Secret Monero Bridge Dapp
Keplr Wallet Security Risk

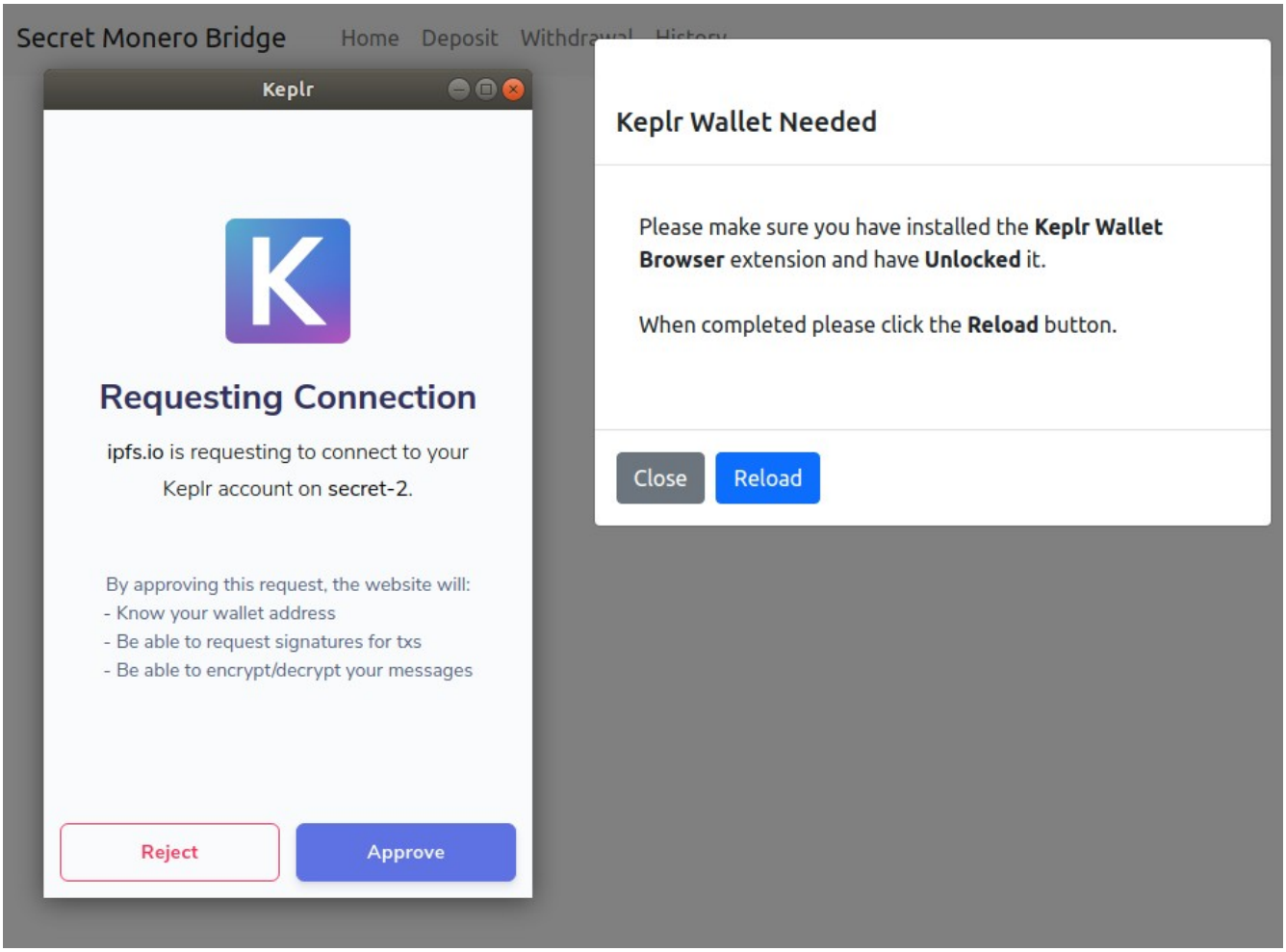
18 August 2021

Why do we use IPFS?

We distribute the Secret Monero Bridge Decentralized Application (Dapp) over the Interplanetary File System (IPFS) in order to massively decentralize the Dapp, to make it unstoppable and uncensorable. If we hosted it on a single web server, that server could easily be seized and shutdown. So IPFS, appears to be a good approach to attaining our objective.

Why the Keplr Wallet Manage Connections Warning?

The Keplr wallet Chrome extension, asks users to authorize the domain of the application to access the wallet. In the case of the Secret Monero Bridge Dapp (being distributed over IPFS public gateways), the Keplr wallet authorizes the domain of the IPFS public gateway to access the user's wallet, and stores this authorization in Settings-Manage Connections until the user removes it.

