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

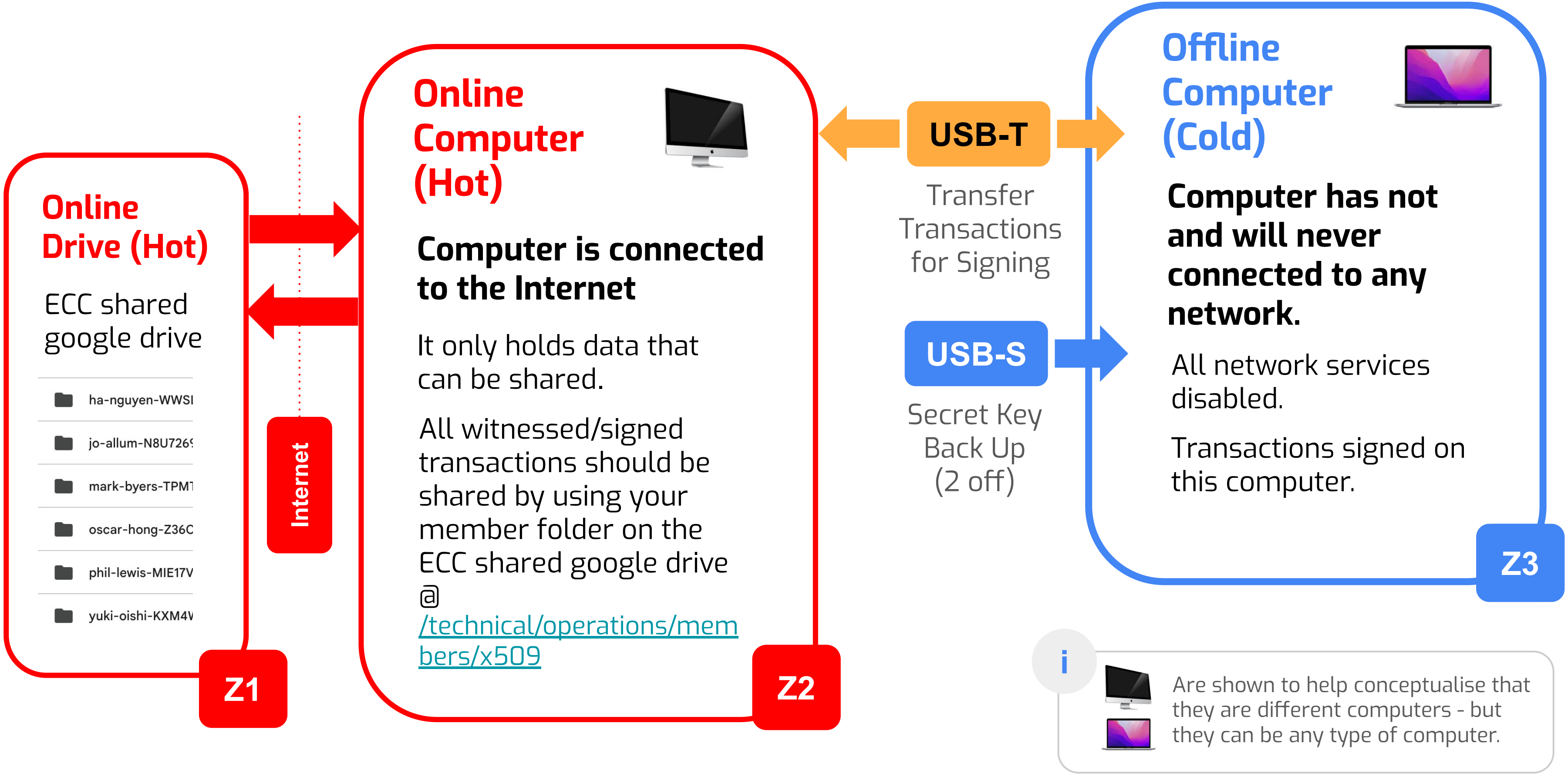
7 Instructions

i

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

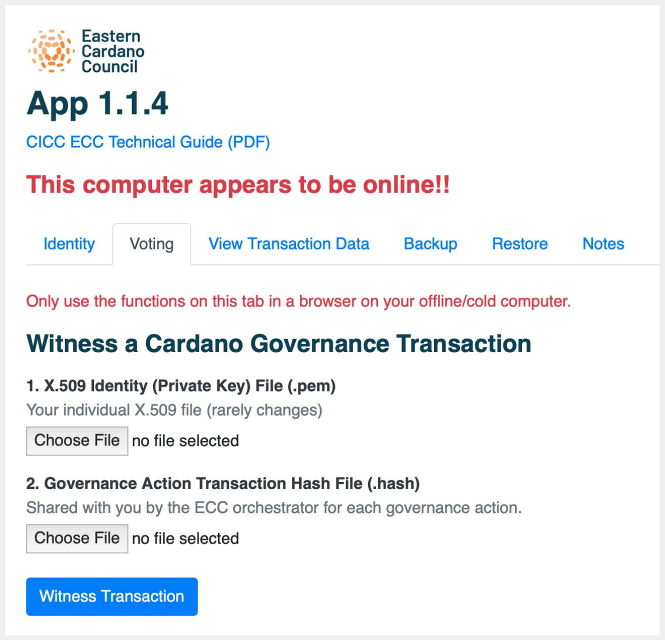
Information security risks are identified and recorded into the ECC Risk Register.
Each risk is then graded as “Negligible”, “Low”, “Medium”, “High”, “Critical”.
And then controls are put in place to ensure they are at the minimum level set by the member’s role.

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.



Eastern Cardano Council

App 1.1.4

CICC ECC 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 Cardano Governance Transaction

1. X.509 Identity (Private Key) File (.pem)
Your individual X.509 file (rarely changes)
Choose File no file selected

2. Governance Action Transaction Hash File (.hash)
Shared with you by the ECC orchestrator for each governance action.
Choose File no file selected

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

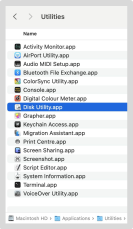
