Technical Guide Voter Role

selfdriven Foundation Governance

Helping Communities
Self-Actuate

1 Zones 🟥 🟦

2 Protection

3 Hardware

4 Software

5 Identity & Roles

6 Voting

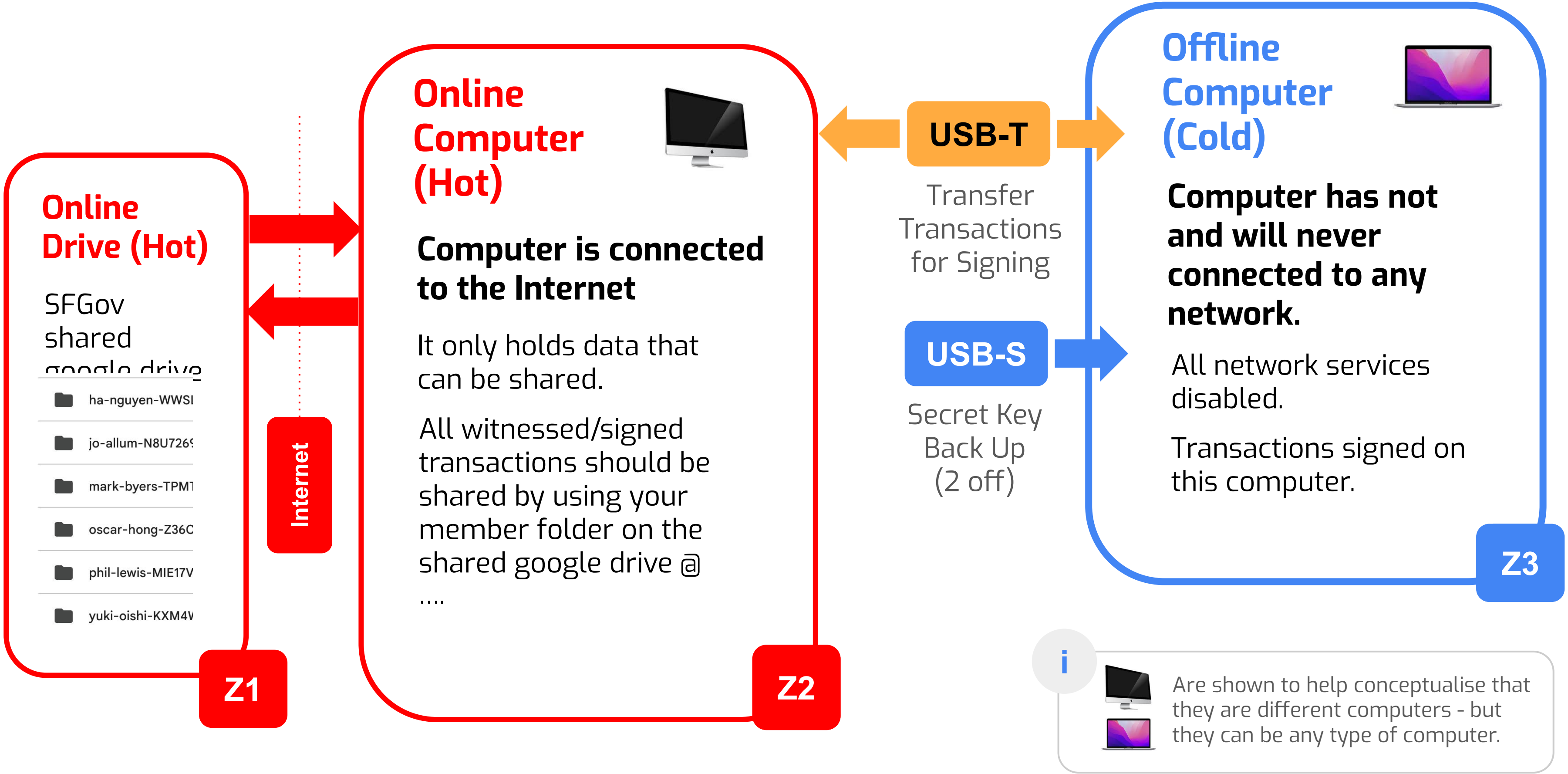
7 Instructions

i

Contact Mark Byers
for any questions
(mark.byers@selfdriven.foundation)

A Appendices

1 Zones



Online Drive (Hot)

SFGov shared google drive

- ha-nguyen-WWSI
- jo-allum-N8U726
- mark-byers-TPM
- oscar-hong-Z36C
- phil-lewis-MIE17V
- yuki-oishi-KXM4V

Online Computer (Hot)

Computer is connected to the Internet

It only holds data that can be shared.

