Technical Guide Voter Role

ICC Eastern Cardano Council

Constitutional Guardians
Bridging Cultures

1. Zones 
2. Protection
3. Hardware
4. Software
5. Identity & Roles
6. Voting
7. Instructions

Contact Mark Byers (Head of Security) for any questions (mark.byers@selfdriven.foundation) or if not available, contact Phil Lewis.

A **Appendices**

1 Zones

Online Drive (Hot)

ECC shared google drive

- ha-nguyen-WWSI
- jo-allum-N8U726
- mark-byers-TPM1
- oscar-hong-Z36C
- phil-lewis-MIE17V
- yuki-oishi-KXM4V

Z1

Internet

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 ECC shared google drive @ /technical/operations/members/x509

Z2

USB-T

Transfer Transactions for Signing

USB-S

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.

Z3

i

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 ECC 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 (Voter)

3A/ Computer connected to the internet (Existing)

Used to access ECC Google Drive /technical/operations 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

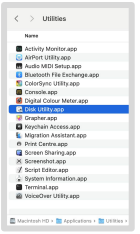
x2

Two(2) used to hold secret keys

Z3

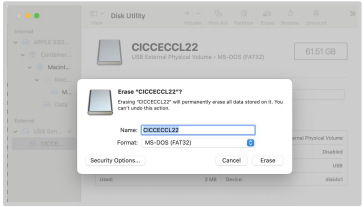
* Sandisk / Samsung / Kingston / Verbatim / Lexar

Preparing USBs



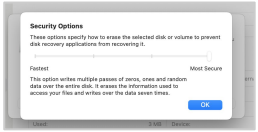
1/ Put the USB into your **offline (cold)** computer

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



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 “CICCECC” & Select ExFat > Click **Erase**

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 ECC Google Drive @ /technical/operations/members/util

4A/ OpenSSL (Ed25519)

This is a terminal tool that can be used to generate your X509 identity. You only need to do this once – and also encrypting your secret keys.

4B/ Cardano-cli

Used to sign the transaction (it does not need a Cardano Node).

4C/ Google Drive (CICC-ECC Shared Folder)

Used to transfer X509 requests/certificates, transactions to be signed, signed transactions.

i There is a more intuitive graphic UI coming, but these are the text based commands that can be used now.

i You can make it easier to access the MacOS terminal using these instructions.

i Instructions for member to generate X509 Certificate.

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 ECC as per its governance document. (Voting Sheet)

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

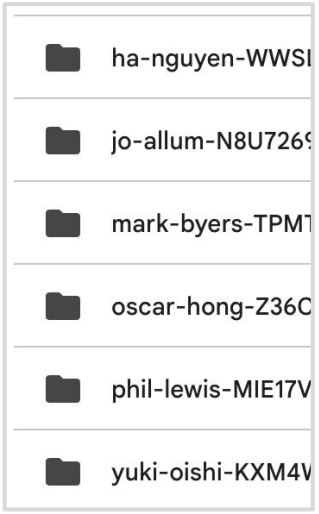
C/ Each member then copies the transaction file to their Transfer USB (USB-T)

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/ *Software voting instructions ...*



7 Instructions (Step by Step)

7A/ Prepare USBs

7B/ Prepare Offline-Cold Computer

7C/ Copy Software to Offline-Cold Computer

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

7E/ Voting on a Governance Action

7A Prepare USBs

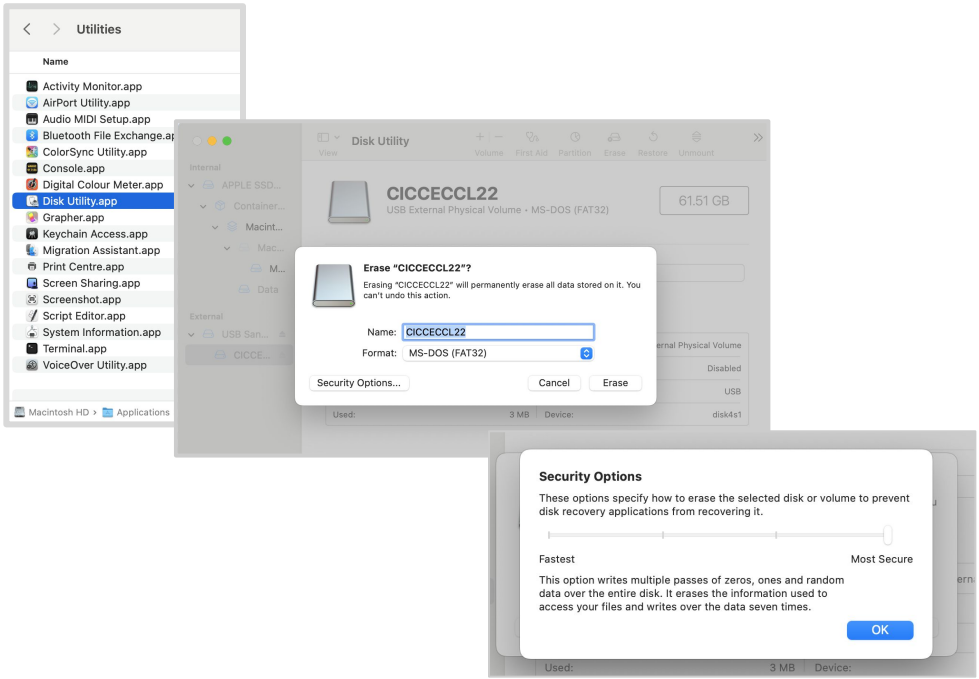
1/ Put the USB into your **offline (cold)** computer