Z3

* Sandisk / Samsung / Kingston / Verbatim / Lexar

Preparing USBs

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

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



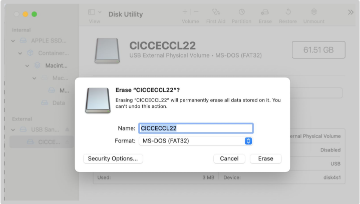
Utilities

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"?

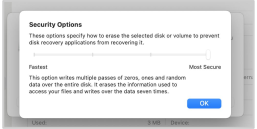
Erasing "CICCECCL22" will permanently erase all data stored on it. You can't undo this action.

Name: CICCECCL22
Format: MS-DOS (FAT32)

Security Options... Cancel Erase

Used: 3 MB Device: disk4s1

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



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.

Used: 3 MB Device:

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.

ECC App is used by members to generate X509 request.

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.

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

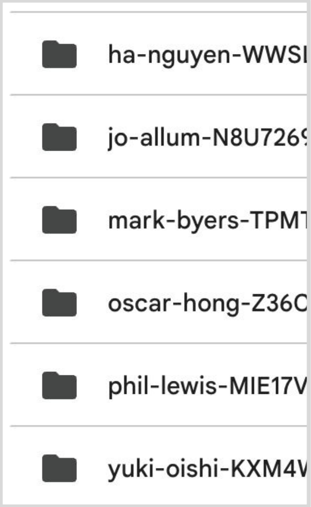
C/ Each member then copies the transaction file to their Transfer USB (USB-T)

