Agora Voting

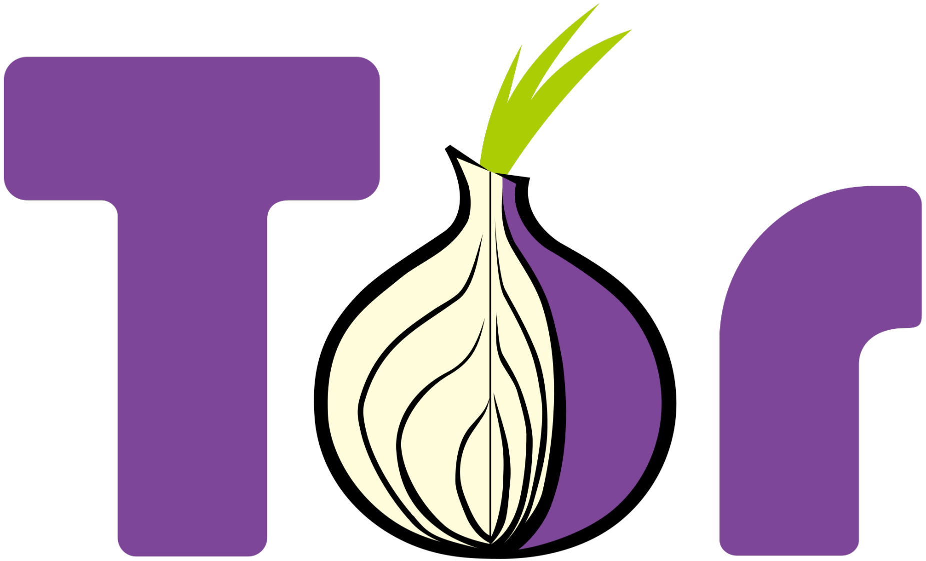
e-voting for skeptics

Eduardo Robles Elvira

https://agoravoting.com

“when we lose privacy we lose liberty itself”