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 “CICCECC” & Select ExFat > Click **Erase**



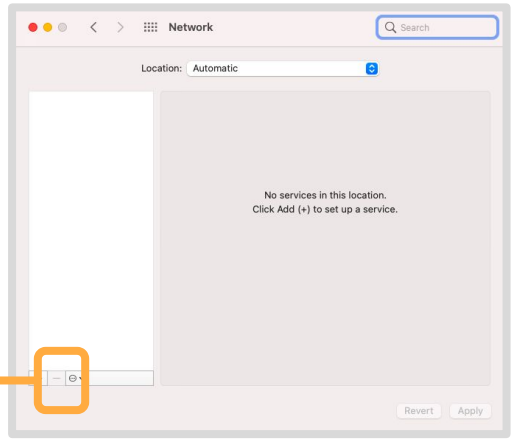
i You can get a safe for the storage of your USBs, but if you are a Voter only, this is not critical as your Identity (X509) keys can be reset.

7B Prepare Offline-Cold Computer

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

2/ Click the **Network** icon

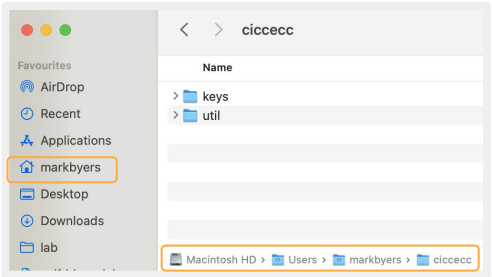
3/ Click the **(-) button** until all the "Wifi, LAN" options are removed.



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

4/ Using MacOS Finder or equivalent, create folders:

- /ciccecc
  - /util
  - /keys



7C Copy Software to Offline-Cold Computer

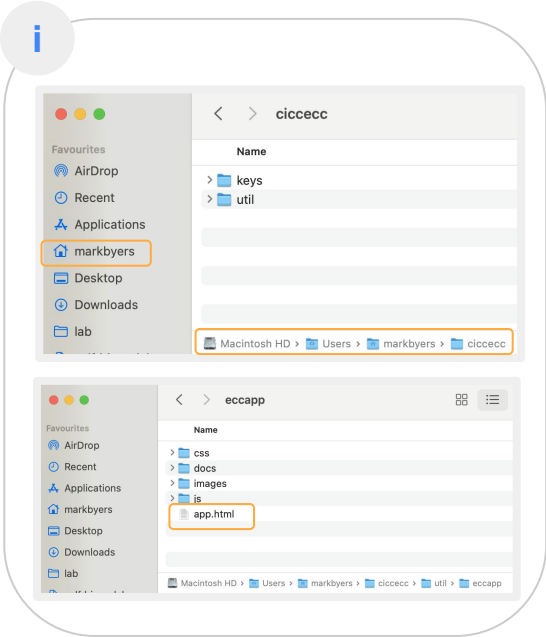
1/ Insert the "USB-T" transfer USB driven into the online/hot computer

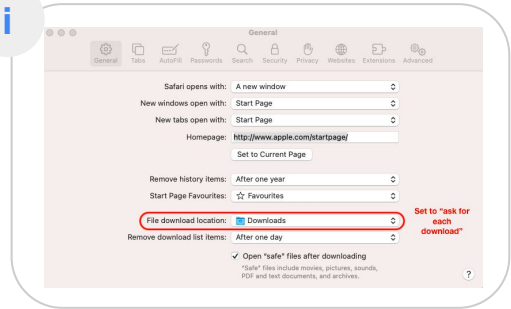
2/ Copy the **technical/operations/members/util** (zip) folder to the USB drive.