All witnessed/signed transactions should be shared by using your member folder on the shared google drive @ ....

Transfer Transactions for Signing

Secret Key Back Up (2 off)

Offline Computer (Cold)

Computer has not and will never connected to any network.

All network services disabled.

Transactions signed on this computer.

Are shown to help conceptualise that they are different computers - but they can be any type of computer.

2 Protection

2A/ Risks

Information security risks are identified and recorded into the selfdriven Foundation Risk Register.
Each risk is then graded as “Negligible”, “Low”, “Medium”, “High”, “Critical”.
And then controls are put in place to ensure they are at the minimum level set by the member’s role.

2B/ Risk Levels based Roles

Voter: Minimum is Low
Membership/Orchestrator: Minimum is Negligible

2C/ Voter Role

This role technical has the lowest level of information security related to it.
Given the keys can easily be reset, are one of many and proxied via the Orchestrator (Head of Security) before use on-chain – mitigating many of the risks.

3 Hardware (Member)

3A/ Computer connected to the internet (Existing)

Used to access SFGov Google Drive foundation/governance/ folder **Z2**

3B/ Computer never connected to the internet

Used to sign transactions **Z3**

3C/ Three(3) USB Drives, Well Known Brand*, 16GB +

One(1) used to transfer files between computers **Z2** **Z3**

x2

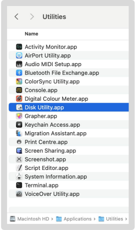
Two(2) used to hold secret keys **Z3**

* Sandisk / Samsung / Kingston / Verbatim / Lexar

Preparing USBs

1/ Put the USB into your **offline (cold)** computer

2/ On MacOS > Applications > Utilities > **Open Disk Utility**



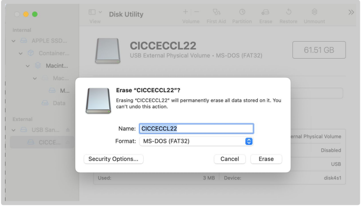
Utilities

Name

- Activity Monitor.app
- AirPort Utility.app
- Audio MIDI Setup.app
- Bluetooth File Exchange.app
- ColorSync Utility.app
- Console.app
- Digital Colour Meter.app
- Disk Utility.app
- Grapher.app
- Keychain Access.app
- Migration Assistant.app
- Print Centre.app
- Screen Sharing.app
- Screenshot.app
- Script Editor.app
- System Information.app
- Terminal.app
- VoiceOver Utility.app

Macintosh HD › Applications › Utilities ›

3/ Click on the USB > Click **Erase ..** button



CICCECCL22

USB External Physical Volume • MS-DOS (FAT32)

61.51 GB

Erase "CICCECCL22"?

Erasing "CICCECCL22" will permanently erase all data stored on it. You can't undo this action.

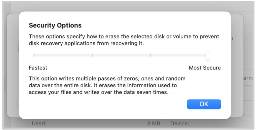
Name: CICCECCL22

Format: MS-DOS (FAT32)

Used: 3 MB Device: disk4s1

4/ Click **Security Options** > Slide to Most Secure > Click OK

5/ Rename the USB Drive to say “SFGov” & Select ExFat > Click **Erase**



Security Options

These options specify how to erase the selected disk or volume to prevent disk recovery applications from recovering it.

This option writes multiple passes of zeros, ones and random data over the entire disk. It erases the information used to access your files and writes over the data seven times.