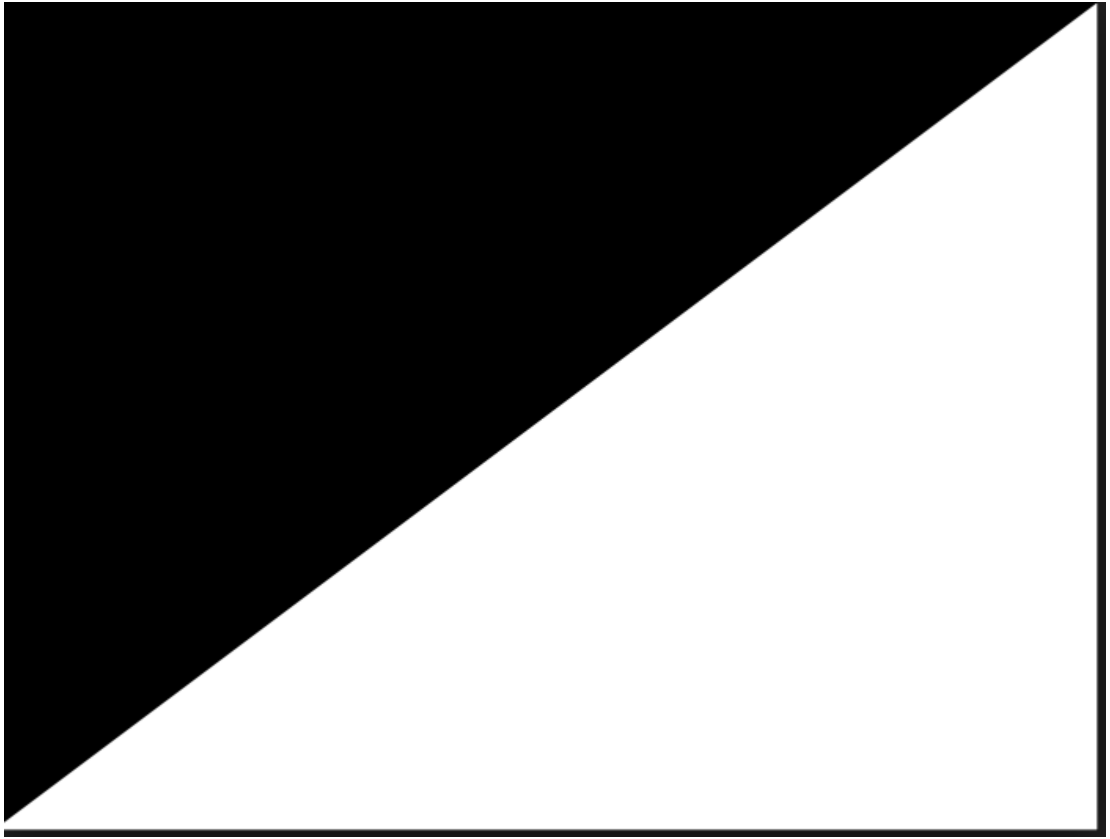
J. Appelbaum, Citizen Four



important tech for preserving privacy via anonimity

technology vs. procedure

Agora Voting



security vs sec. measures

asymmetric resources

is it safe to use? how?
depends on the case

No fooling, Reality:
people need and use it. that’s why it’s important

e-voting?

rewind

we are in the same page

Agora Voting

e-voting: what’s so hard?