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 "ciccecc" 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 ciccecc-util.zip and selecting Open With ... Archive Utility,app ...





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 **/ciccecc/util/eccapp** folder on your offline computer,

2/ **Get your unique "ECC ID Code"** allocated by the ECC 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 **/ciccecc/util/eccapp** folder, and **double click on app.html.** This will open the web browser and show the **Eastern Cardano App.**

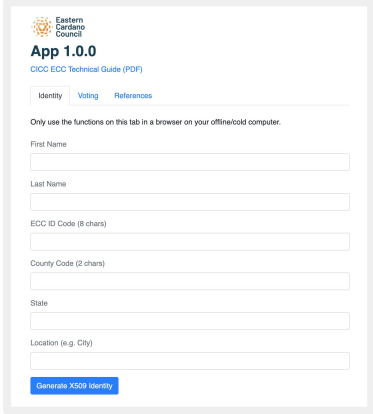
4/ Fill in your details and click "**Generate X509 Identity**" and **save the .pem file** to your **"keys" folder.** This is your private key that you must keep safe.

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 CICC-ECC shared google drive** - then let Head of Security (e.g. Mark) know.

i **/ciccecc/ecc/app/app.html**



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

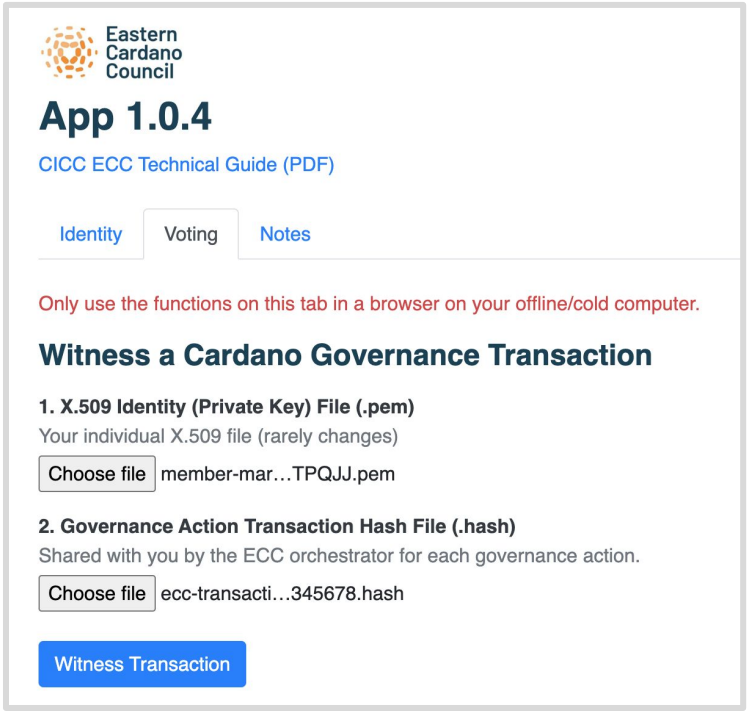
7E Voting on a Governance Action

1/ **As instructed by the ECC Voting Orchestrator, copy the ecc-transaction-(govactionid).hash file** from the members voting folder on the CICC-ECC shared drive to your **/ciccecc/voting** folder on your offline computer using your USB-T,

2/ **Open the ECC 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 ecc-transaction-(govactionid)-member-(firstname)-(lastname)-(code).witness** to your USB-T and then plug it into your online computer.

4/ **Copy ecc-transaction-(govactionid)-member-(firstname)-(lastname)-(code).witness** to your member folder on the ECC Shared Members Folder.



Z3

A Appendices

A1/ Util Advanced - Using openssl for X509 Identity

A2/ Converting Your Keys

A3/ Protecting & Storing Your Keys

A1 Util Advanced - Using openssl for X509 Identity #1

Z3

1/ Set up openSSL by copying the files to a specific folder on your MacOS

If you using Mac with a Silicon chip (e.g. M1, M2, M3, M4) then replace util/openssl with /util/openssl-silicon

```
cd ~/ciccecc
```

```
sudo mkdir -p /usr/local/Cellar/openssl@3/3.3.1
```

```
sudo cp -r util/openssl/ /usr/local/Cellar/openssl@3/3.3.1
```

```
export PATH="$HOME/ciccecc/util/openssl/bin:$PATH"
```

```
xattr -d com.apple.quarantine ~/ciccecc/util/*
```

i **To work out if you have a Silicon chip** - click the **Apple icon** top-left and **About This Mac**. If you see **Chip: Apple M1 M2, M3 or M4** then you have a Silicon chip and need to use the /openssl-silicon folder.

i **"sudo" is short for super user do. It will prompt you for your computer logon password.**

2/ Test that files copied and are set up OK, using MacOS Terminal, run:

```
openssl version
```

You should see:
"OpenSSL 3.3.1 4 Jun 2024 (Library: OpenSSL 3.3.1 4 Jun 2024)"

A1 Util Advanced - Using openssl for X509 Identity #2

Z3

1/ This will use software that you have copied to your offline computer to the **/util** folder.