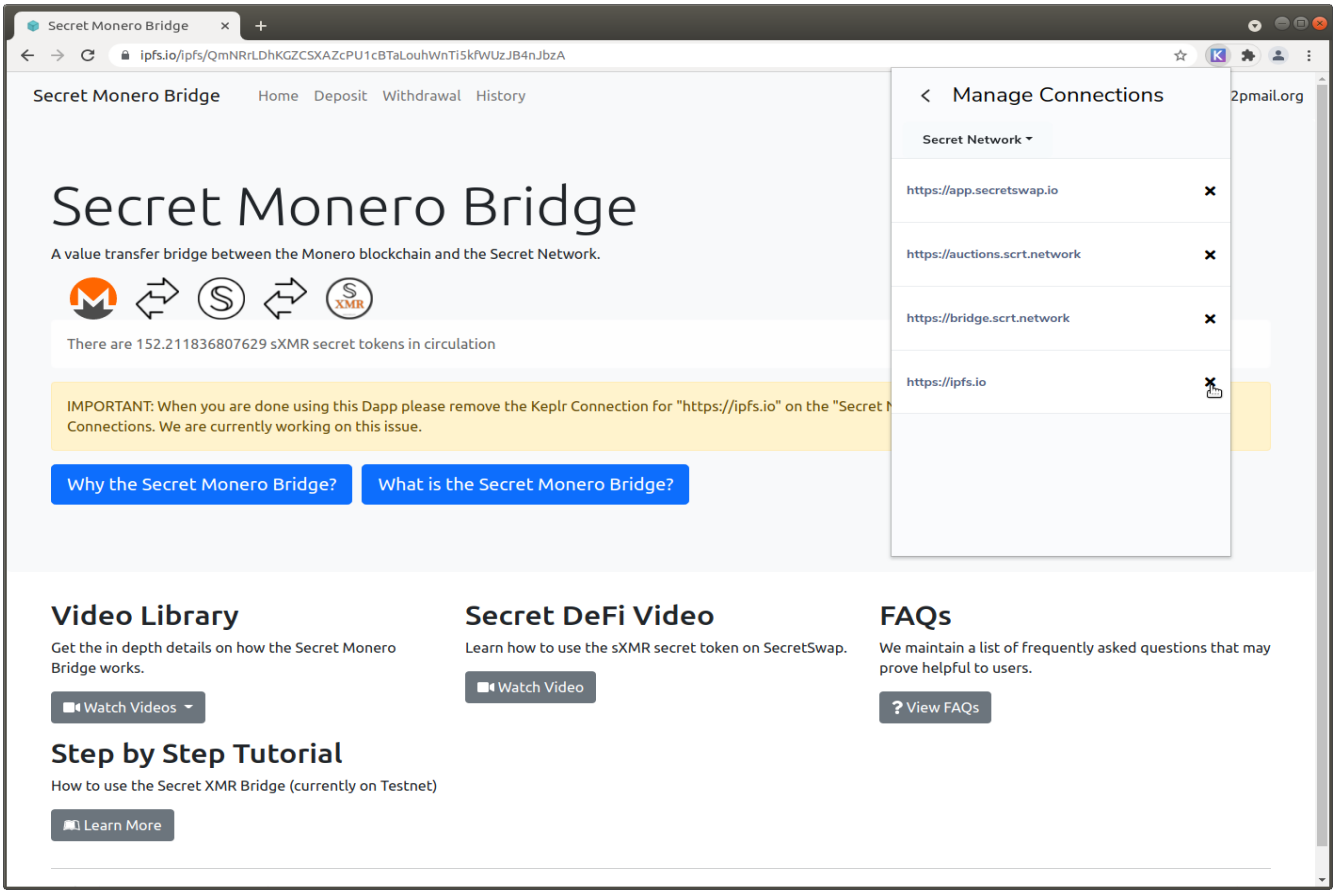


As can be seen in the screen shot above, Keplr is asking the user to authorize ipfs.io to connect to the wallet. Also note, that the request states:

> By approving this request, the website will:
> •Know your wallet address
> •Be able to request signatures for txs
> •Be able to encrypt/decrypt your messages

It is expected that users would approve this request if it applied directly to the Secret Monero Bridge Dapp. However, the Keplr wallet extension applies the authorization to the IPFS public gateway domain (ipfs.io in this case). This is a security risk, in that any other application presenting itself from the IPFS public gateway (ipfs.io in this case) would have access to the users wallet.

The only way to avoid the security risk is to remove the IPFS public gateway domain from the Settings → Manage Connections



By clicking the **X** in the Manage Connections window when you are finished using the Secret Monero Bridge is the only way to eliminate the security risk.

This is not an acceptable mitigation however, because users could forget to remove the IPFS public gateway domain authorization and in such circumstance, susceptible to the security risk.

Steps We Have Taken to Avoid this security risk

First step: notifying users of the security risk.

Second step, we have notified the Keplr wallet extension team of the security risk: https://github.com/chainapsis/keplr-extension/issues/136

Third step, we have made available a simple open-source web server application that runs on the user's machine to run the Secret Monero Bridge Dapp. Using our simple web server app with the Secret Monero Bridge Dapp and the Keplr wallet extension, the user ends up authorizing a localhost:port# to access the Keplr wallet. This eliminates the security risk mentioned above.

We will make the simple web application binaries available, and place the source code in our github repository for users who would prefer to inspect the code and/or build the binary themselves.

If you have questions regarding this security risk or our provided mitigation please feel free to send them to: smb@i2pmail.org