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))*



ha-nguyen-WWSI

jo-allum-N8U726

mark-byers-TPMT

oscar-hong-Z36C

phil-lewis-MIE17V

yuki-oishi-KXM4V

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

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

7A Prepare USBs

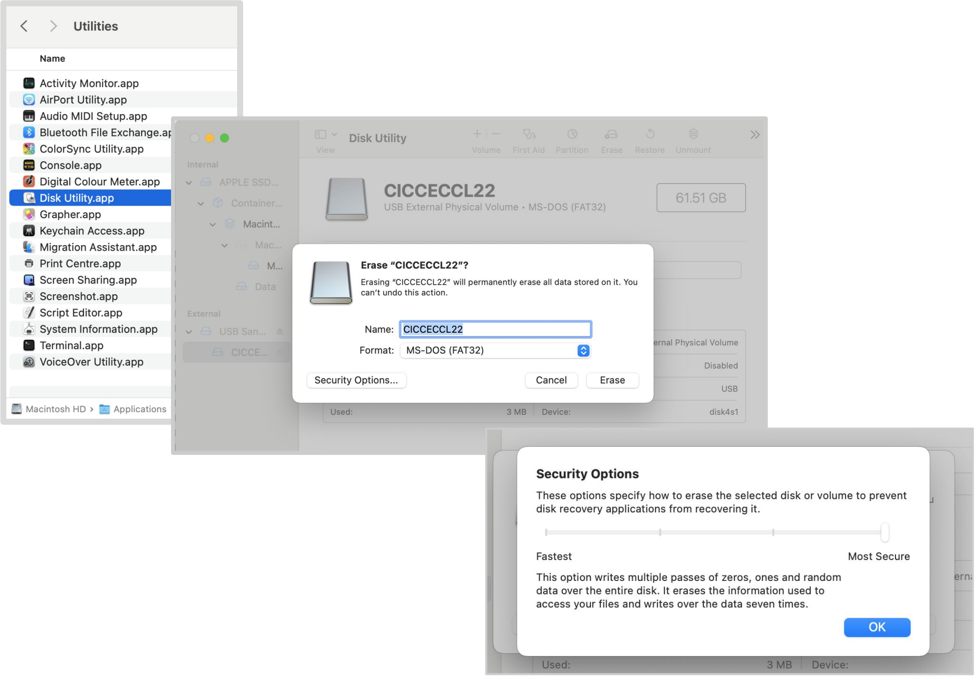
1/ Put the USB into your **offline (cold)** computer

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



Utilities

Name

- Activity Monitor.app
- AirPort Utility.app
- Audio MIDI Setup.app
- Bluetooth File Exchange.ap
- 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

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)

ernal Physical Volume
Disabled
USB
Used: 3 MB
Device: disk4s1

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

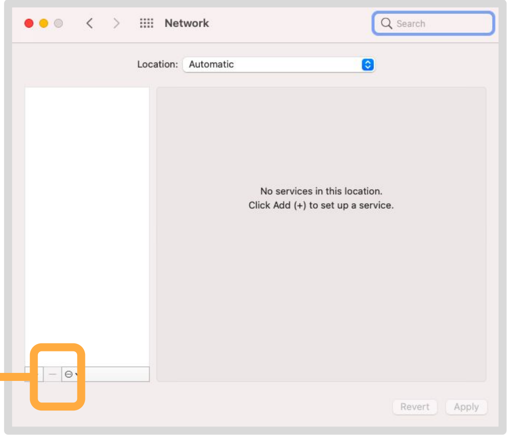
You can get a safe for the storage of your USBs, but if you are a Voter only, this is not critical as your Identity (X509) keys can be reset.

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.



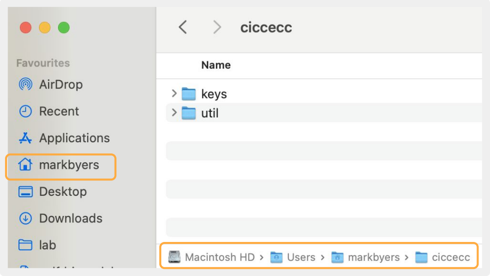
No services in this location.
Click Add (+) to set up a service.

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

USB-T Z2

USB-T Z3

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

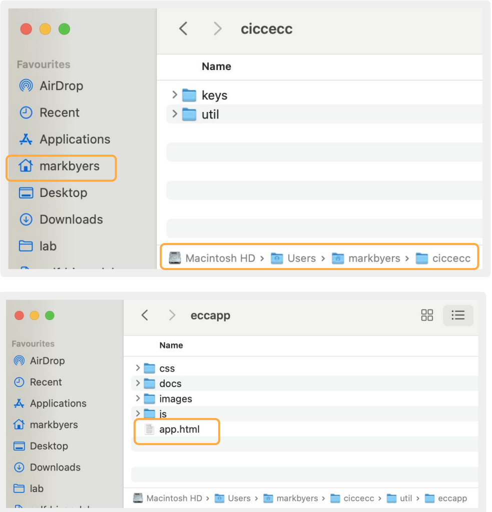
2/ Copy the **technical/operations/members/util** ([zip](zip)) folder to the USB drive.