2/ Each member has a unique code allocated by the ECC Head of Security (e.g. Mark).
You can get your code from the list @ **Instructions for member to generate X509 Certificate**.

3/ Open the MacOS Terminal and navigate to the **/keys** folder and run:

```
cd ~/ciccecc/keys
```

```
openssl genpkey -algorithm ed25519 \
-out member-[firstname]-[surname]-[code].pem
```

```
openssl req -new \
-key member-[firstname]-[surname]-[code].pem \
-out member-[firstname]-[surname]-[code].csr
```

Example answers, leave all other questions blank.

```
C = [your country code]
ST = [your state]
L = [your location/city]
O = Eastern Cardano Council
OU = Operations
CN = [firstname].[surname].[code].council.eastern.cardano
```

i **You can make it easier to access the MacOS terminal for a particular folder using these instructions.**

i **Text file with the MacOS terminal commands**

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

4/ Copy only the .csr file to your folder on the CICC-ECC shared google drive - then let Head of Security (e.g. Mark) know.

A2 Converting Your Keys

Z3

1/ You need to convert your .pem file to a Cardano formatted key, so it can be used to witness voting transactions.

2/ Open the MacOS Terminal and navigate to the **/keys** folder and run:

```
cp member-[firstname]-[surname]-[code].pem member.pem
```

```
node convert-pem-to-skey.js
```

```
rm member.pem
```

```
cp member-cardano.skey member-[firstname]-[surname]-[code].skey
```

```
rm member-cardano.skey
```

i [Text file with the MacOS terminal commands]

! **The .pem & .skey files are your private key - you must keep them secret!**

3/ Follow commands in the next slide to **encrypt the /keys folder** and then **copy to the "USB-S" USB drives** as a back up.

A3 Protecting & Storing Your Keys

Z3

USB-S

1/ **Your keys need to be encrypted with a password before storing on your "USB-S" USB drives.**

2/ **Encrypting using the MacOS Terminal in your /keys folder**

```
zip -r skeys.zip skeys/
```

```
openssl enc -aes-256-cbc -salt -in skeys.zip -out skeys.zip.enc -k
[password]
```

```
dd if=/dev/urandom of=skeys.zip bs=512 count=10
```

```
rm skeys.zip
```

Copy zkeys.zip.enc to your "USB-S" USB drives

3/ **Decrypt using the MacOS Terminal in your /keys folder**

Copy zkeys.zip.enc from your "USB-S" USB drive to /keys folder

```
openssl enc -aes-256-cbc -d -in skeys.zip.enc -out skeys.zip -k [password]
```

```
unzip skeys.zip -d /skeys
```

i **Text file with the MacOS terminal commands**

! **The .pem & .skey files are your private key - you must keep them secret!**

A4 Witnessing using cardano-cli

Z3

USB-S

1/ **Your keys need to be encrypted with a password before storing on your "USB-S" USB drives.**

2/ Open the MacOS Terminal and navigate to the **/voting** folder and run:

```
cardano-cli transaction witness \
    --tx-body-file transaction-[govactionid].json \
    --signing-key-file ../keys/member-[firstname]-[lastname]-[code].skey \
    --mainnet \
    --out-file transaction-[govactionid]-witness-[firstname]-[lastname]-[code].json
```

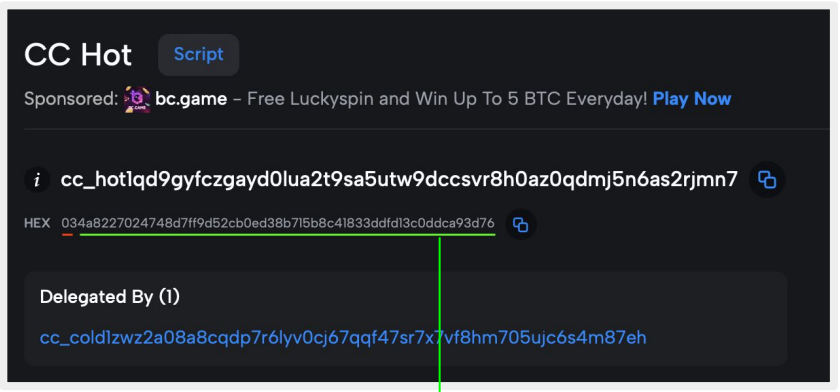
!

