Scytl

Innovating Democracy

Voting Among Sharks

H2HC Hackers to Hackers Conference

São Paulo, Brasil

22-23 October, 2016

Sandra Guasch
Jesús Chóliz

H2HC

HACKERS TO HACKERS CONFERENCE

Internet voting… ARE YOU SURE?

There are thousands of ways to **do it wrong.**
But there are also ways of **doing it RIGHT!**

About us

Cryptography Researcher

PhD on Electronic Voting

@sandraguasch

Director of Security

+15 years working on Security

@jesuscholiz

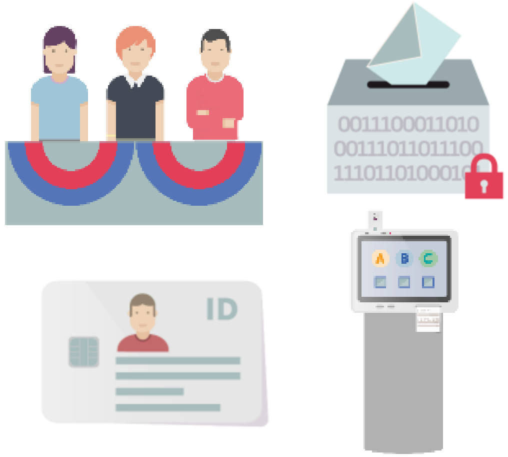
Discussing internet voting for over 6 years

Research & Security

At @SCYTL_SA

Types of electronic voting

Voting **machines**



Online voting **from poll sites**

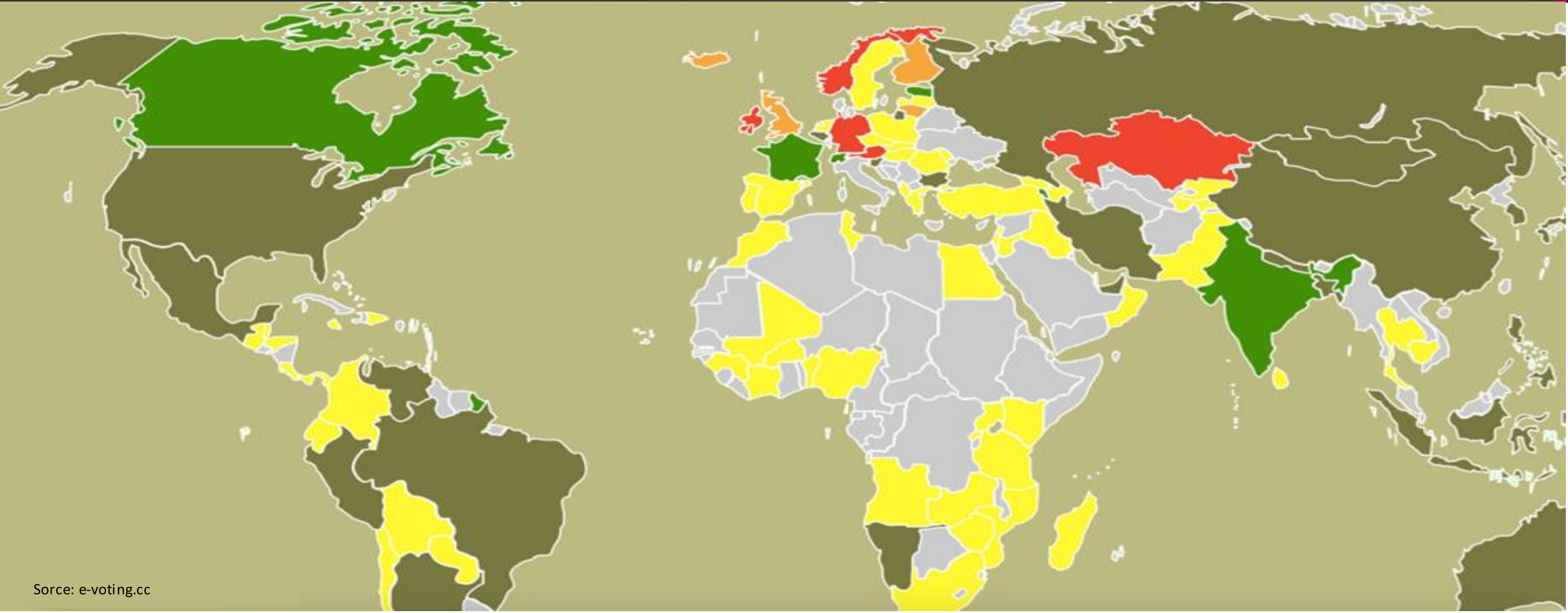
Remote internet voting

Motivation

- Increase **participation**?
- Decrease **cost**?
- Easier for voters with **disabilities**?
- Enabling **hospitalized** or **convalescent** voters?
- Efficiency for citizens living **abroad**?
- Feasible to do elections / consultations more **often**?
- Provide **faster** and more **accurate** results?
- Decrease **queues** in poll sites?

Scytl
Innovating Democracy

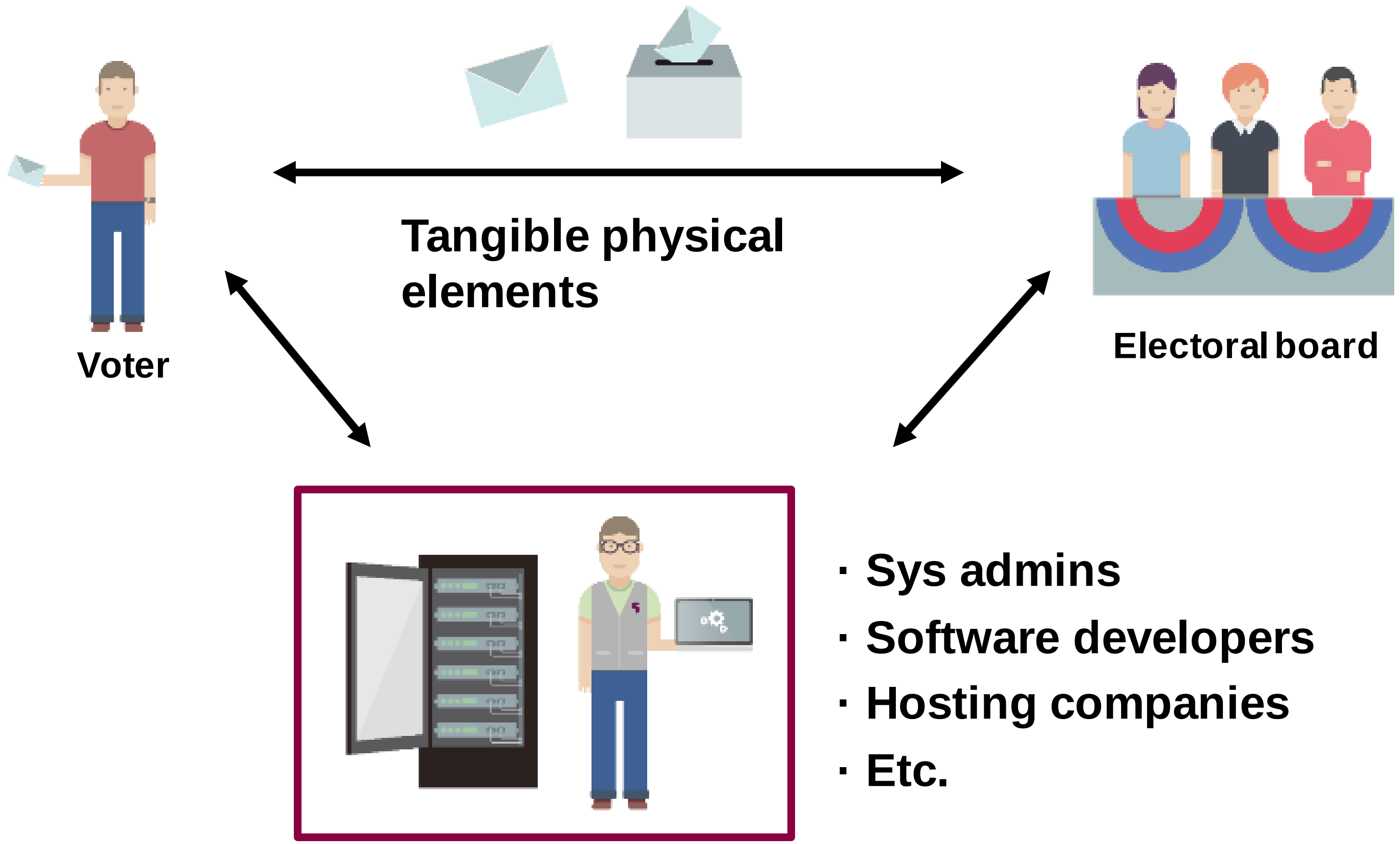
Motivation



Sorce: e-voting.cc

- 🟩 Internet voting (legally binding)
- ▨ Ballot scanners and/or Electronic Voting Machines (legally binding)
- 🟨 Discussing or doing pilots
- 🟧 Discussion concrete plans
- 🟥 Used in the past
- ⬜ No plans already

Changes in the voting paradigm



Tangible physical elements

Voter

Electoral board

- Sys admins
- Software developers
- Hosting companies
- Etc.

New indirect voting relationship that brings new security risks

But… what could go wrong??