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 …

i



ciccecc

- keys
- util

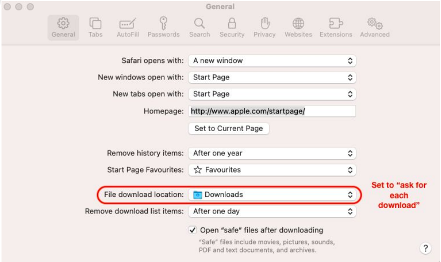
Macintosh HD › Users › markbyers › ciccecc

eccapp

- 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/

Remove history items: After one year

Start Page Favourites: ☆ Favourites

File download location: Downloads

Remove download list items: After one day

☑ Open “safe” files after downloading

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

Set to “ask for each download”

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 online members list,

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.

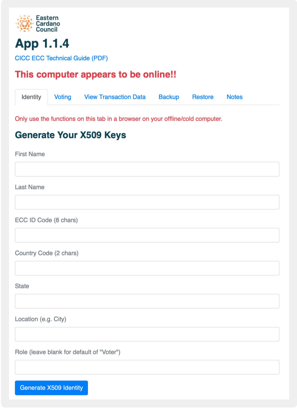
5/ Then click "**Generate X509 Certificate Signing Request**" and **save the .csr file** to your **"keys"** folder. This is your file that you need to share with Head of Security (e.g. Mark)

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.

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

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



Eastern Cardano Council

App 1.1.4

CICC ECC Technical Guide (PDF)

This computer appears to be online!!

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

Generate Your X509 Keys

First Name

Last Name

ECC 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

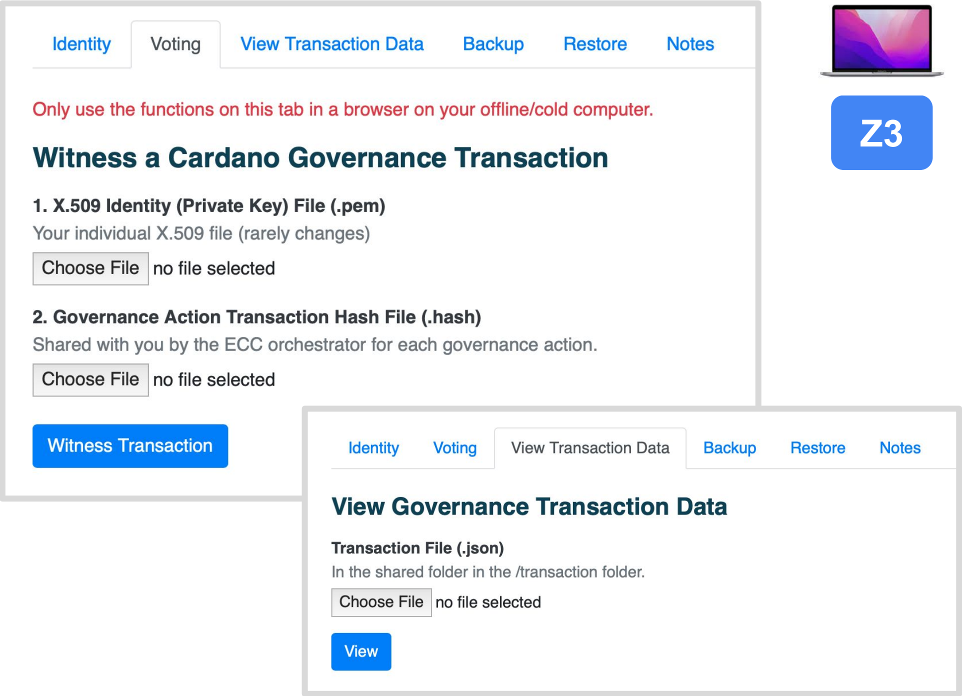
1/ **As instructed by the ECC Voting Orchestrator, copy the mainnet-ecc-vote-[govaction reference].hash file** from the members voting folder on the CICC-ECC shared drive to your **/ciccecc/voting** folder on your offline computer using your USB-T,

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

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

Z3



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)

no file selected

2. Governance Action Transaction Hash File (.hash)

Shared with you by the ECC orchestrator for each governance action.

no file selected

View Governance Transaction Data

Transaction File (.json)

In the shared folder in the /transaction folder.