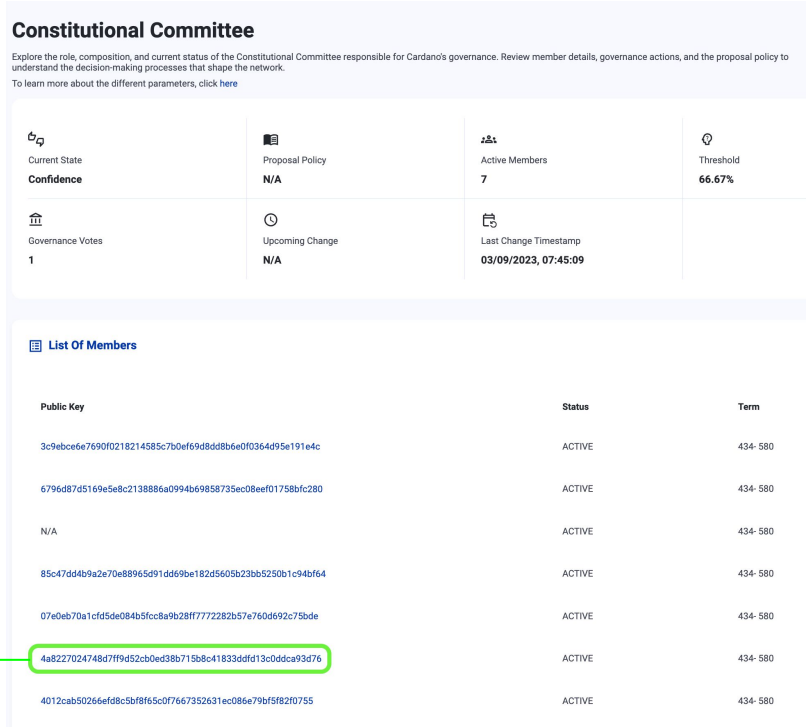
The .pem & .skey files are your private key - you must keep them secret!

A5 ECC Credentials On-Chain

https://cardanoscan.io/cchot/cc_hot1qd9gyfczgayd0lua2t9sa5utw9dccsvr8h0az0qdmj5n6as2rjmn7

https://beta.explorer.cardano.org/en/constitutional-committees/listMembers

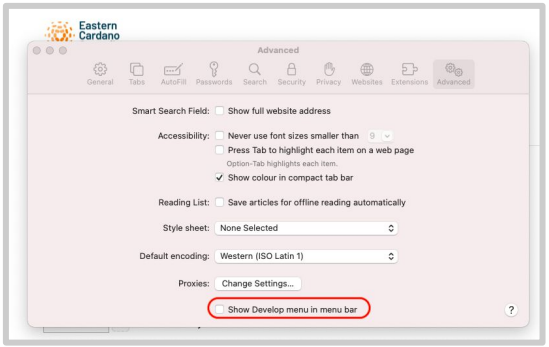




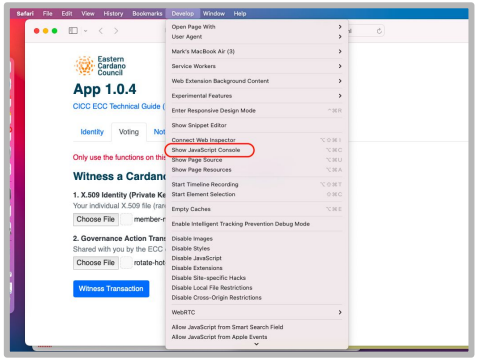
A6 Safari Enabling Develop Mode

Z3

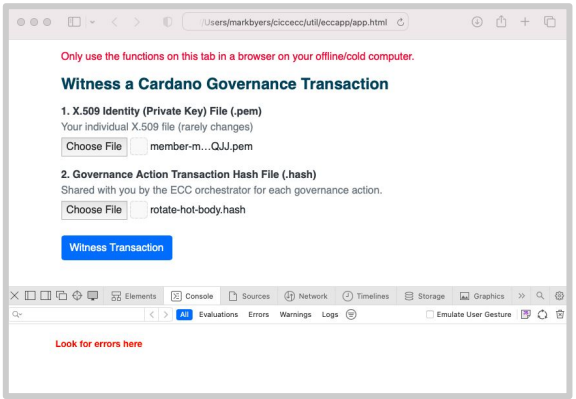
1/ Menu > **Safari > Preferences.. > Advanced Tab, tick "Show Develop menu in bar" and close the Preferences window..**



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.



i