PRIVACY

INTEGRITY / TRUST

SECURITY / MALWARE

PRIVATE COMPANIES

VOTER COERCION

HACKING

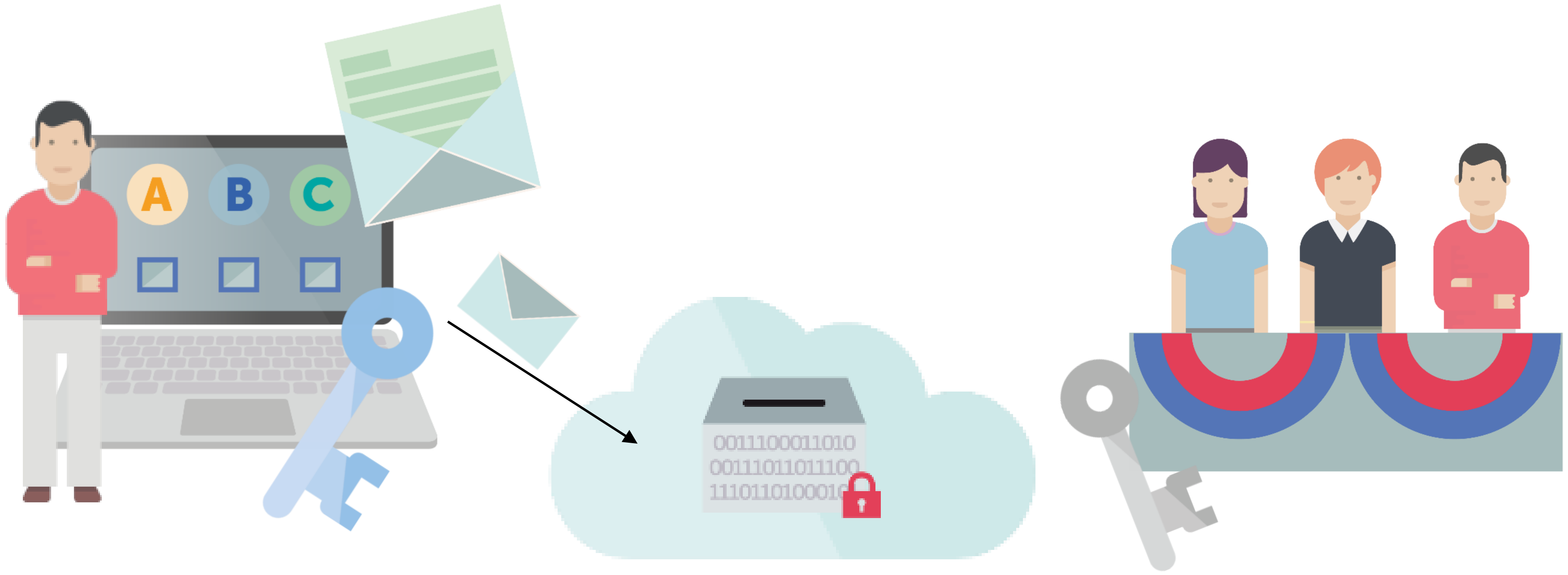
SYSADMINS

Sorce: www.geekculture.com

AD NETWORK GUY
THE NSA
ANOTHER AD NETWORK GUY
AMAZON
ANOTHER NSA GUY
FACEBOOK
pulse
NEWS APPS
MORE AD NETWORK FOLKS!
YAHOO!
TWITTER
GOOGLE GUYS
YOUR ISP
AND DON'T FORGET YOUR SPOUSE CHECKING YOUR HISTORY!

Privacy on the Internet does not exist!!!

End to end encryption

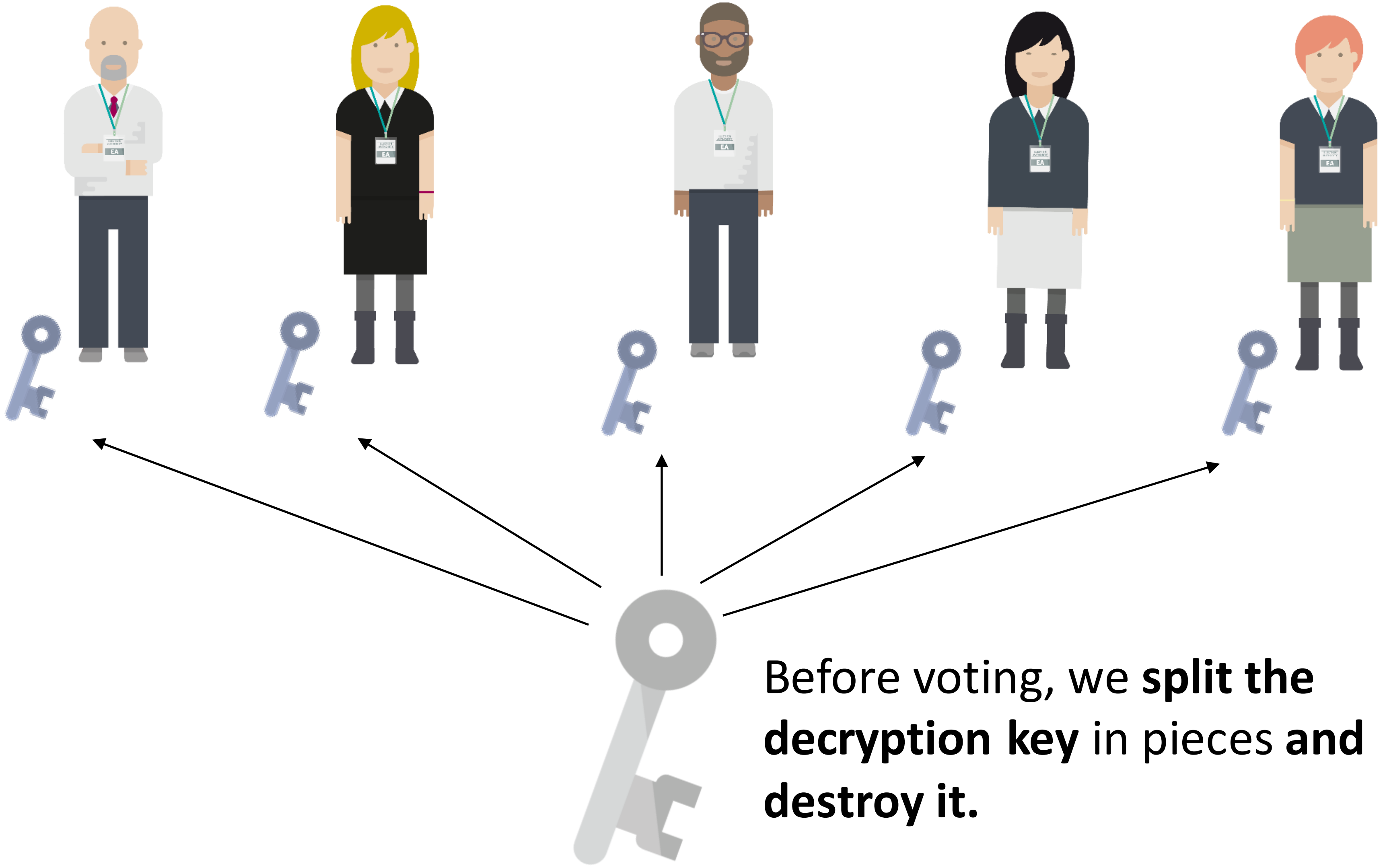


Vote is **encrypted** on the voters computer

End-to-end encryption

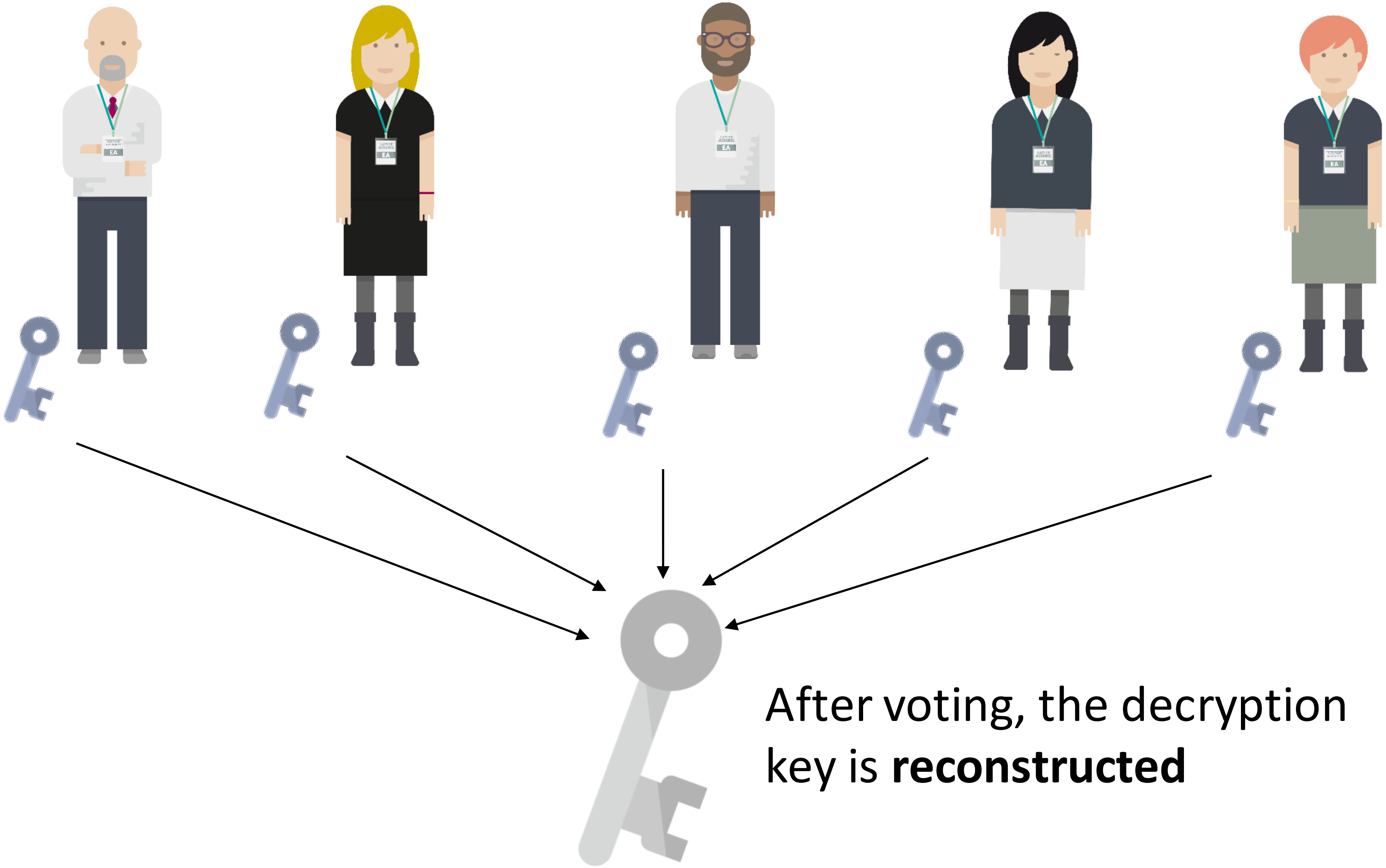
The Electoral Board holds the **decryption key**