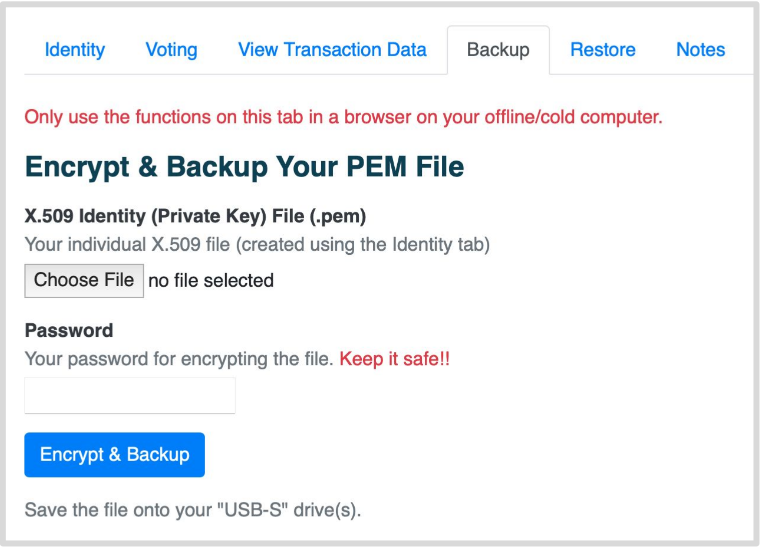
no file selected

! **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 ECC App Backup tab to encrypt your keys



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)

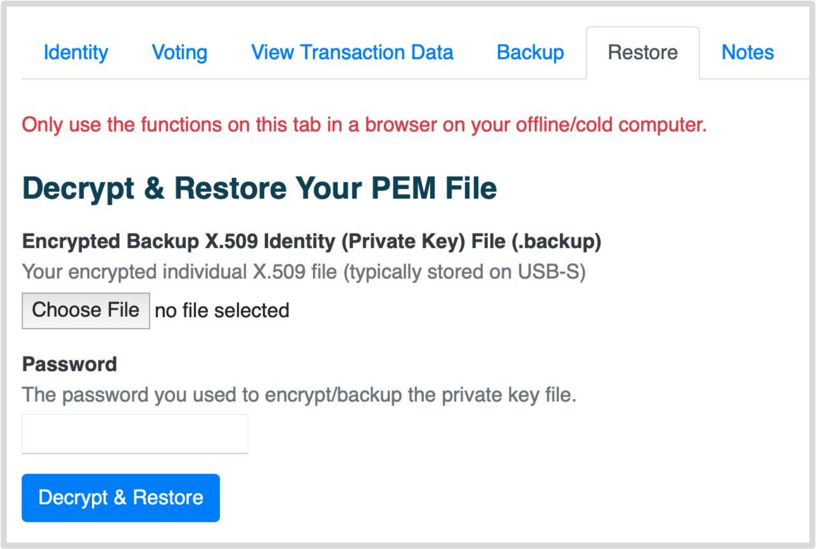
Your individual X.509 file (created using the Identity tab)

Password

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

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

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



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)

Password

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

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
```

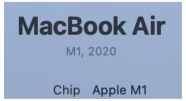
```
sudo cp -r util/openssl/ /usr/local/Cellar/openssl@3/3.3.1
```

```
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.