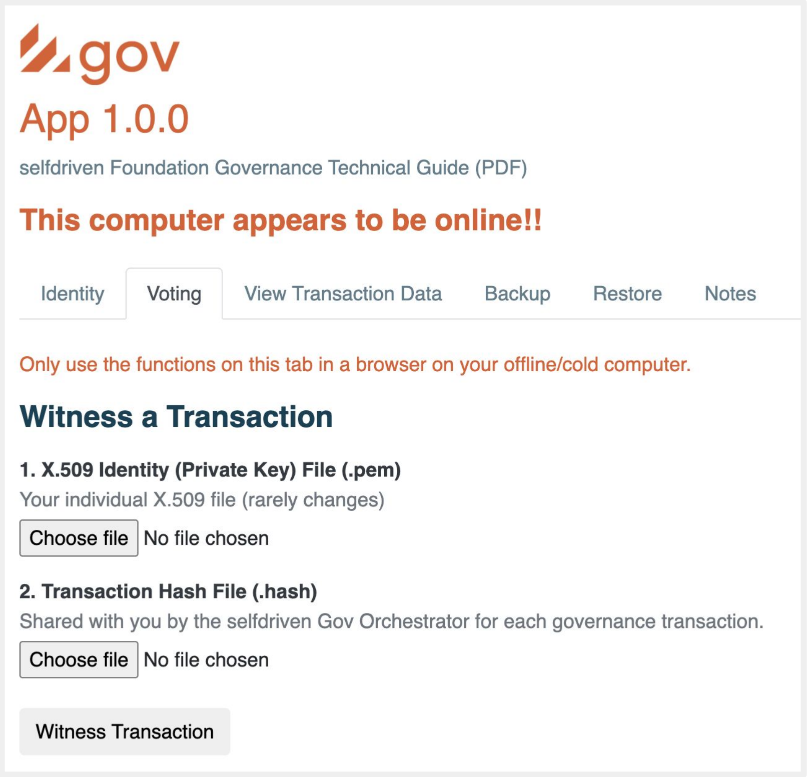
i

You can get a safe for the storage of your USBs, but if you are a Voter only, this is not critical as your Identity (X509) keys can be reset.

4 Software (Voter)

Z3

The follow software is in the Google Drive @ **/organisation/foundation/governance/app**



App 1.0.0

selfdriven Foundation Governance Technical Guide (PDF)

This computer appears to be online!!

Only use the functions on this tab in a browser on your offline/cold computer.

Witness a Transaction

1. X.509 Identity (Private Key) File (.pem)

Your individual X.509 file (rarely changes)

2. Transaction Hash File (.hash)

Shared with you by the selfdriven Gov Orchestrator for each governance transaction.

5 Identity & Roles

5A/ X509 Standard for Identity

X509 used by the internet to establish the identity of things (e.g. websites) and people.
It creates a set of keys linked to you. One key is public and one is private.
The private key needs to be kept secret and never leave the offline (code) “Z3” code.
You keep an encrypted copy of the private key on your “USB-S” drives.

(Instructions for member to generate X509 Certificate)

5B/ Roles / Voter Role

There a number of technical roles; Membership / Delegator / Voter.
This guide is focused on the Voter role.
This role technical has the lowest level of information security related to it.
Given the keys can easily be reset, are one of many and proxied via the Orchestrator (Head of Security) before use on-chain.

6 Voting

A/ Orchestrator (Head of Security) creates the transaction for the gov action id and sets the the vote to be as agreed by the SFGov as per its governance document. [Voting Sheet]

B/ Transaction put into each of the members Google Drive folder

C/ Each member then copies the transaction file to their Transfer USB (USB-T)

D/ Member then puts the USB-T drive into their offline (cold) computer [Z3] and copies the transaction file to the Computer hard drive.

E/ The USB-T drive is then removed from the computer.

F/ One of the USB-S drives is plugged into offline (cold) computer [Z3].

G/ Member follows the *Software voting instructions … (later in this doc [7E])*

7 Instructions (Step by Step)

7A/ Prepare USBs

7B/ Prepare Offline-Cold Computer

7C/ Copy Software to Offline-Cold Computer

7D/ Create Your SF Member Identity (X509 Keys)

7E/ Voting on a Governance Action

7F/ Backing Up & Restoring Private X509 Keys (PEM File)