Split the trust (I)



Before voting, we **split the decryption key** in pieces **and destroy it.**

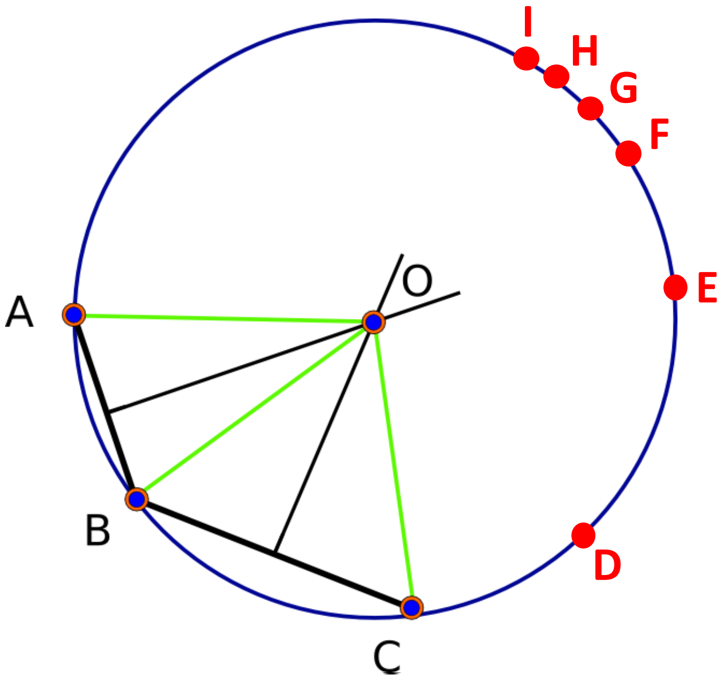
Split the trust (II)

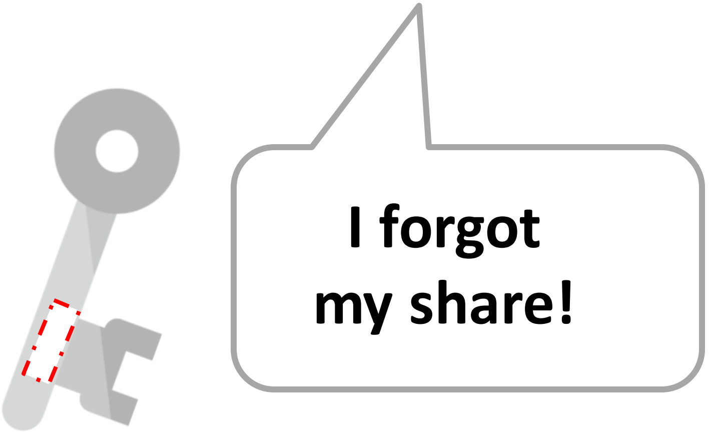


After voting, the decryption key is **reconstructed**

Threshold Secret sharing

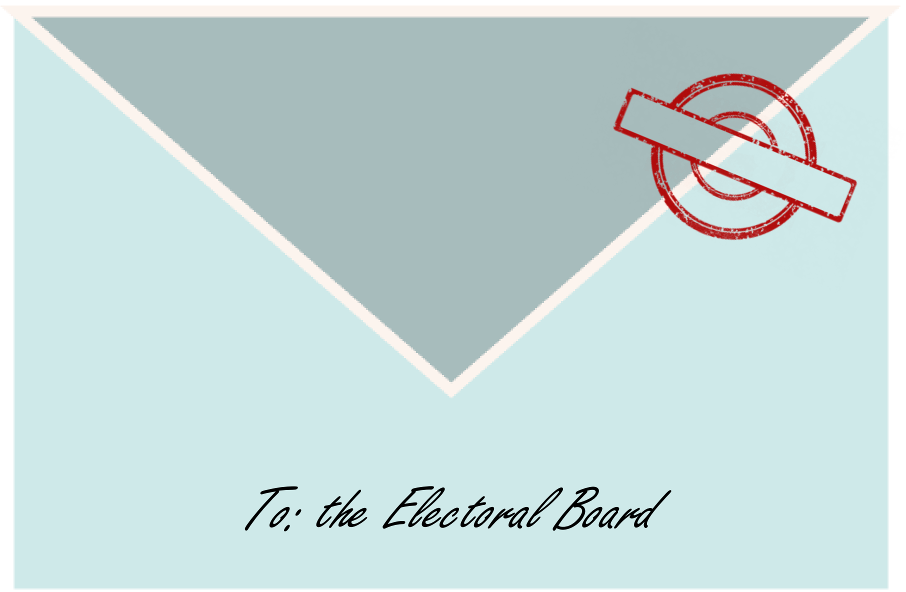
How many points of a circle are needed to find the center?



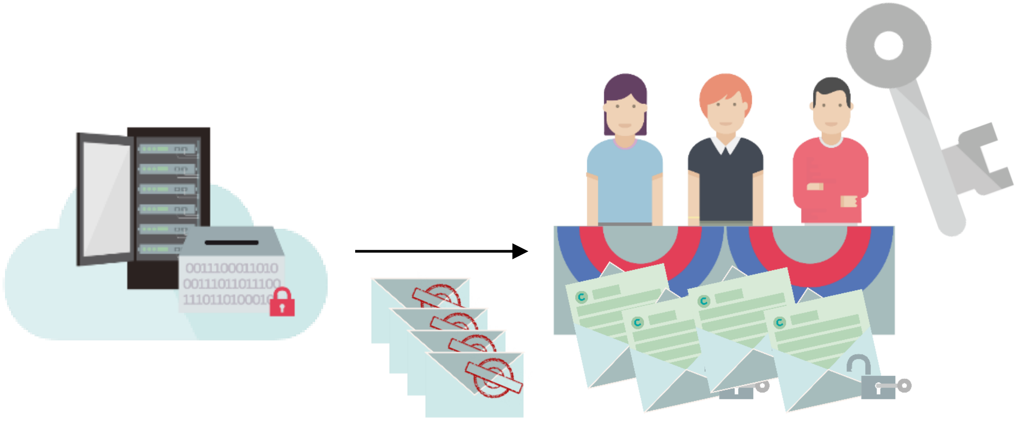


But then…
the electoral board
will see my vote, right?

