BitGo KeyCard

Created on Tue Dec 26 2017 for wallet named:

My BitGo Wallet

Print this document, or keep it securely offline. See second page for FAQ.

A: User Key

This is your private key, encrypted with your passcode.

Data:

{"iv":"pod678tOfp2tqbZm+MRsUw==","v":1,"iter":10000,"ks":256,"ts":64,"mode":"ccm","adata":"","cipher":"aes","salt":"hPhy2zE0l+Q=","ct":"jsDbxIYMjx81q5sfpYVsBOBlzJGwgzNqtJgOl5+BJPEFAi5mzK6i/bjRsTLQL5leUKBK0HA0O7EHbn7N/cbMSynKKvJ3APe/YAXtENcSZovG53eaJb4yDF8BBYcN3EFaUIPiD2KBAi1GObhpUES7N/xMlMoySXc="}

B: Backup Key

This is the public key held at Keyternal, a key recovery service. If you lose your key, Keyternal will be able to sign transactions to recover funds.

Data:

xpub6GiRC55CSC88u9uK4J8peToA6EzYr4MR97q8n8YpBewTJHXf5JbQUha1e7z8PHD9wyfnGYcE2V8ekh7EuFur12Kfw4RVCtdL4kCqoioNNwP

C: BitGo Public Key

This is the public part of the key that BitGo will use to co-sign transactions with you on your wallet.

Data:

xpub661MyMwAqRbcEaoyqu3TJJk3EGizbNM71KZ79r1QU9RBZ52TEq2CFU19BvwJusMMk91fFp7ms5skK4vbuz7BVbjzj7dSEDumJzi4PNa4a5Z

D: Encrypted Wallet Password

This is the wallet password, encrypted client-side with a key held by BitGo.

Data:

{"iv":"vD8HU0W3u7WbsjNS493zAQ==","v":1,"iter":10000,"ks":256,"ts":64,"mode":"ccm","adata":"","cipher":"aes","salt":"ZINSHWcjwcQ=","ct":"m1QUPNpBVRmvluZy2i7+XbVCtHG/"}

BitGo KeyCard FAQ

What is the KeyCard?

The KeyCard contains important information which can be used to recover the bitcoin from your wallet in several situations. Each BitGo wallet has its own, unique KeyCard. If you have created multiple wallets, you should retain the KeyCard for each of them.

What should I do with it?

You should print the KeyCard and/or save the PDF to an offline storage device. The print-out or USB stick should be kept in a safe place, such as a bank vault or home safe. It's a good idea to keep a second copy in a different location.

Important: If you haven't provided an external backup key, then the original PDF should be deleted from any machine where the wallet will be regularly accessed to prevent malware from capturing both the KeyCard and your wallet passcode.

What should I do if I lose it?

If you have lost or damaged all copies of your KeyCard, your bitcoin is still safe, but this wallet should be considered at risk for loss. As soon as is convenient, you should use BitGo to empty the wallet into a new wallet, and discontinue use of the old wallet.

What if someone sees my KeyCard?

Don't panic! All sensitive information on the KeyCard is encrypted with your passcode, or with a key which only BitGo has. But, in general, you should make best efforts to keep your KeyCard private. If your KeyCard does get exposed or copied in a way that makes you uncomfortable, the best course of action is to empty the corresponding wallet into another wallet and discontinue use of the old wallet.

What if I forget or lose my wallet password?

BitGo can use the information in QR Code D to help you recover access to your wallet. Without the KeyCard, BitGo is not able to recover funds from a wallet with a lost password.

What if BitGo becomes inaccessible for an extended period?

Your KeyCard and wallet passcode can be used together with BitGo’s published open source tools at https://github.com/bitgo to recover your bitcoin. Note: You should never enter information from your KeyCard into tools other than the tools BitGo has published, or your funds may be at risk for theft.

Should I write my wallet password on my KeyCard?

No! BitGo’s multi-signature approach to security depends on there not being a single point of attack. But if your wallet password is on your KeyCard, then anyone who gains access to your KeyCard will be able to steal your bitcoin. We recommend keeping your wallet password safe in a secure password manager such as LastPass, 1Password or KeePass.