7A Prepare USBs

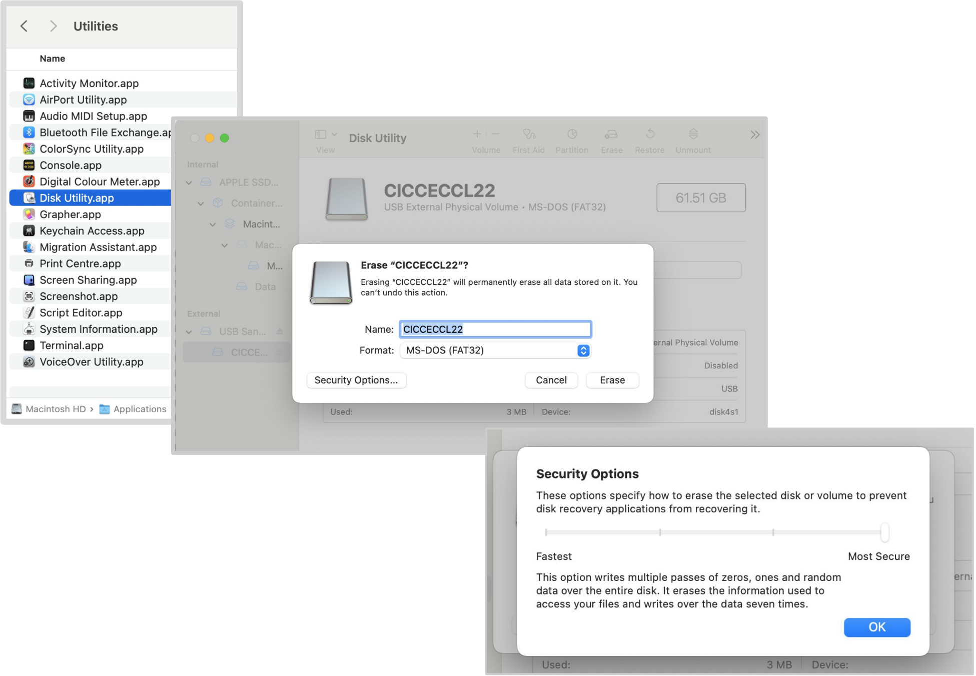
1/ Put the USB into your **offline (cold)** computer

2/ On MacOS > Applications > Utilities > **Open Disk Utility**

3/ Click on the USB > Click **Erase ..** button

4/ Click **Security Options** > Slide to Most Secure > Click OK

5/ Rename the USB Drive to say “SFGov” & Select ExFat > Click **Erase**



Erase “CICCECCL22”?

Erasing “CICCECCL22” will permanently erase all data stored on it. You can't undo this action.

Name: CICCECCL22

Format: MS-DOS (FAT32)

Security Options

These options specify how to erase the selected disk or volume to prevent disk recovery applications from recovering it.

This option writes multiple passes of zeros, ones and random data over the entire disk. It erases the information used to access your files and writes over the data seven times.

i

You can get a safe for the storage of your USBs, but if you are a Voter only, this is not critical as your Identity (X509) keys can be reset.

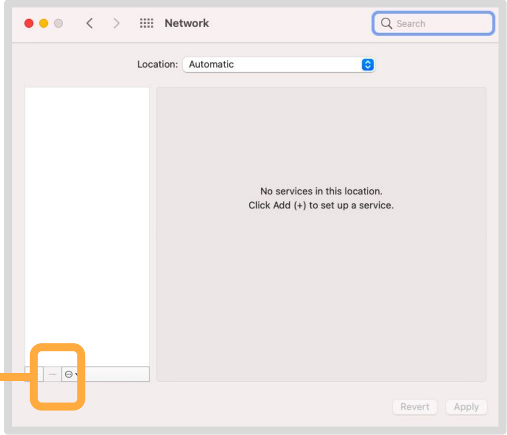
7B Prepare Offline-Cold Computer

1/ On MacOS > (Apple Logo) > **System Preferences ...**

2/ Click the **Network** icon

3/ Click the **(-) button** until all the “Wifi, LAN” options are removed.

> i
>
> If using the latest version of MacOS this is slightly different process, but it is the same intent of removing all network access.

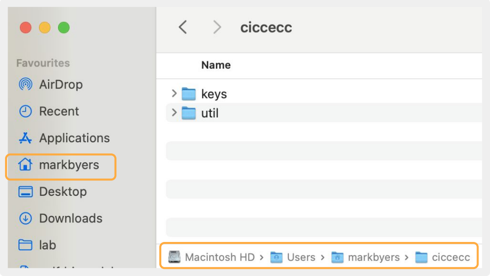


Location: Automatic

No services in this location.
Click Add (+) to set up a service.