Privacy vs. Results

Ben Adida

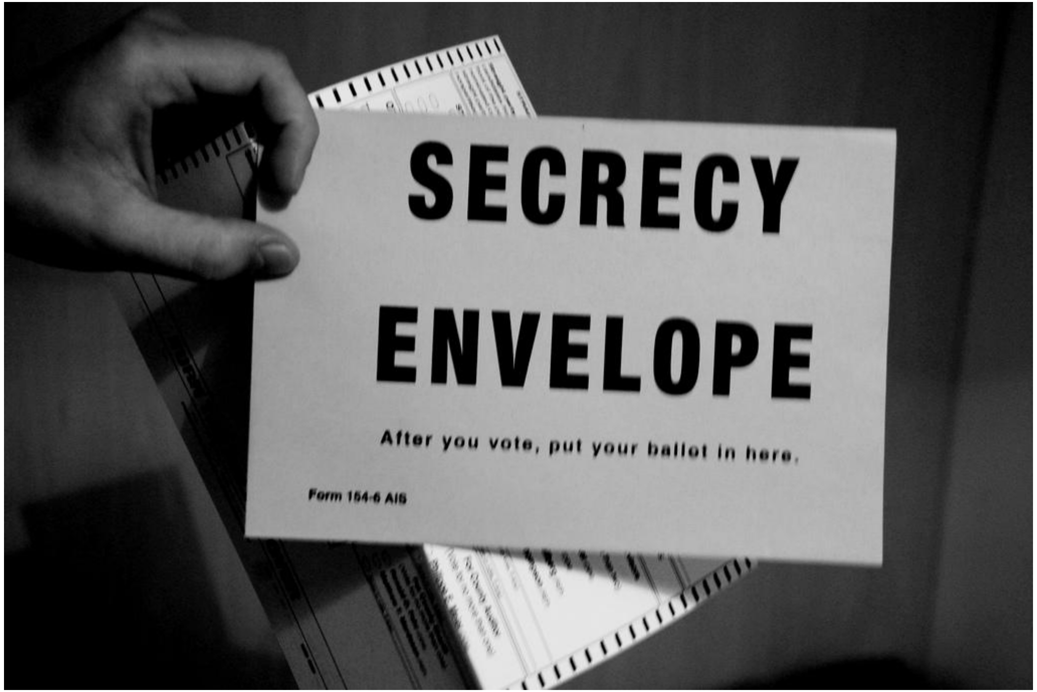
Agora Voting

History

5 years

Technology

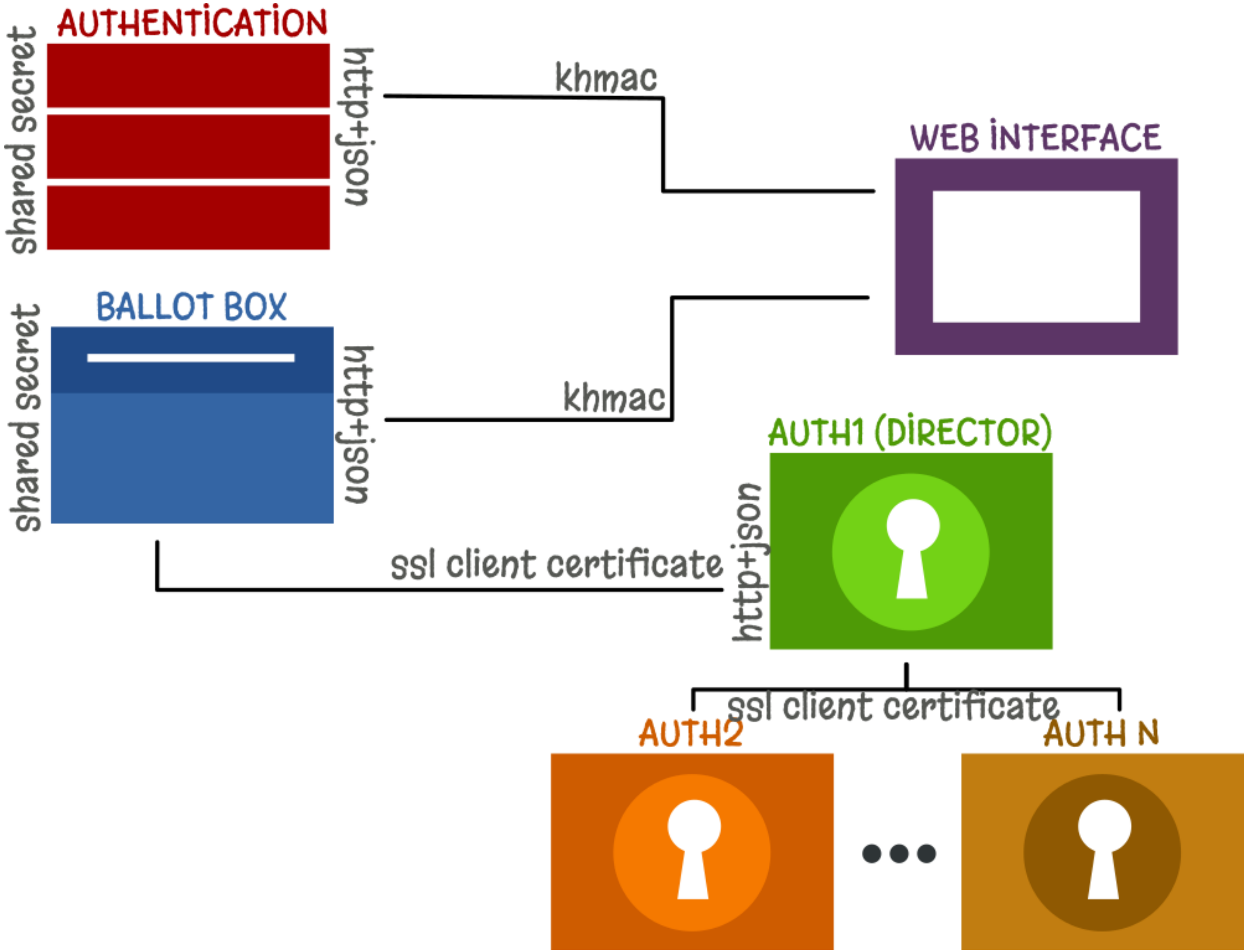
flexible and security focused e-voting


SECRECY
ENVELOPE
After you vote, put your ballot in here.
Form 154-6 AIS

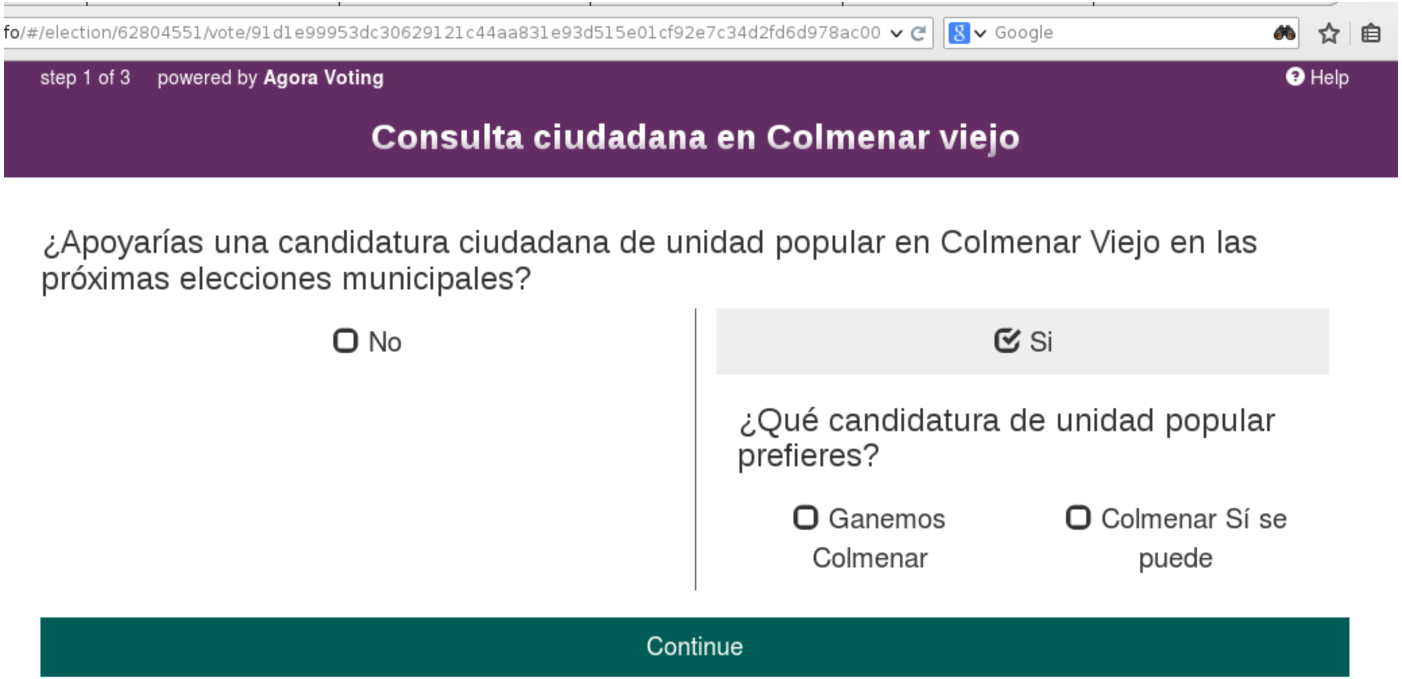
Flexible

voting systems, auth methods, layouts, extra fields, tally options..

Agora Voting



Agora Voting


fo/#/election/62804551/vote/91d1e99953dc30629121c44aa831e93d515e01cf92e7c34d2fd6d978ac00
Google

step 1 of 3 powered by **Agora Voting**

Consulta ciudadana en Colmenar viejo

¿Apoyarías una candidatura ciudadana de unidad popular en Colmenar Viejo en las próximas elecciones municipales?