Your vote contains your data

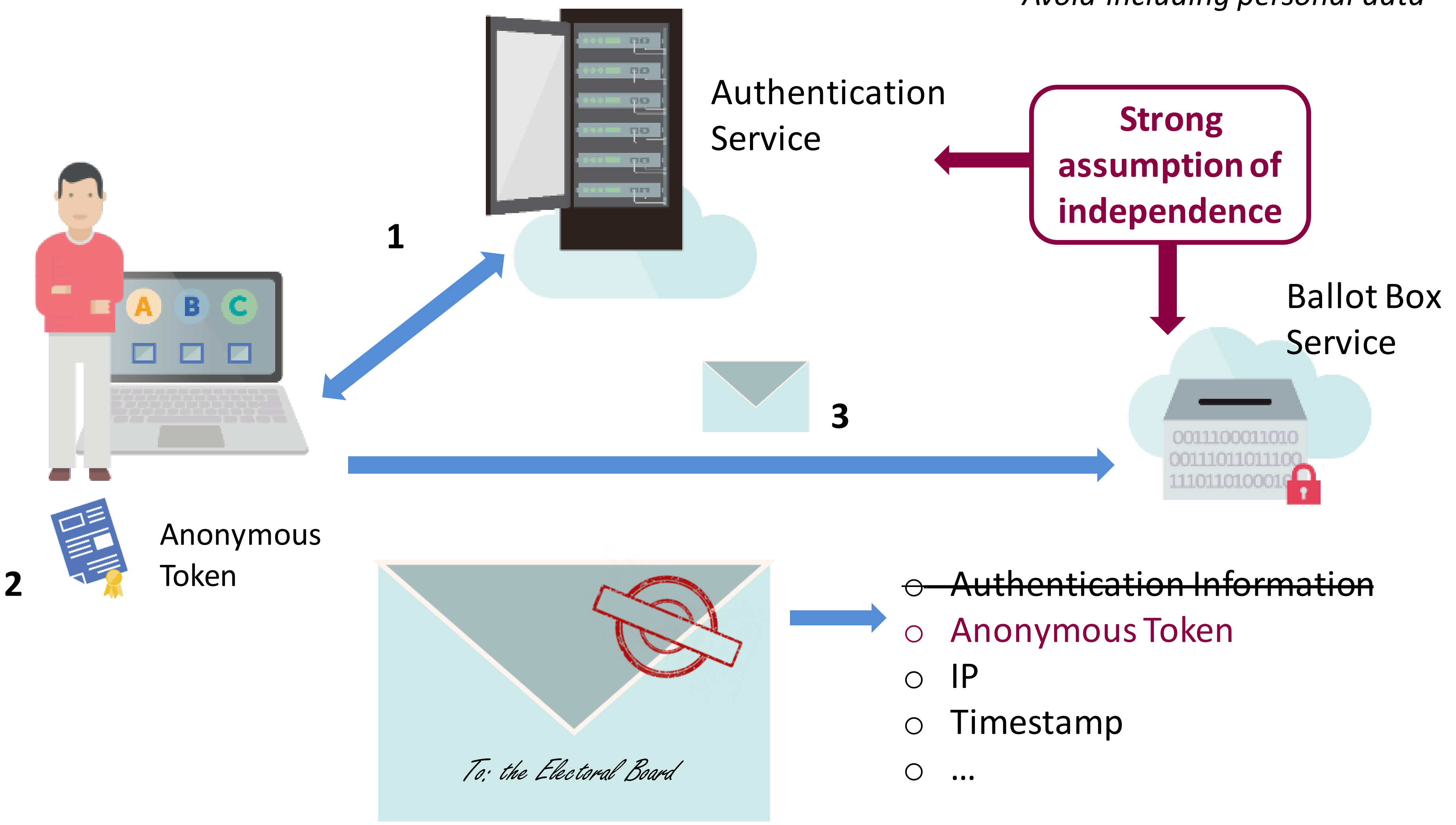


- Authentication Information
- IP
- Timestamp
- …



(1) Two agencies model

Avoid including personal data



Authentication Service

Strong assumption of independence

Ballot Box Service

1

2

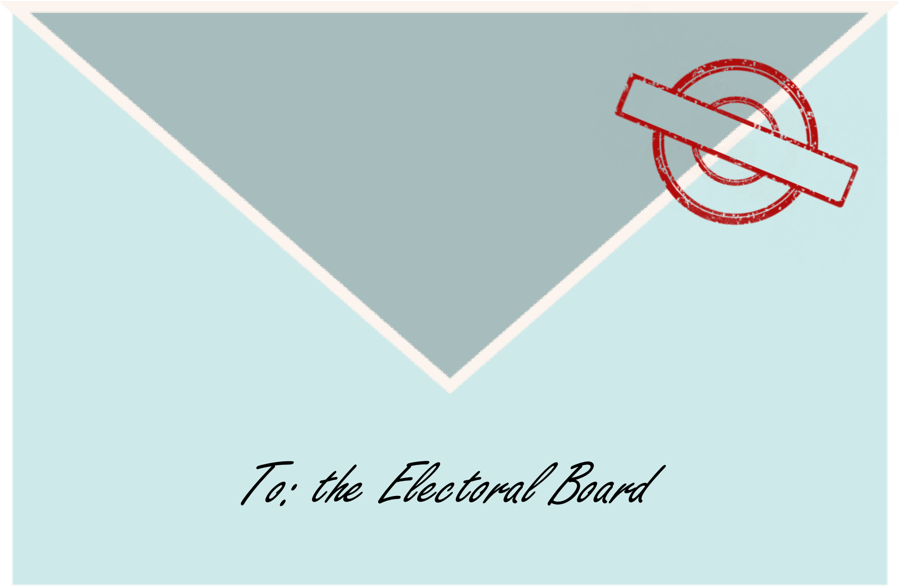
3

Anonymous Token

- ~~Authentication Information~~
- Anonymous Token
- IP
- Timestamp
- …

(2) Mix-net

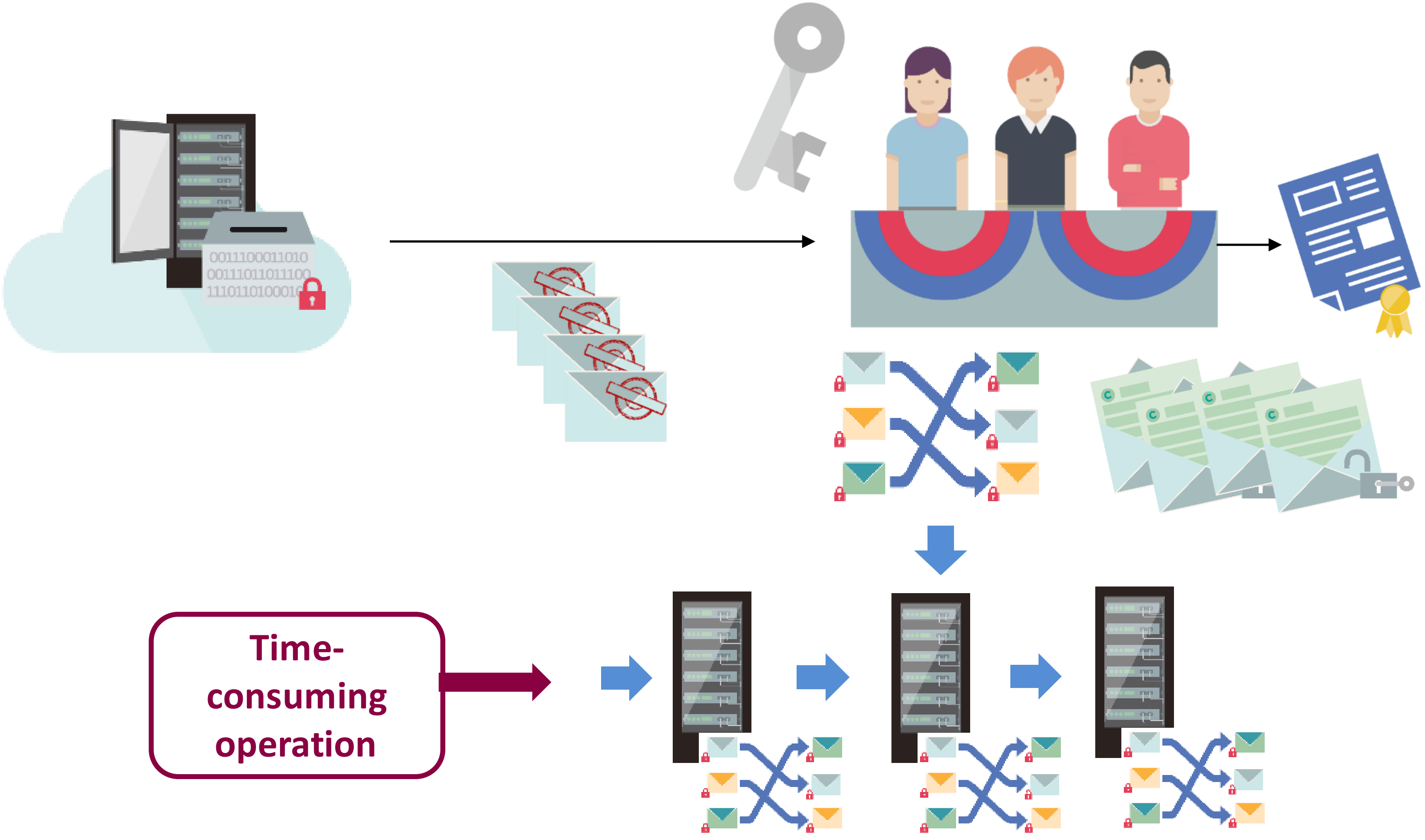
Remove information and anonymize the votes



- Authentication Information
- IP
- Timestamp
- …

(2) Mix-net

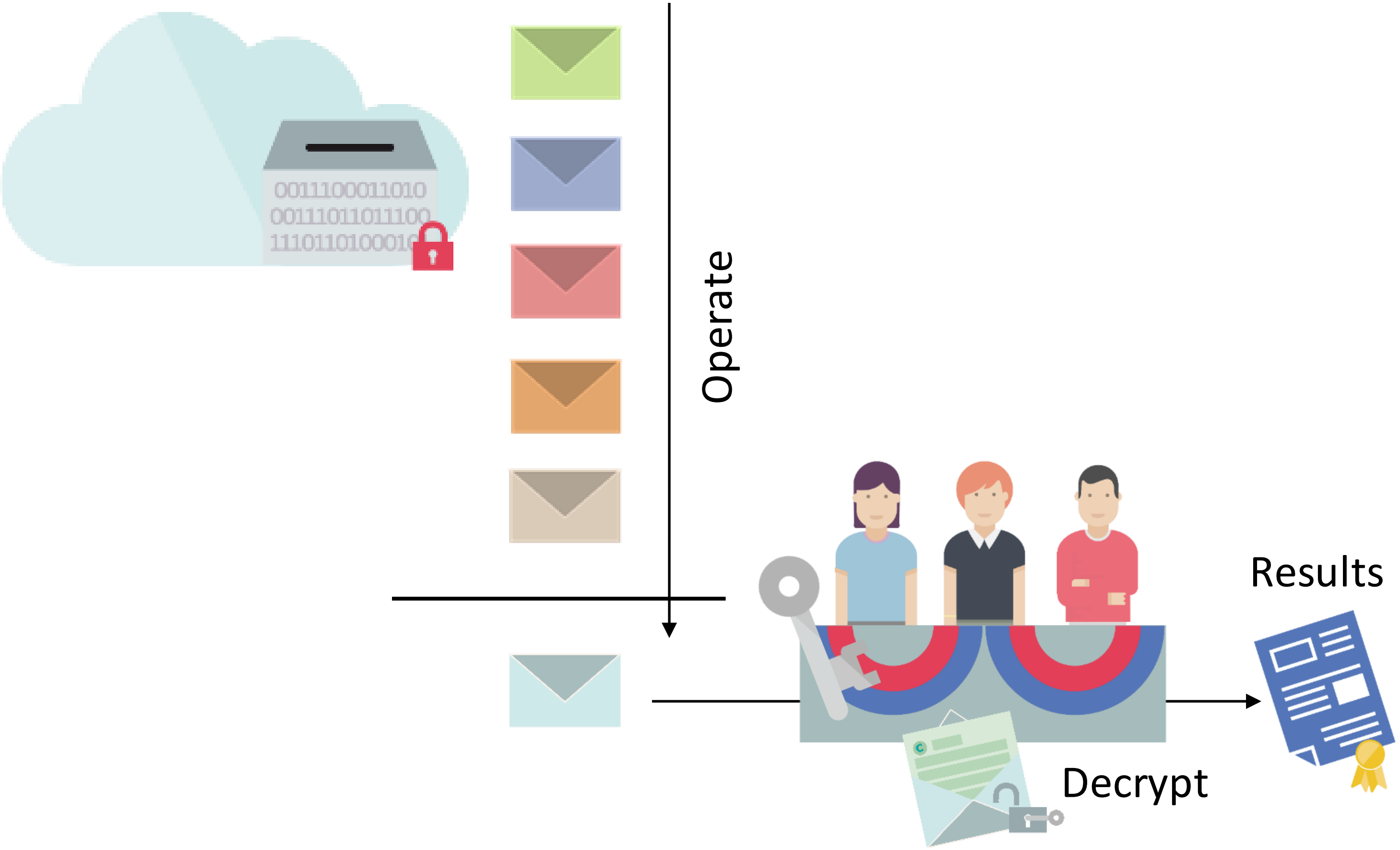
Remove information and anonymize the votes