MacBook Air

M1, 2020

Chip Apple M1

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 = Voter
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
```

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
```

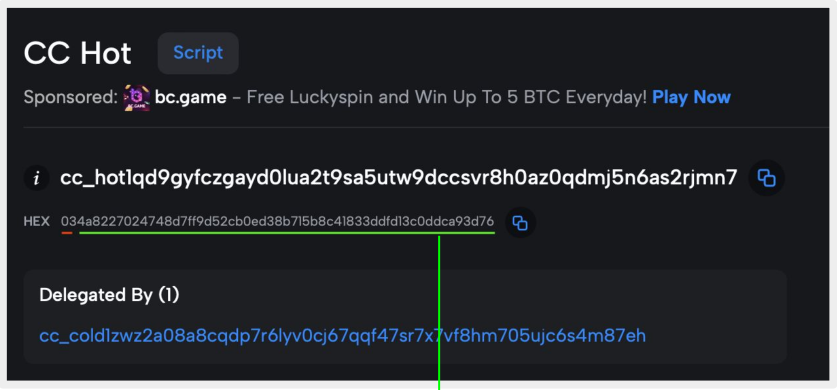
!

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



CC Hot

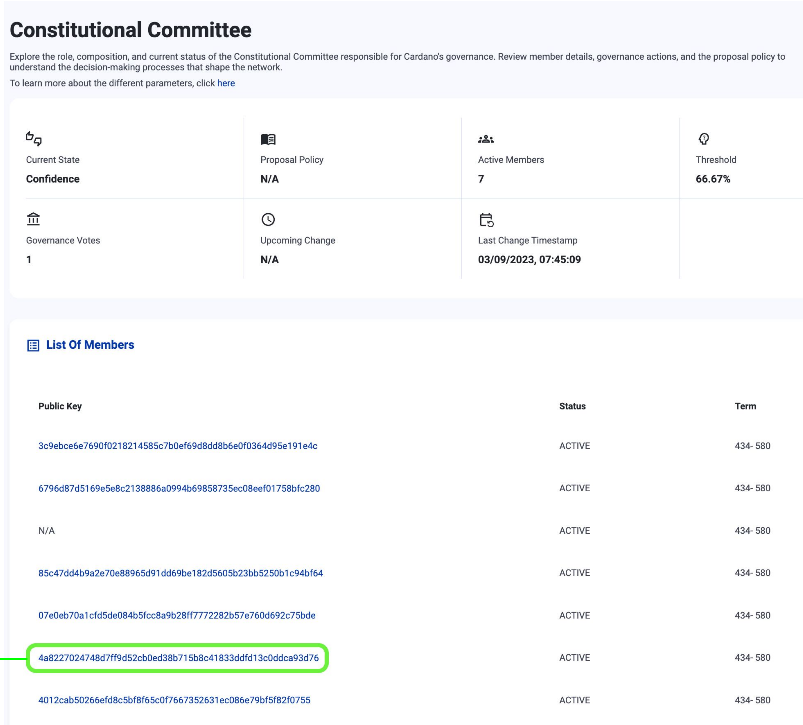
Script

i cc_hot1qd9gyfczgayd0lua2t9sa5utw9dccsvr8h0az0qdmj5n6as2rjmn7

HEX 034a8227024748d7ff9d52cb0ed38b715b8c41833ddfd13c0ddca93d76

Delegated By (1)

cc_cold1zwz2a08a8cqdp7r6lyv0cj67qqf47sr7x7vf8hm705ujc6s4m87eh



Constitutional Committee

Explore the role, composition, and current status of the Constitutional Committee responsible for Cardano's governance. Review member details, governance actions, and the proposal policy to understand the decision-making processes that shape the network.

To learn more about the different parameters, click here

Current State Confidence	Proposal Policy N/A	Active Members 7	Threshold 66.67%
Governance Votes 1	Upcoming Change N/A	Last Change Timestamp 03/09/2023, 07:45:09	

