

Agora Voting

an end to end verifiable system

Eduardo Robles Elvira

<https://nvotes.com>

flexible and security
focused e-voting

Flexible

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

Continue

step 2 of 3, question 1 of 1

Help

¿Cómo te gustaría 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

filter..



selected options (1)

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

Coalición de partidos siendo Ganemos Sevilla partido político

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

Continue

Mozilla Firefox

http://agora....#/admin/login

agora.dev/#/admin/dashboard/35

Search

New election

Import

Current election **Congress**

Dashboard

Basic details

Questions

Census

Authentication

Tally

My account

Billing information

Billing history

Buy credits

registered

created

Start voting
click to do now

stopped

tally done

results done

0
Votes

653091
Census

Questions 1
Answers 8

Status created

Authentication email

Election Id 35

Authorities 2

local-auth1

local-auth2

Election public site

Preview voting booth

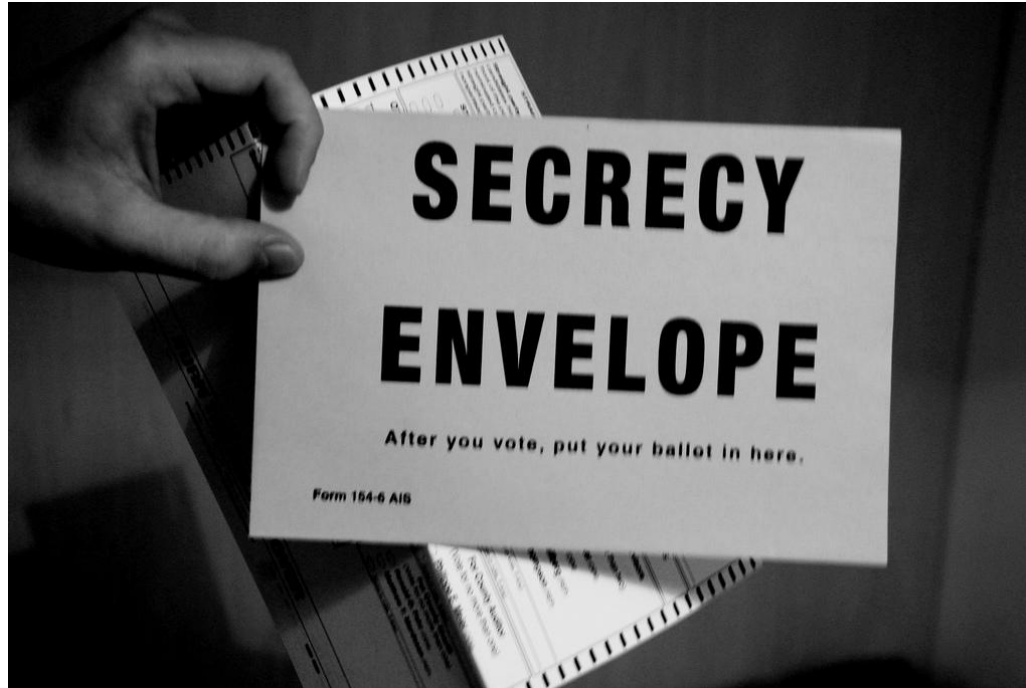
Embed election

Start voting

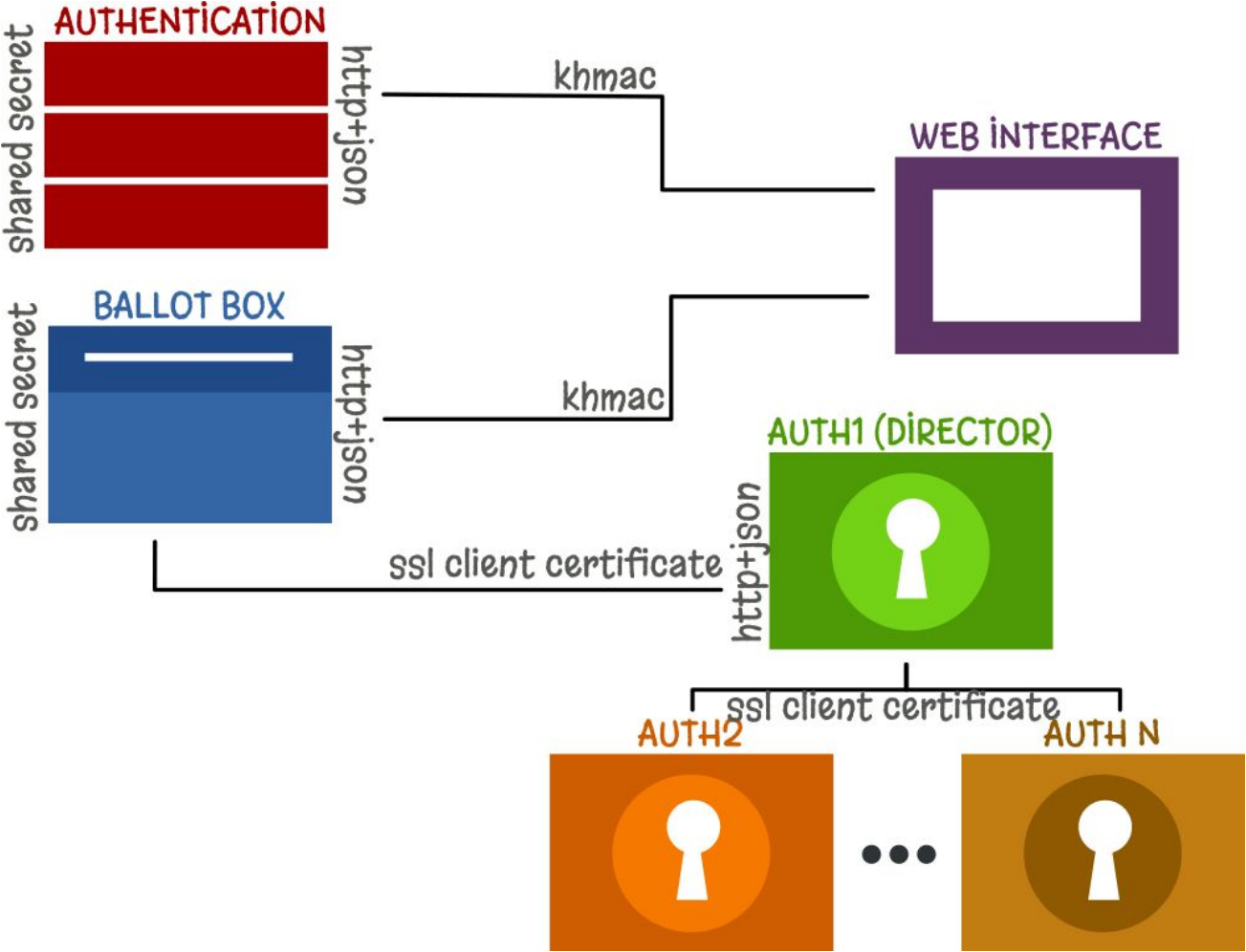
Public results url

Security focused

Agora Voting



Agora Voting



End-to-end verifiable

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

Agora Voting

Original vote	=>	Coded vote	=>	Encrypted vote (secret)
Option A		1		"alpha:""42589531826777223714538804092687490513896336998991390971033335609799611441877064526136245284657244122497804586518859294565187778554187485976538525967877077332767449390435547586232307982449004221185788081839146233855834552792403587041865476454151642574286811110595709606305943585368898322670544410819455389389831367809958730183299594989130076538510945687635663683098296210633619365132089120745366382408142036522747296230873086226136520543602814223229543379123164699348284892677673309747460759427014198448582