Time-consuming operation

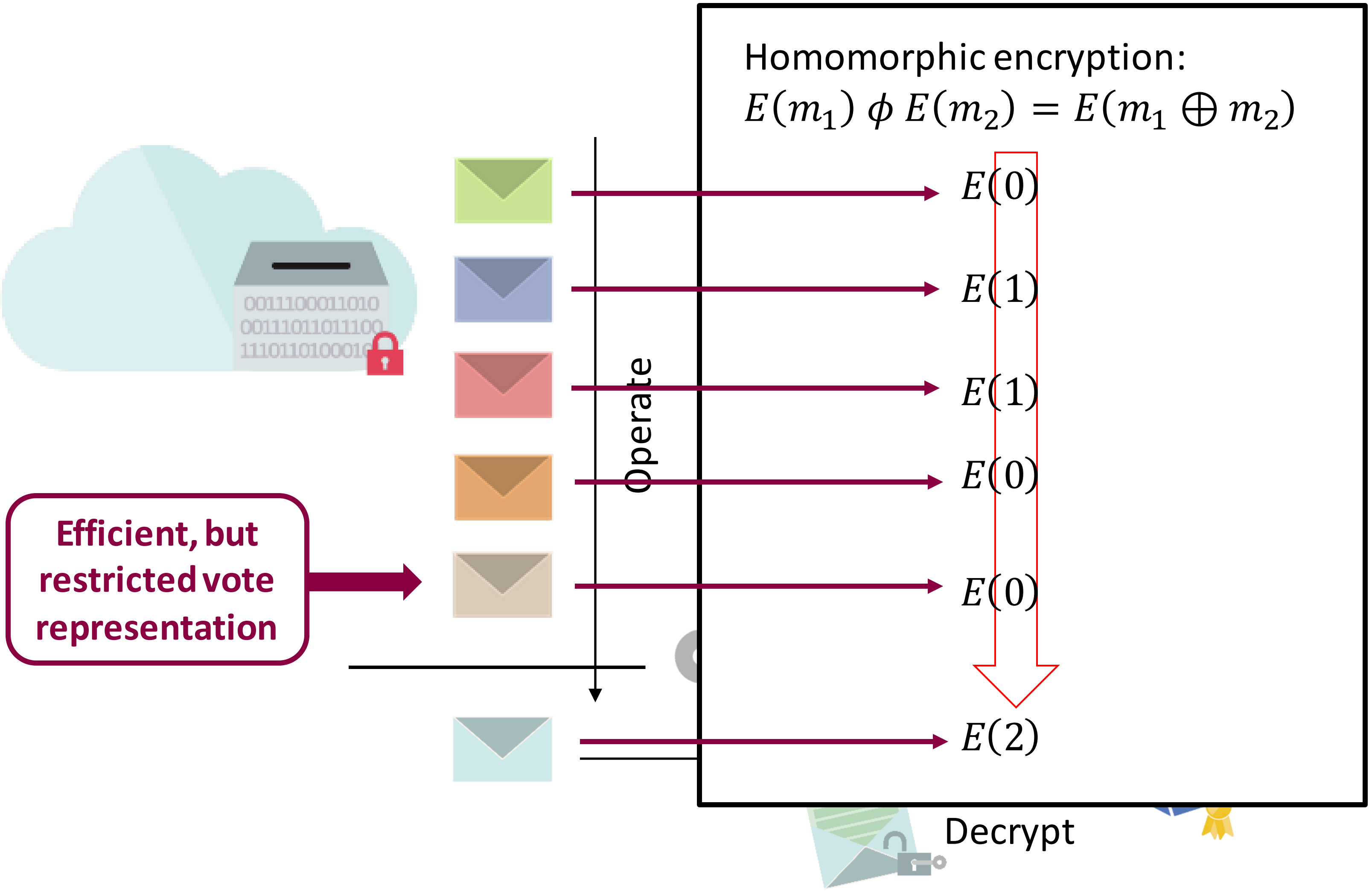
(3) Homomorphic tally

Don't decrypt individual votes



(3) Homomorphic tally

Don’t decrypt individual votes



Homomorphic encryption:

$$E(m_1)\ \phi\ E(m_2) = E(m_1 \oplus m_2)$$

Efficient, but restricted vote representation

Summary of privacy methods

Strategy	PROs	CONs
Two agencies model	Easy to implement	Strong trust assumptions
Mix-net	Lower trust assumptions, flexible electoral models	Time-consuming
Homomorphic tally	Efficient	Restricted electoral models

How can I be sure that my vote has been counted?

Auditability in traditional elections

We can see our **votes in the ballot box**

We can check how the **Electoral Board counts**

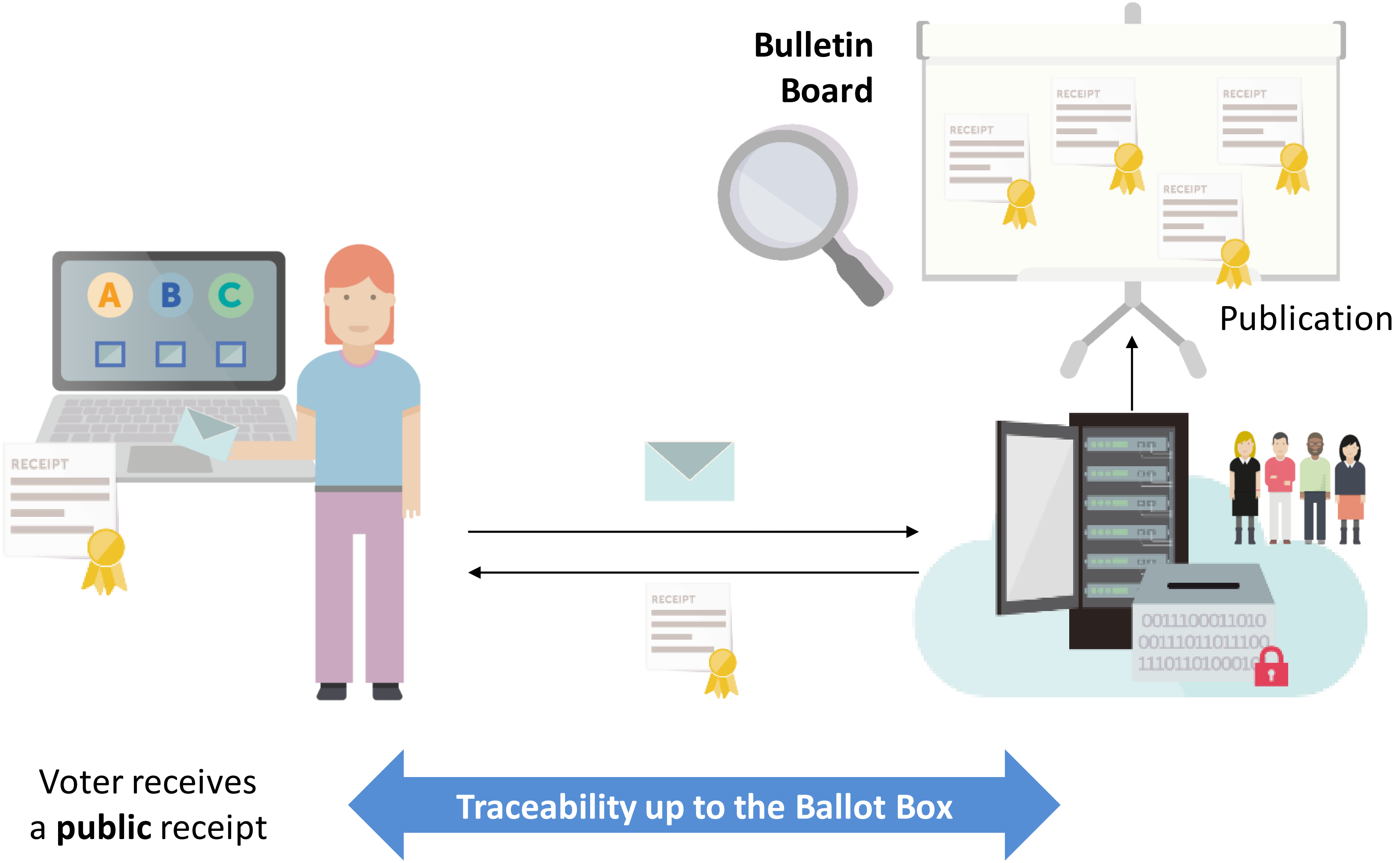
Auditability of voting machines in Brazil

Trust based on **source code** audits, **parallel voting test** with randomly selected machines, **controlled environment**

Lei nº 10.826, de 22/12/2003
O comércio de armas de fogo e munição deve ser proibido no Brasil?
1 - SIM
2 - NÃO
JUSTIÇA ELEITORAL
1
2
3
4
5
6
7
8
9
0
BRANCO
CORRIGE
CONFIRMA