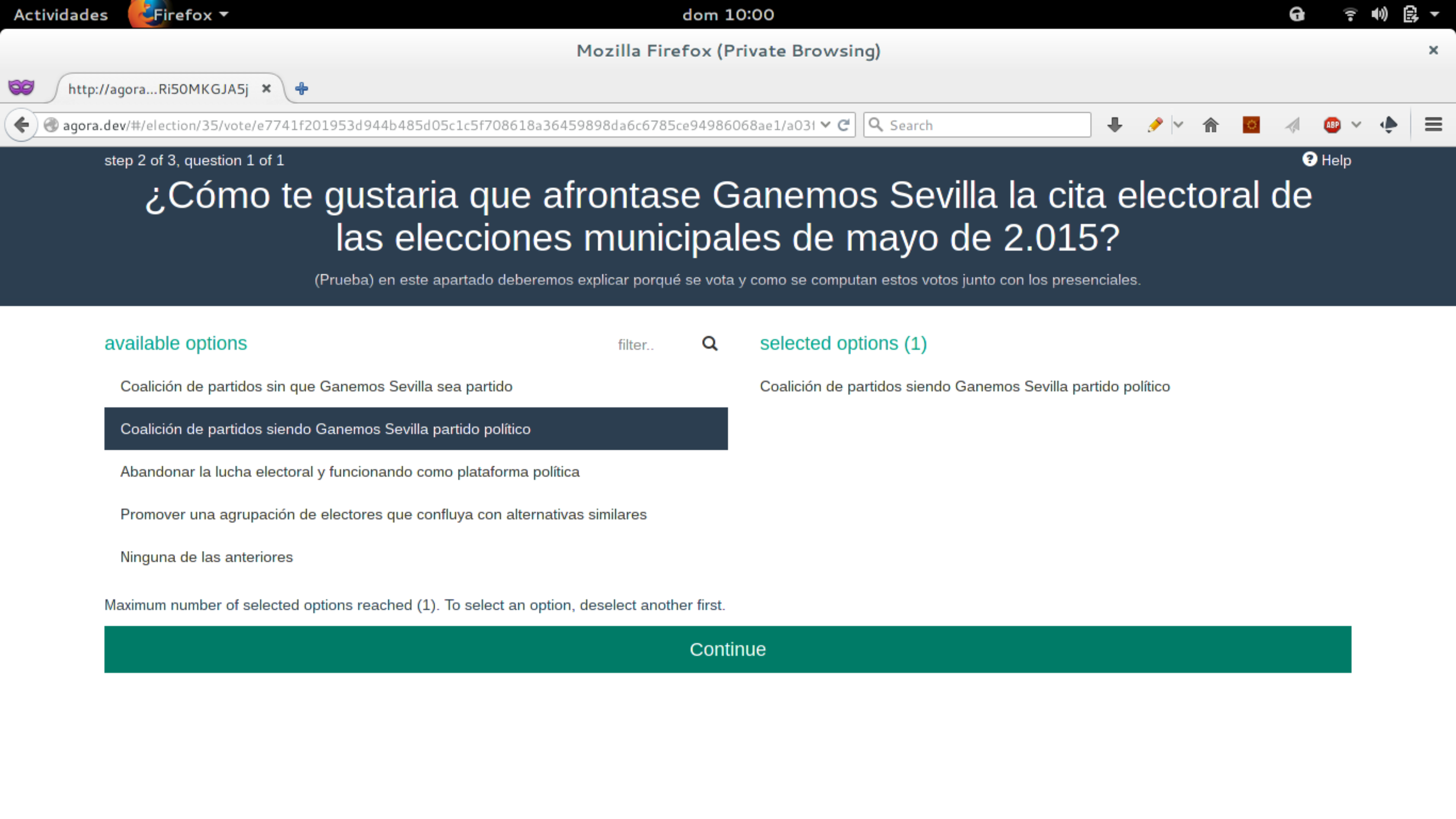
□ No

☑ Si

¿Qué candidatura de unidad popular prefieres?

□ Ganemos Colmenar

□ Colmenar Sí se puede


Actividades
Firefox
dom 10:00
Mozilla Firefox (Private Browsing)
http://agora...Ri50MKGJA5j
agora.dev/#/election/35/vote/e7741f201953d944b485d05c1c5f708618a36459898da6c6785ce94986068ae1/a03
Search
Help
filter..
Continue

step 2 of 3, question 1 of 1

¿Cómo te gustaria que afrontase Ganemos Sevilla la cita electoral de las elecciones municipales de mayo de 2.015?