435475370584046553547900607489172617753476769197677750611446020858121000279239450315248197518536252253443532905","beta":"27185711437157390826188462678332007109355128799729923110799814299160657193983088363684193264062089876081017637156241870149226894349790653957339213642936456546081086374214876408722586178972284160068530329077918884142340319827202955478014940261441607806659182188705541155188761329158988352447193849484578841064651028930832649200323884321863998212200685812785602618056731914184968739004824668257801231248906386111937435829903224619050149130528774456591475897031746579331975898008525610664867080700485881529738556514489995892728401965651600190808861489183448335215763800148372583170115673515442416962822562545490072555258"

Authorities



Agora Voting

Encrypted votes

=>

mixnet

=>

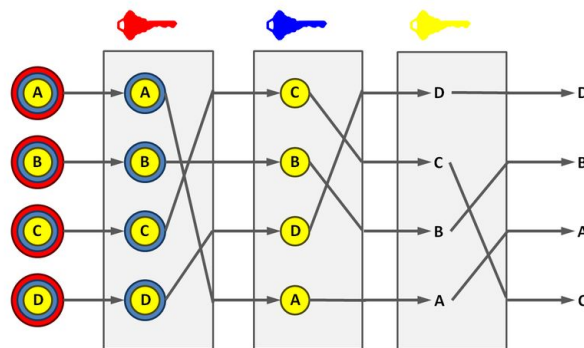
clear text votes and anonymous

John Vote

"alpha:""425895318267772237145388040926874905138
9633699899139097103333560979961144187706452613
6245284657244122497804586518859294565187778554
1874859765385259678770773327674493904355475862
3230798244900422118578808183914623385583455279
2403587041865476454151642574286811110595709606
3059435853688983226705444108194553893898313678
0995873018329959498913007653851094568763566368
3098296210633619365132089120745366382408142036
5227472962308730

Jane Vote

"alpha:""425895318267772237145388040926874905138
9633699899139097103333560979961144187706452613
6245284657244122497804586518859294565187778554
1874859765385259678770773327674493904355475862
3230798244900422118578808183914623385583455279
2403587041865476454151642574286811110595709606
3059435853688983226705444108194553893898313678
0995873018329959498913007653851094568763566368
3098296210633619365132089120745366382408142036
5227472962308730



Source: wikipedia.org

.. and more votes ..

Used in real elections

+100k votes in a single election

Software Libre

<http://github.com/agoravoting>