4/ Using MacOS Finder or equivalent, create folders:

```
-   /sfgov
    -   /util
    -   /keys
```



7C Copy Software to Offline-Cold Computer

USB-T

Z2

USB-T

Z3

1/ **Insert the “USB-T”** transfer USB driven into the online/hot computer

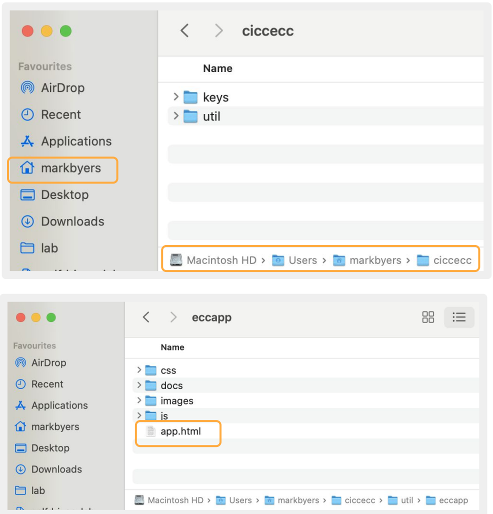
2/ **Copy** the **organisation/foundation/governance/app** zipped file to the USB drive.

3/ **Eject the USB** from the online-hot computer and **insert into your offline-cold computer**.

4/ **Copy the “util” folder from the USB** to the “sfgov” folder you created in step 7B

Note: If you downloaded the zip file, then you will need to unzip it it first, by right clicking on the ciccSFGov-util.zip and selecting Open With … Archive Utility,app …

i



ciccecc

Favourites: AirDrop, Recent, Applications, markbyers, Desktop, Downloads, lab

Name

- keys
- util

Macintosh HD › Users › markbyers › ciccecc

eccapp

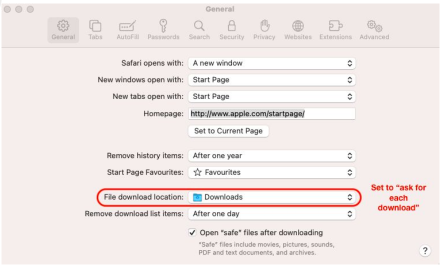
Favourites: AirDrop, Recent, Applications, markbyers, Desktop, Downloads, lab

Name

- css
- docs
- images
- js
- app.html

Macintosh HD › Users › markbyers › ciccecc › util › eccapp

i



Safari opens with: A new window

New windows open with: Start Page

New tabs open with: Start Page

Homepage: http://www.apple.com/startpage/

Set to Current Page

Remove history items: After one year

Start Page Favourites: ☆ Favourites

File download location: Downloads

Set to “ask for each download”

Remove download list items: After one day

☑ Open “safe” files after downloading

“Safe” files include movies, pictures, sounds, PDF and text documents, and archives.

Continued (7D Create X509 Identity) …

7D Create X509 Identity (.pem/.csr)

USB-T

Z3

1/ This will use a simple browser app that is in the **/sfgov/app** folder on your offline computer,

2/ **Get your unique "SF ID Code"** allocated by the SF Head of Security (e.g. Mark). You can get your code from the list @ Instructions for member to generate X509 Certificate.

3/ On your offline/cold computer using the MacOS Finder (or equivalent) open the **/sfgov/app** folder, and **double click on app.html.** This will open the web browser and show the **Eastern Cardano App.**

4/ Fill in your details and click "**Generate X509 Identity**" and **save the .pem file** to your **"keys" folder.** This is your private key that you must keep safe.

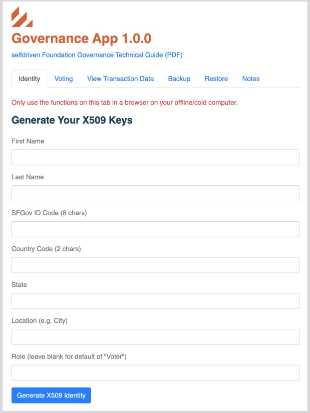
5/ Then click "**Generate X509 Certificate Signing Request**" and **save the .csr file** to your **"keys"** folder. This is your file that you need to share with Head of Security (e.g. Mark)

6/ **Copy the .csr file to your "USB-T" USB drive** and eject the drive and plug into your online computer.