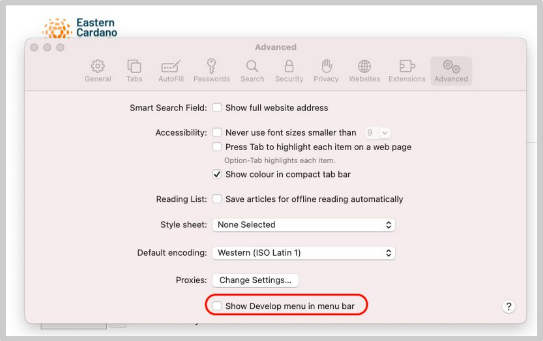
List Of Members

Public Key	Status	Term
3c9ebce6e7690f0218214585c7b0ef69d8dd8b6e0f0364d95e191e4c	ACTIVE	434- 580
6796d87d5169e5e8c2138886a0994b69858735ec08eef01758bfc280	ACTIVE	434- 580
N/A	ACTIVE	434- 580
85c47dd4b9a2e70e88965d91dd69be182d5605b23bb5250b1c94bf64	ACTIVE	434- 580
07e0eb70a1cfd5de084b5fcc8a9b28ff7772282b57e760d692c75bde	ACTIVE	434- 580
4a8227024748d7ff9d52cb0ed38b715b8c41833ddfd13c0ddca93d76	ACTIVE	434- 580
4012cab50266efd8c5bf8f65c0f7667352631ec086e79bf5f82f0755	ACTIVE	434- 580

A6 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

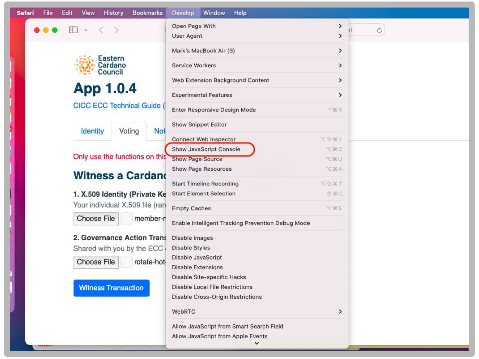
Style sheet: None Selected

Default encoding: Western (ISO Latin 1)

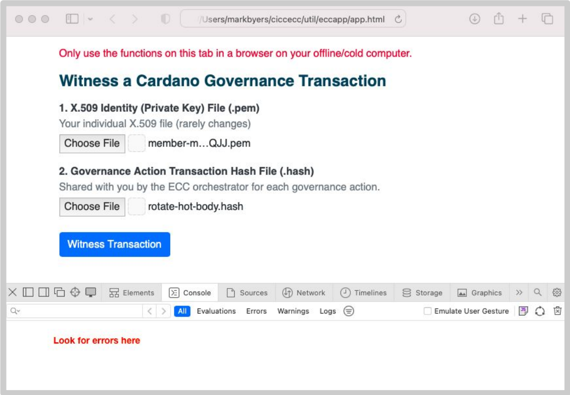
Proxies: Change Settings...

□ Show Develop menu in menu bar

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


Safari
File
Edit
View
History
Bookmarks
Develop
Window
Help
Open Page With
User Agent
Mark's MacBook Air (3)
Service Workers
Web Extension Background Content
Experimental Features
Enter Responsive Design Mode ^⌘R
Show Snippet Editor
Connect Web Inspector ⌥⇧⌘I
Show JavaScript Console ⌥⌘C
Show Page Source ⌥⌘U
Show Page Resources ⌥⌘A
Start Timeline Recording ⌥⇧⌘T
Start Element Selection ⇧⌘C
Empty Caches ⌥⌘E
Enable Intelligent Tracking Prevention Debug Mode
Disable Images
Disable Styles
Disable JavaScript
Disable Extensions
Disable Site-specific Hacks
Disable Local File Restrictions
Disable Cross-Origin Restrictions
WebRTC
Allow JavaScript from Smart Search Field
Allow JavaScript from Apple Events
Eastern
Cardano
Council
App 1.0.4
CICC ECC Technical Guide (
Identity
Voting
Not
Only use the functions on this
Witness a Cardano
1. X.509 Identity (Private Ke
Your individual X.509 file (rar
Choose File
member-r
2. Governance Action Trans
Shared with you by the ECC
Choose File
rotate-hot
Witness Transaction

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)

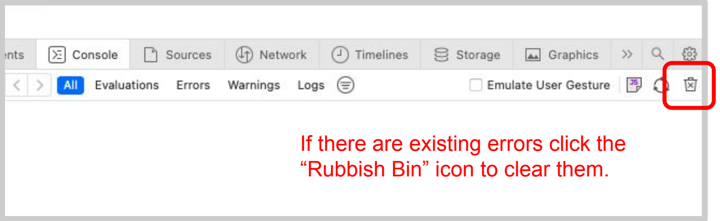
Shared with you by the ECC orchestrator for each governance action.

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.