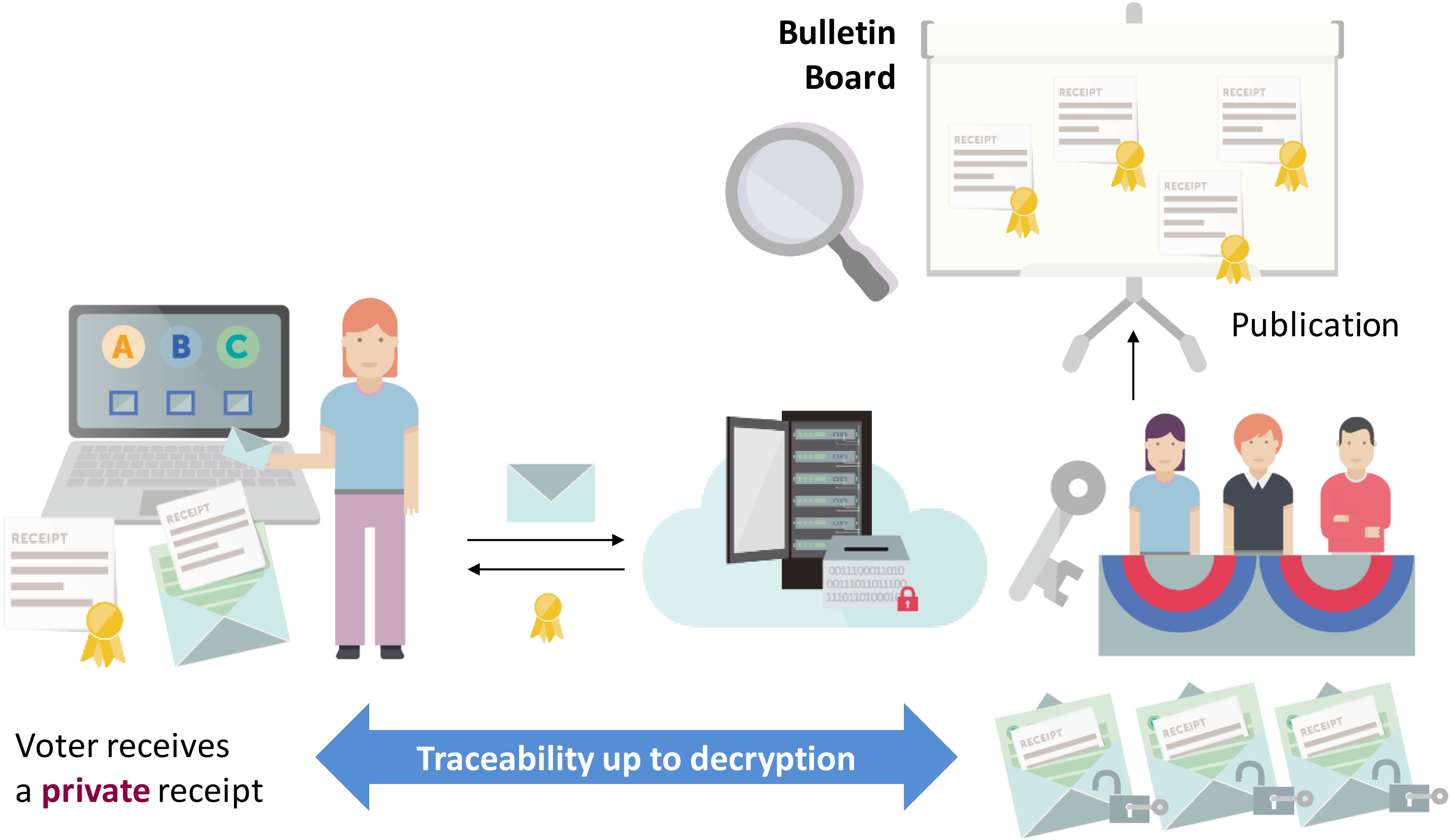
Not enough for Internet Voting

(1) Tracing up to the Ballot Box



Voter receives
a **public** receipt

(2) Tracing up to decryption



Bulletin Board

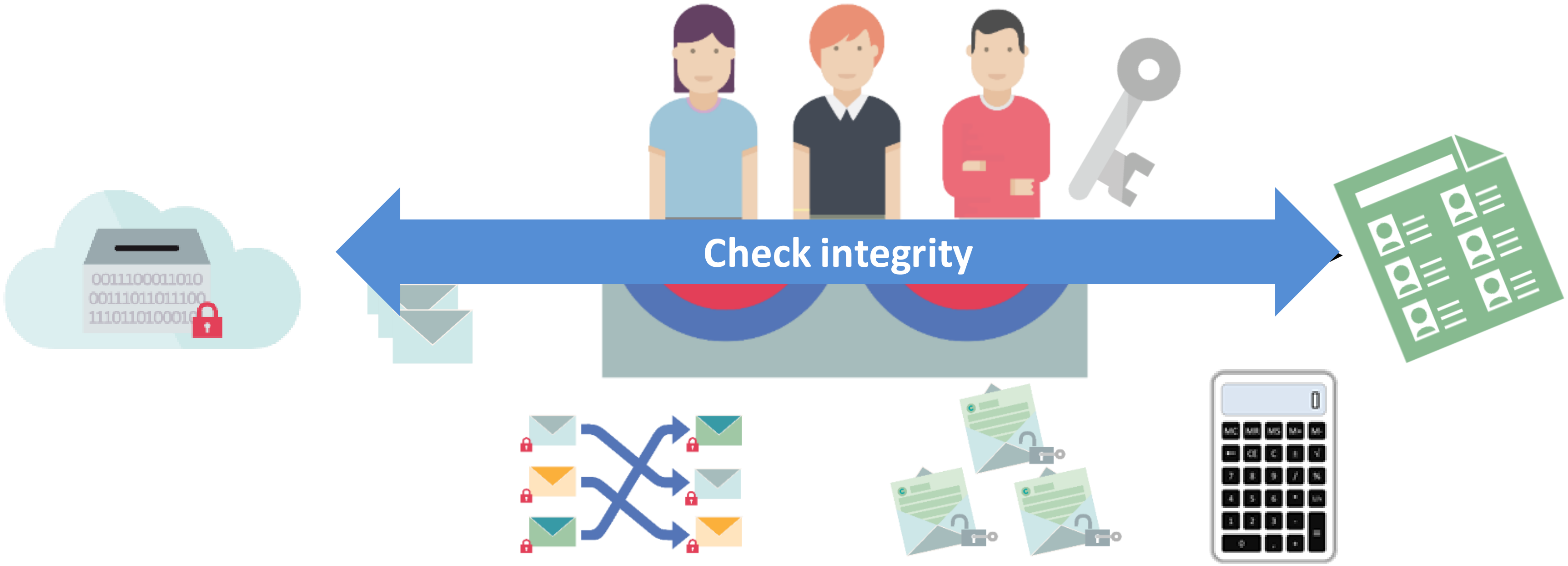
Publication

Voter receives a **private** receipt

Traceability up to decryption

(3) Verifying the counting process

The Electoral Board **does more than in traditional elections**



Check integrity

Check that votes have not been **modified / added / deleted**

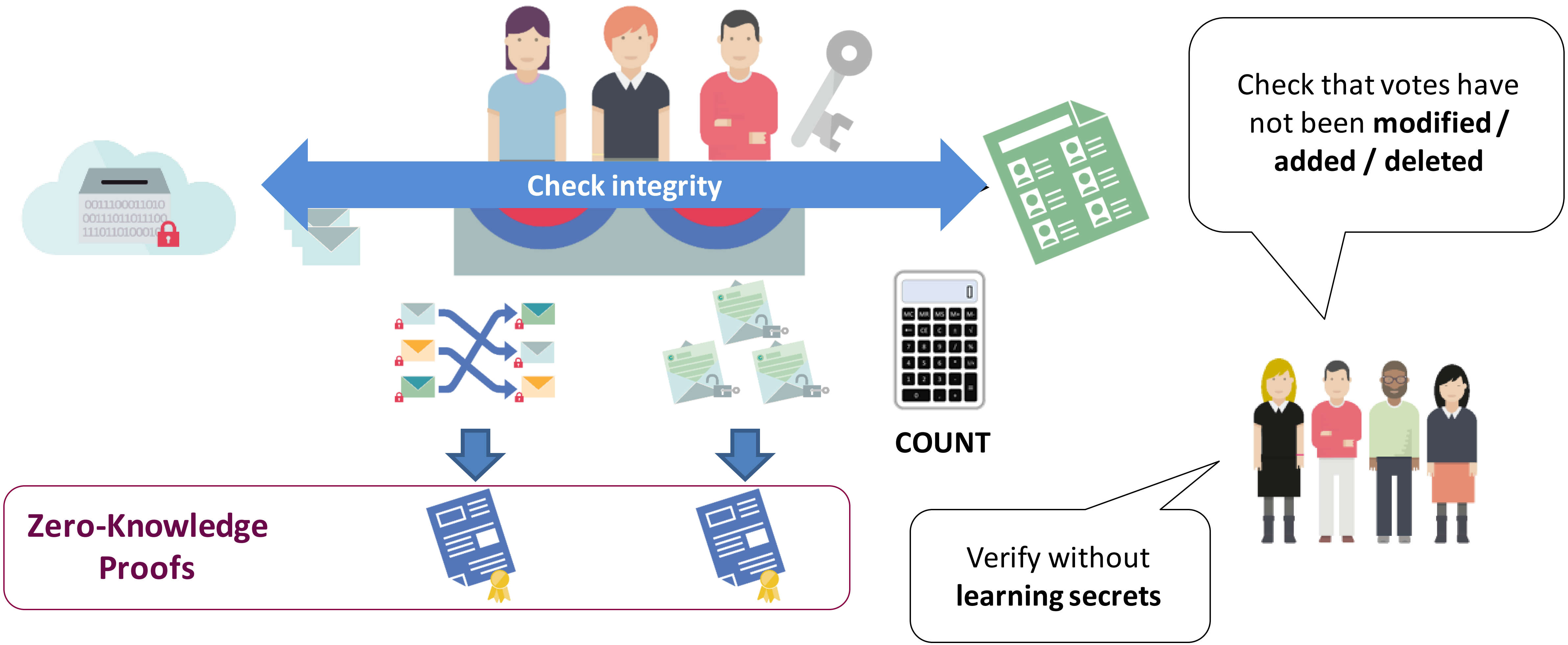
SHUFFLE
with a
secret permutation

DECRYPT
with a