7/ **Copy the .csr file to your folder on the SFGov shared google drive** - then let Head of Security (e.g. Mark) know.

! **After all steps completed, power-down your offline computer, to clear all memory of private information.**

i **/sfgov/sfgovapp/app.html**



Governance App 1.0.0

selfdriven Foundation Governance Technical Guide (PDF)

Only use the functions on this tab in a browser on your offline/cold computer.

Generate Your X509 Keys

First Name

Last Name

SFGov ID Code (8 chars)

Country Code (2 chars)

State

Location (e.g. City)

Role (leave blank for default of "Voter")

! **The .pem file is your private key, you must keep this secret!**

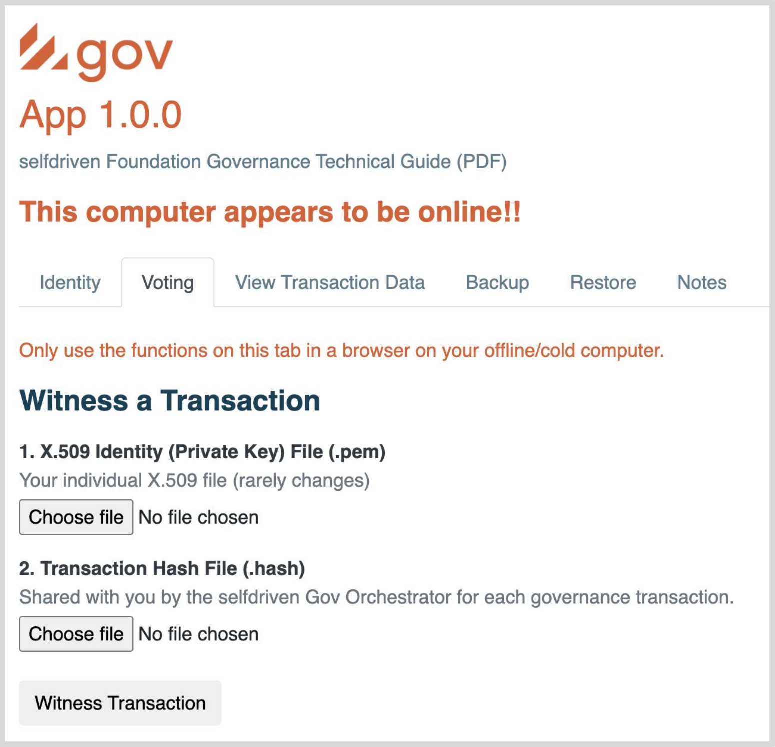
7E Voting on a Governance Action

1/ **As instructed by the SFGov Voting Orchestrator, copy the mainnet-sfgov-vote-[govaction reference].hash file** from the members voting folder on the SFGov shared drive to your **/sfgov/voting** folder on your offline computer using your USB-T,

2/ **Open the SFGov App on your offline computer** (/util/app.html), **select the files & click Witness Transaction, save the .witness file to the /voting folder on your offline computer.**

3/ **Copy mainnet-SFGov-vote-[govaction reference].-member-[firstname]-[lastname]-[code].witness** to your USB-T and then plug it into your online computer.

4/ **Copy mainnet-SFGov-vote-[govaction reference].-member-[firstname]-[lastname]-[code].witness** to your member folder on the SFGov Shared Members Folder.



gov

App 1.0.0

selfdriven Foundation Governance Technical Guide (PDF)

This computer appears to be online!!

Only use the functions on this tab in a browser on your offline/cold computer.

Witness a Transaction

1. X.509 Identity (Private Key) File (.pem)

Your individual X.509 file (rarely changes)

Choose file No file chosen

2. Transaction Hash File (.hash)

Shared with you by the selfdriven Gov Orchestrator for each governance transaction.