(Prueba) en este apartado deberemos explicar porqué se vota y como se computan estos votos junto con los presenciales.

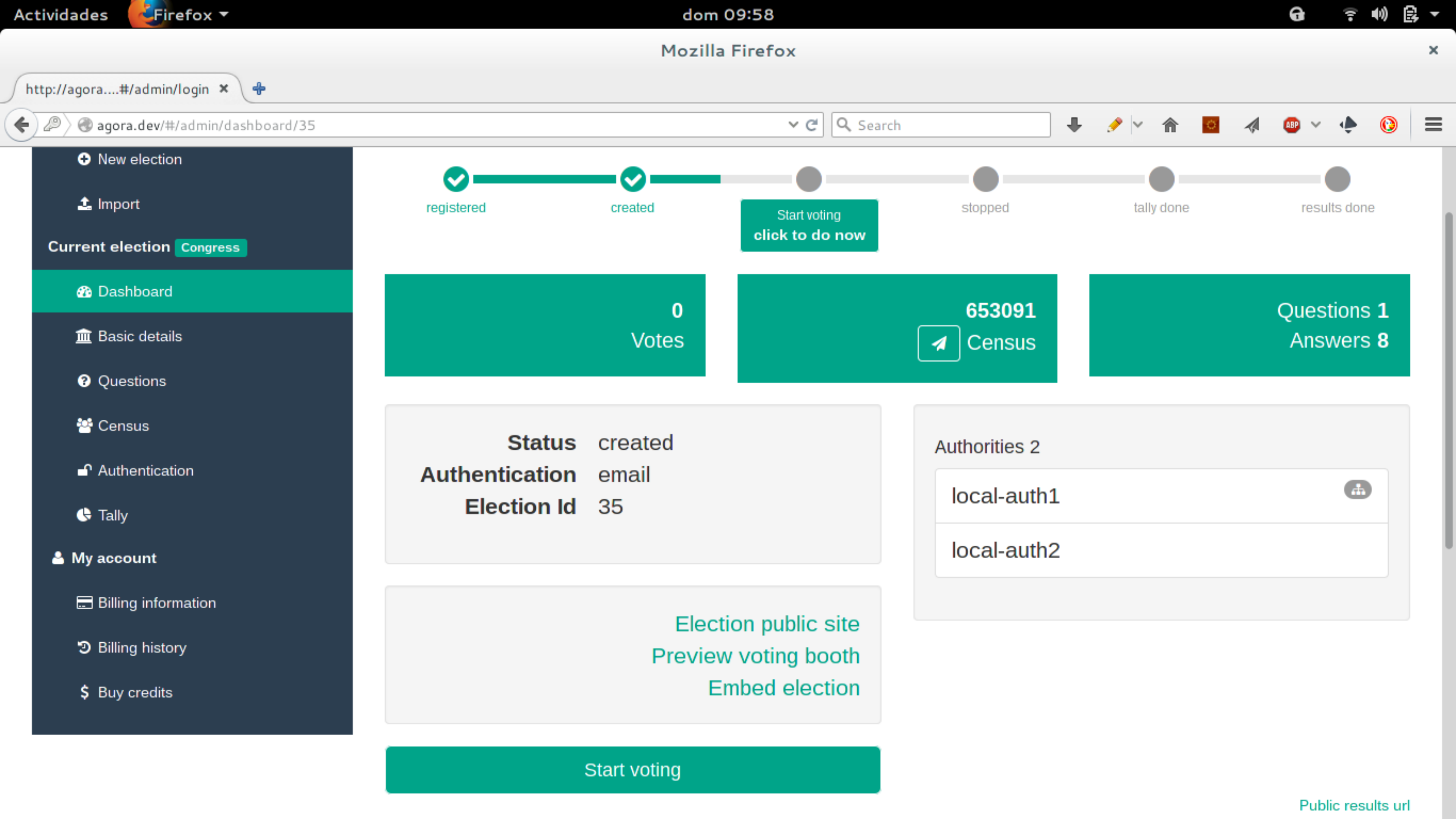
available options

- Coalición de partidos sin que Ganemos Sevilla sea partido
- Coalición de partidos siendo Ganemos Sevilla partido político
- Abandonar la lucha electoral y funcionando como plataforma política
- Promover una agrupación de electores que confluya con alternativas similares
- Ninguna de las anteriores

selected options (1)

- Coalición de partidos siendo Ganemos Sevilla partido político

Maximum number of selected options reached (1). To select an option, deselect another first.