private key

COUNT

(3) Verifying the counting process

The Electoral Board **does more than in traditional elections**



Check integrity

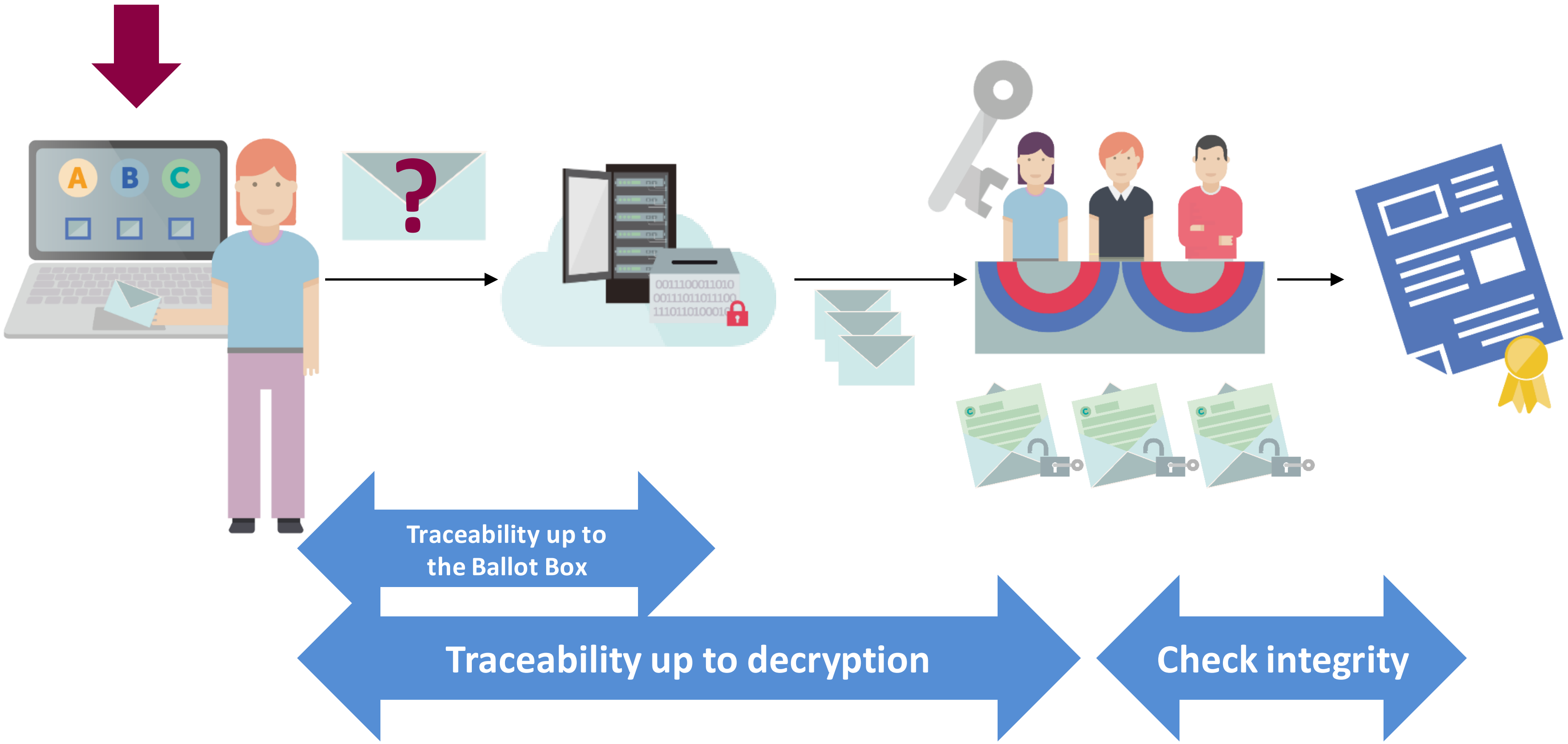
COUNT

Check that votes have not been **modified / added / deleted**

Zero-Knowledge Proofs

Verify without **learning secrets**

Verifiability in online voting

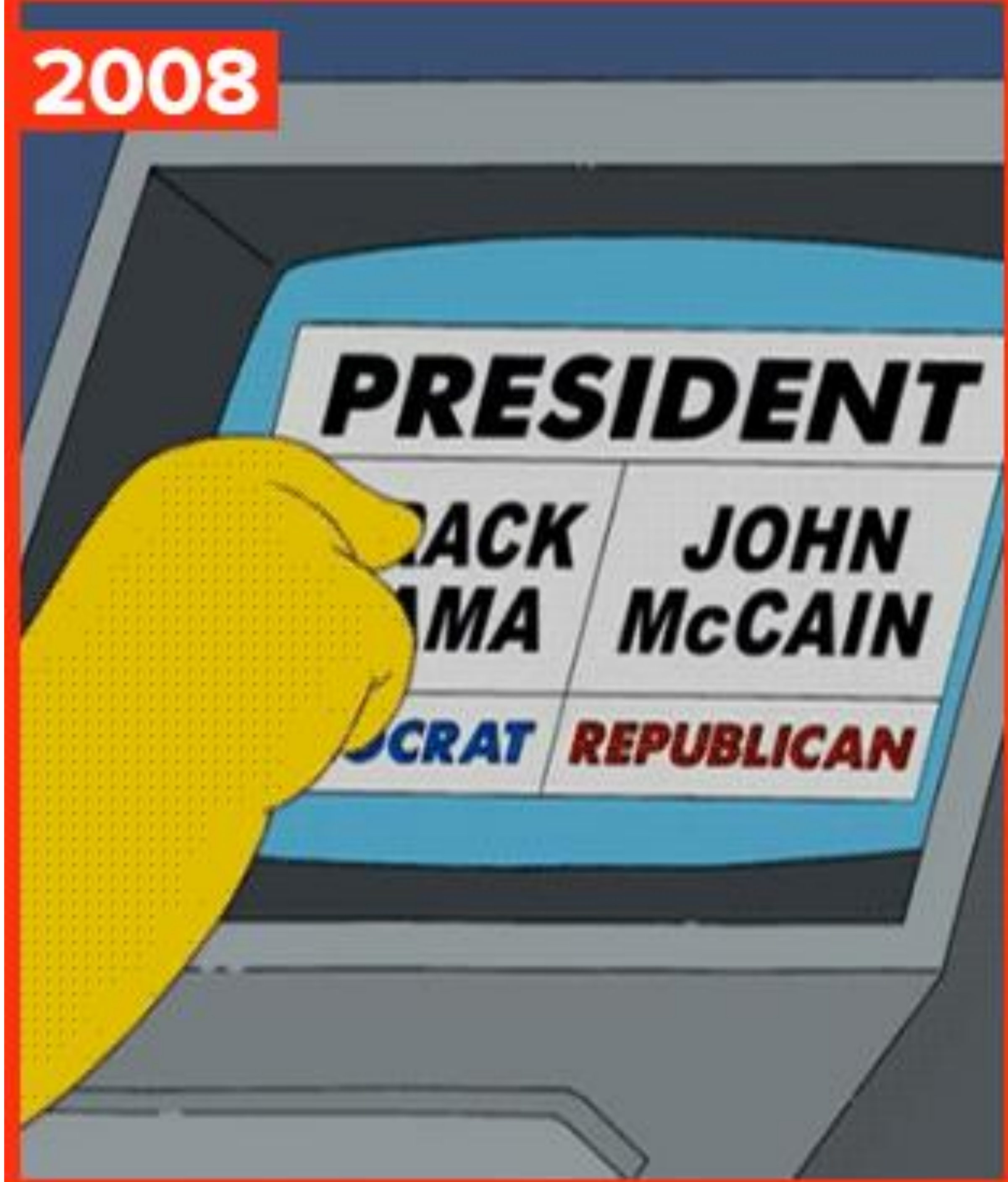


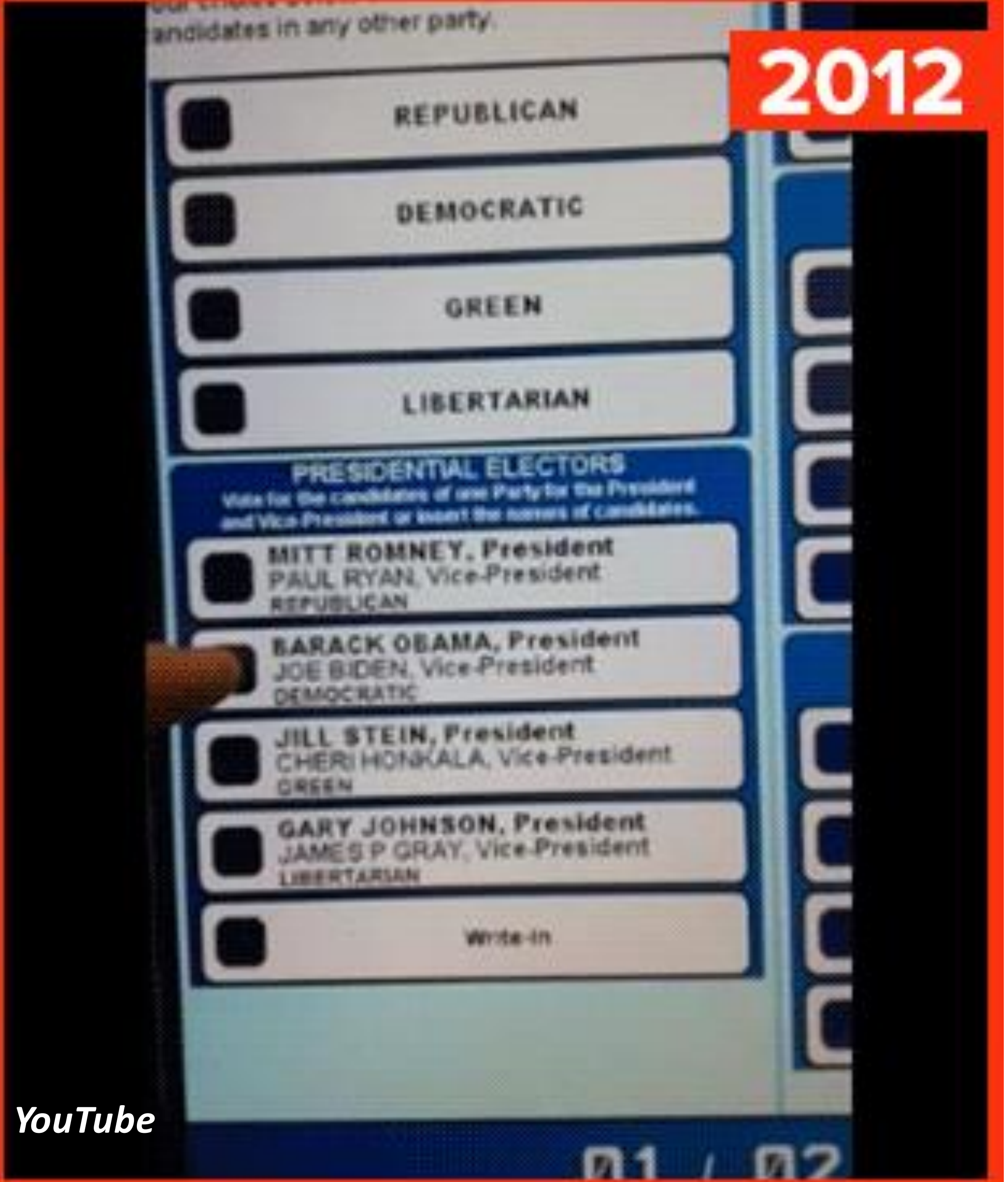
Traceability up to the Ballot Box

Traceability up to decryption

Check integrity

What happens if I have malware in my computer?





andidates in any other party.