Choose file No file chosen

Witness Transaction

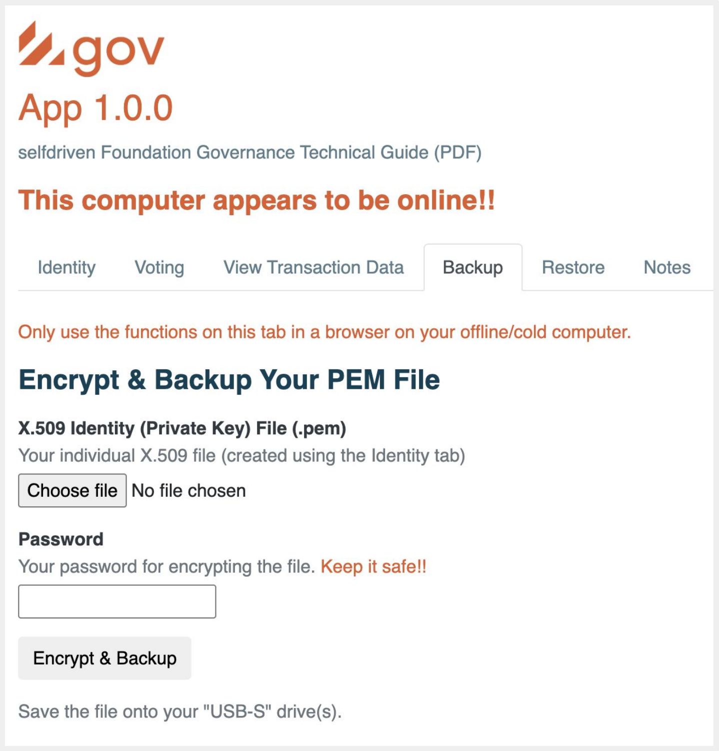
Z3

! **After all steps completed, power-down your offline computer, to clear all memory of private information.**

7F Backing Up & Restoring Private X509 Keys (PEM File)

Z3

1/ Use the SFGov App Backup tab to encrypt your keys



App 1.0.0

selfdriven Foundation Governance Technical Guide (PDF)

This computer appears to be online!!

Only use the functions on this tab in a browser on your offline/cold computer.

Encrypt & Backup Your PEM File

X.509 Identity (Private Key) File (.pem)

Your individual X.509 file (created using the Identity tab)

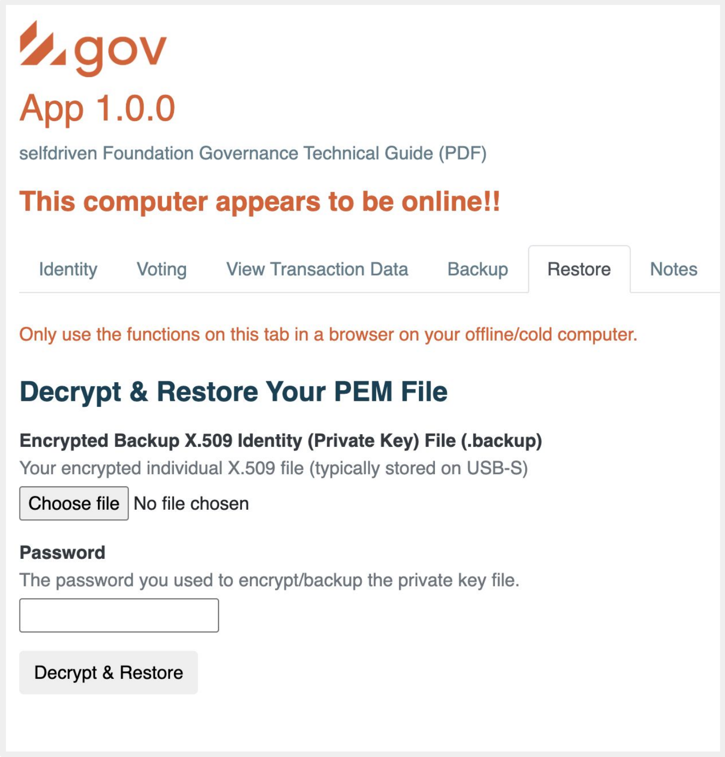
No file chosen

Password

Your password for encrypting the file. Keep it safe!!

Save the file onto your "USB-S" drive(s).

2/ Use the SFGov App Restore tab to decrypt your keys



App 1.0.0

selfdriven Foundation Governance Technical Guide (PDF)

This computer appears to be online!!

