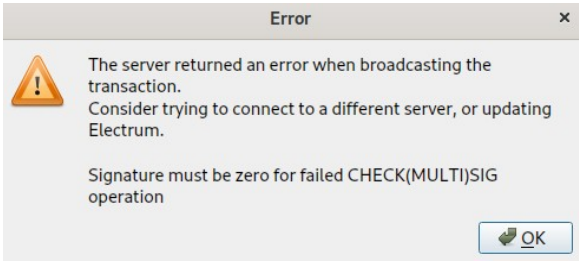
As part of initial signup for a Basic Multisig plan, and anytime you change one of the devices in your keyset, Casa sends out a templated email with Sovereign Recovery instructions. The primary information that changes, and is important to maintain, is the **Hardware wallet derivation path**, and the Ypub for the **Recovery Device Key**. For testnet, similar information is included as the Upub. I recommend printing the email and keeping with your important documents. For a sample of the instructions, see the Wallet Recovery website.

The steps are actually similar to when setting up a Watch Wallet.

⚠ At time of writing, I was unable to actually sweep funds from the multisig account as the instructions were written with the Coldcard setup for Firmware 3.1.9, Bitcoin 0.20.1 with Electrum 4.0.2.

When setting up in Electrum, I could only set the derivation path if I created the wallet with the Coldcards physically connected over USB. This largely negates the sought after benefits of being air-gapped.

With the wallet setup in Electrum, you can see all prior transactions, and this helps ensure you have set the correct derivation paths. A transaction can be created, exported for hardware device as PSBT files, and signed by each of the Coldcards. Subsequently these signed parts can be loaded and combined in the transaction and Electrum indicates the message as being Signed and ready for broadcast. However, once broadcast, an error is received indicating it is not valid. Through further diagnostics it seems that there is a problem in how Electrum is currently preparing transactions with respect to the bip32 derivation path in the exported PSBT.



⚠ The only way I could actually sweep funds was to retain the seed words when I setup the Coldcards, and use that information when creating the wallet in Electrum along with the derivation path and recovery device key.

Website Account Management

If you forget your password to Casa, or your account credentials are compromised, or you just want to change your password, you'll find that there is no automated "click here" and follow steps to change the password as you may be accustomed to on other services. Instead, per the FAQ article, you send an email request to support@team.casa. They will then send an email with a link that must be followed within a period of time

✔ Verified ability to change my account password
✔ Verified ability to logout/login on website and app with new credentials

⚠ Plan for up to a day for changing your account password

⚠ The Support option is Zendesk driven, but expands articles to support.keys.casa. The Sign in options on this page are not for the Casa account and are posted to https://casahodl.zendesk.com/access/login

The online Casa app shows your account status and provides a capability to allow you to Download Transaction History. This includes fields for

- Timestamp in UTC
- Coin Type (Presumably for TBTC in addition to BTC)
- Keyset Type (Phone or Basic Multisig, as differentiator)
- Amount (Satoshi)
- To Address
- Transaction ID
- Fees (Satoshi)
- Fee Rate (sat/kb)
- Change Address Path (1 based)
- Casa Transaction ID
- Casa Wallet Account ID
- Casa ID of the User That Initiated the Transaction
- Raw Transaction Data

✔ Downloaded transaction history in CSV format
✔ Verified transactions match expectations

Settings allow for reviewing your payment method, adding new payment methods, and cancelling membership. Apart from reviewing information displayed, no options were tested here
✔ Verified payment information does not display full card number
✔ Verified ability to see when my subscription will renew.

Conclusion

Casa has a great start to making multisig wallets for users of all technical levels easy to embrace at a reasonable fee for the service they provide.

I recommend anyone considering Casa, or existing Casa users, to do their own due diligence in testing the setup, and periodically reverifying as the application and service may be updated over time.

Most critical for sovereignty is that users should not be embracing seedless setups at this time until its verified it can function for the hardware devices in use.

To reiterate -- **Do Not Trust what I have written in this article.**
Verify it for yourself!

Use the information as you see fit as a jumping off point to run through your own scenarios based on your personal threat model.