Status created
Authentication email
Election Id 35

Authorities 2

local-auth1

local-auth2

Security focused

End-to-end verifiable

- Cast-as-intended
- Recorded-as-cast
- Counted-as-recorded

Agora Voting

Agora Voting

Original vote => Coded vote => Encrypted vote (secret)

Option A

1

```
“alpha:“”
4258953182677722371453880409268749051389633699899139097103333
5609799611441877064526136245284657244122497804586518859294565
1877785541874859765385259678770773327674493904355475862323079
8244900422118578808183914623385583455279240358704186547645415
1642574286811110595709606305943585368898322670544410819455389
3898313678099587301832995949891300765385109456876356636830982
9621063361936513208912074536638240814203652274729623087308622
6136520543602814223229543379123164699348284892677673309747460
7594270141984485824354753705840465535479006074891726177534767
6919767775061144602085812100027923945031524819751853625225344
3532905","beta":"
2718571143715739082618846267833200710935512879972992311079981
4299160657193983088363684193264062089876081017637156241870149
2268943497906539573392136429364565460810863742148764087225861
7897228416006853032907791888414234031982720295547801494026144
1607806659182188705541155188761329158988352447193849484578841
0646510289308326492003238843218639982122006858127856026180567
3191418496873900482466825780123124890638611193743582990322461
9050149130528774456591475897031746579331975898008525610664867
0807004858815297385565144899958927284019656516001908088614891
8344833521576380014837258317011567351544241696282256254549007
2555258”
```

Authorities

Agora Voting

Encrypted votes => mixnet => clear text votes and anonymous

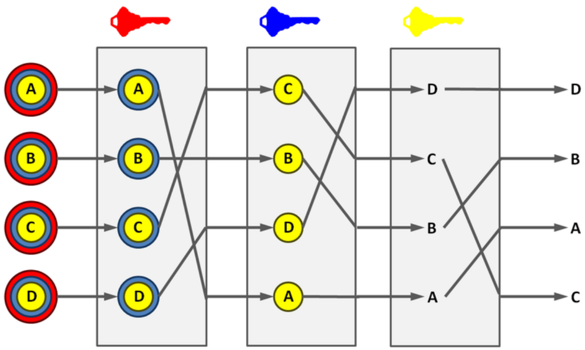
John Vote

“alpha:“”
4258953182677722371453880409268749051389633699
8991390971033335609799611441877064526136245284
6572441224978045865188592945651877785541874859
7653852596787707733276744939043554758623230798
2449004221185788081839146233855834552792403587
0418654764541516425742868111105957096063059435
8536889832267054441081945538938983136780995873
0183299594989130076538510945687635663683098296
2106336193651320891207453663824081420365227472
962308730

Jane Vote

“alpha:“”
4258953182677722371453880409268749051389633699
8991390971033335609799611441877064526136245284
6572441224978045865188592945651877785541874859
7653852596787707733276744939043554758623230798
2449004221185788081839146233855834552792403587
0418654764541516425742868111105957096063059435
8536889832267054441081945538938983136780995873
0183299594989130076538510945687635663683098296
2106336193651320891207453663824081420365227472
962308730

.. and more votes ..



Source: wikipedia.org

option A

option B

option A

option C

option A

option A

option C

.. and more votes ..

Just getting started

Statistically sound auditing

Open hardware

Improve dispute-freeness

Distributed ballot-box

Deterministic builds

Formally verify code (sel4)

Authentication

Used in binding elections

+100k votes in a single election

Software Libre

http://github.com/agoravoting

The Company

professional services

SaaS beta