Only use the functions on this tab in a browser on your offline/cold computer.

Decrypt & Restore Your PEM File

Encrypted Backup X.509 Identity (Private Key) File (.backup)

Your encrypted individual X.509 file (typically stored on USB-S)

No file chosen

Password

The password you used to encrypt/backup the private key file.

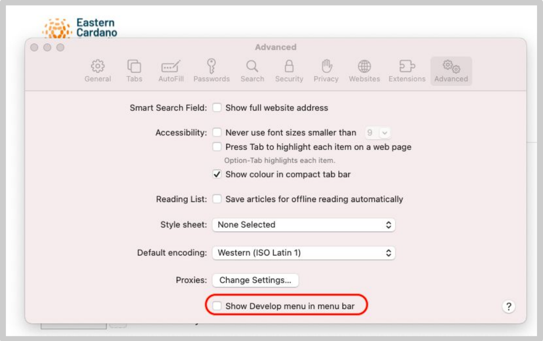
A Appendices

A1/ Safari - Enabling Developer Mode

A1 Safari Enabling Developer Mode

Z3

1/ Menu > **Safari > Preferences.. > Advanced Tab, tick “Show Develop menu in bar” and close the Preferences window..**



Smart Search Field: □ Show full website address

Accessibility: □ Never use font sizes smaller than 9
□ Press Tab to highlight each item on a web page
Option-Tab highlights each item.
☑ Show colour in compact tab bar

Reading List: □ Save articles for offline reading automatically

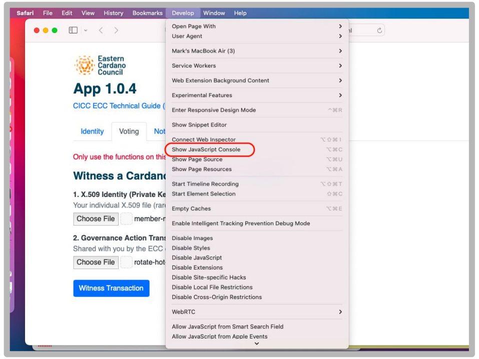
Style sheet: None Selected

Default encoding: Western (ISO Latin 1)

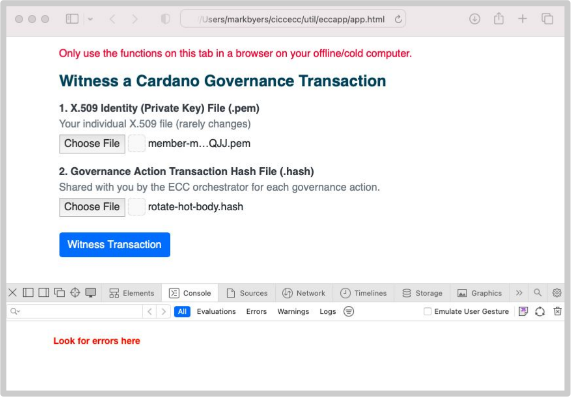
Proxies: Change Settings...

□ Show Develop menu in menu bar

2/ Menu > **Develop > Show Javascript Console.**



3/ Select the files & click Witness Transaction and then see if any errors in the Console tab. If there are then screenshot and send to the Orchestrator.



Only use the functions on this tab in a browser on your offline/cold computer.

Witness a Cardano Governance Transaction

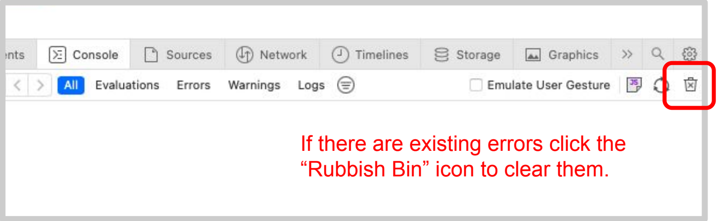
1. X.509 Identity (Private Key) File (.pem)
Your individual X.509 file (rarely changes)
Choose File member-m...QJJ.pem

2. Governance Action Transaction Hash File (.hash)
Shared with you by the ECC orchestrator for each governance action.
Choose File rotate-hot-body.hash

Witness Transaction

Look for errors here

i



If there are existing errors click the “Rubbish Bin” icon to clear them.