□ REPUBLICAN

□ DEMOCRATIC

□ GREEN

□ LIBERTARIAN

PRESIDENTIAL ELECTORS
Vote for the candidates of one Party for the President and Vice-President or insert the names of candidates.

□ MITT ROMNEY, President
PAUL RYAN, Vice-President
REPUBLICAN

□ BARACK OBAMA, President
JOE BIDEN, Vice-President
DEMOCRATIC

□ JILL STEIN, President
CHERI HONKALA, Vice-President
GREEN

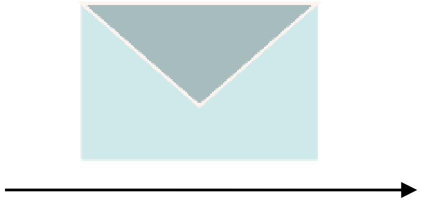
□ GARY JOHNSON, President
JAMES P GRAY, Vice-President
LIBERTARIAN

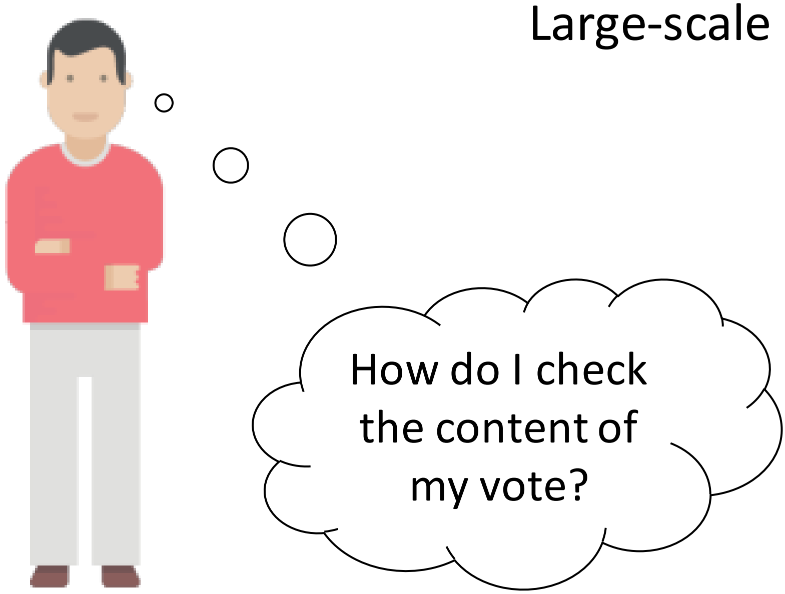
□ Write-in

01 / 02

Check the content of my vote

Vote is encrypted on the voter´s computer



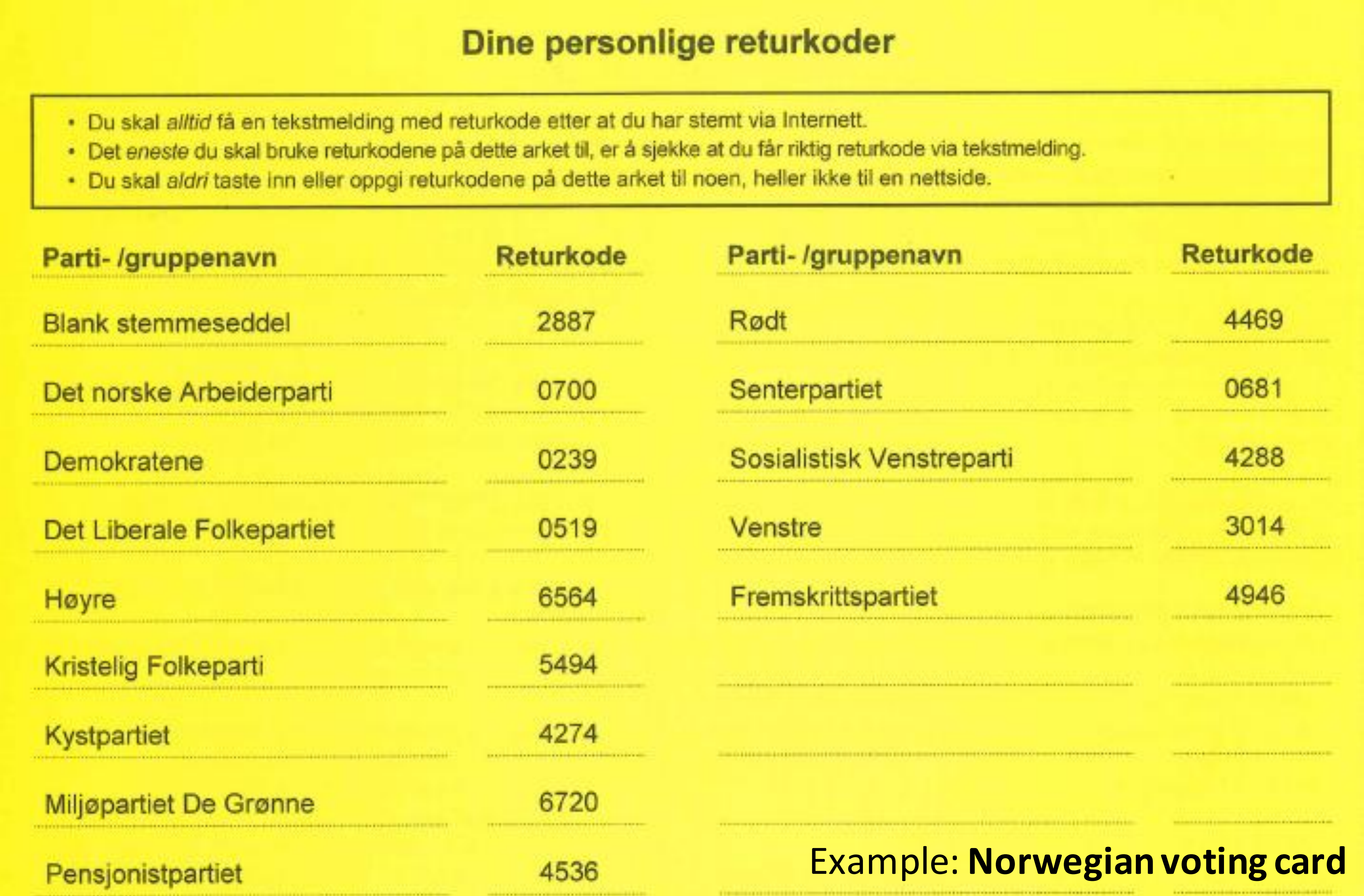


Cast-as-intended verification

- Audit of cryptographic operations
- Usually using a trusted component

Some voters verifying
=
Large-scale attacks detected

(1) Return codes



Dine personlige returkoder

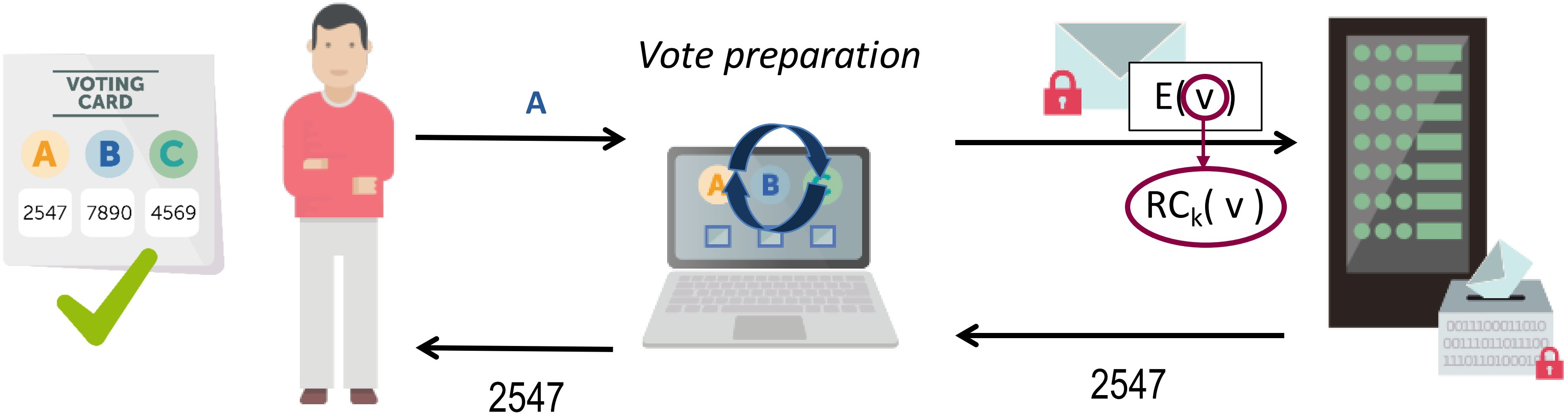
- Du skal *alltid* få en tekstmelding med returkode etter at du har stemt via Internett.
- Det *eneste* du skal bruke returkodene på dette arket til, er å sjekke at du får riktig returkode via tekstmelding.
- Du skal *aldri* taste inn eller oppgi returkodene på dette arket til noen, heller ikke til en nettside.

Parti- /gruppenavn	Returkode	Parti- /gruppenavn	Returkode
Blank stemmeseddel	2887	Rødt	4469
Det norske Arbeiderparti	0700	Senterpartiet	0681
Demokratene	0239	Sosialistisk Venstreparti	4288
Det Liberale Folkepartiet	0519	Venstre	3014
Høyre	6564	Fremskrittspartiet	4946
Kristelig Folkeparti	5494		
Kystpartiet	4274		
Miljøpartiet De Grønne	6720		
Pensjonistpartiet	4536		

Example: **Norwegian voting card**

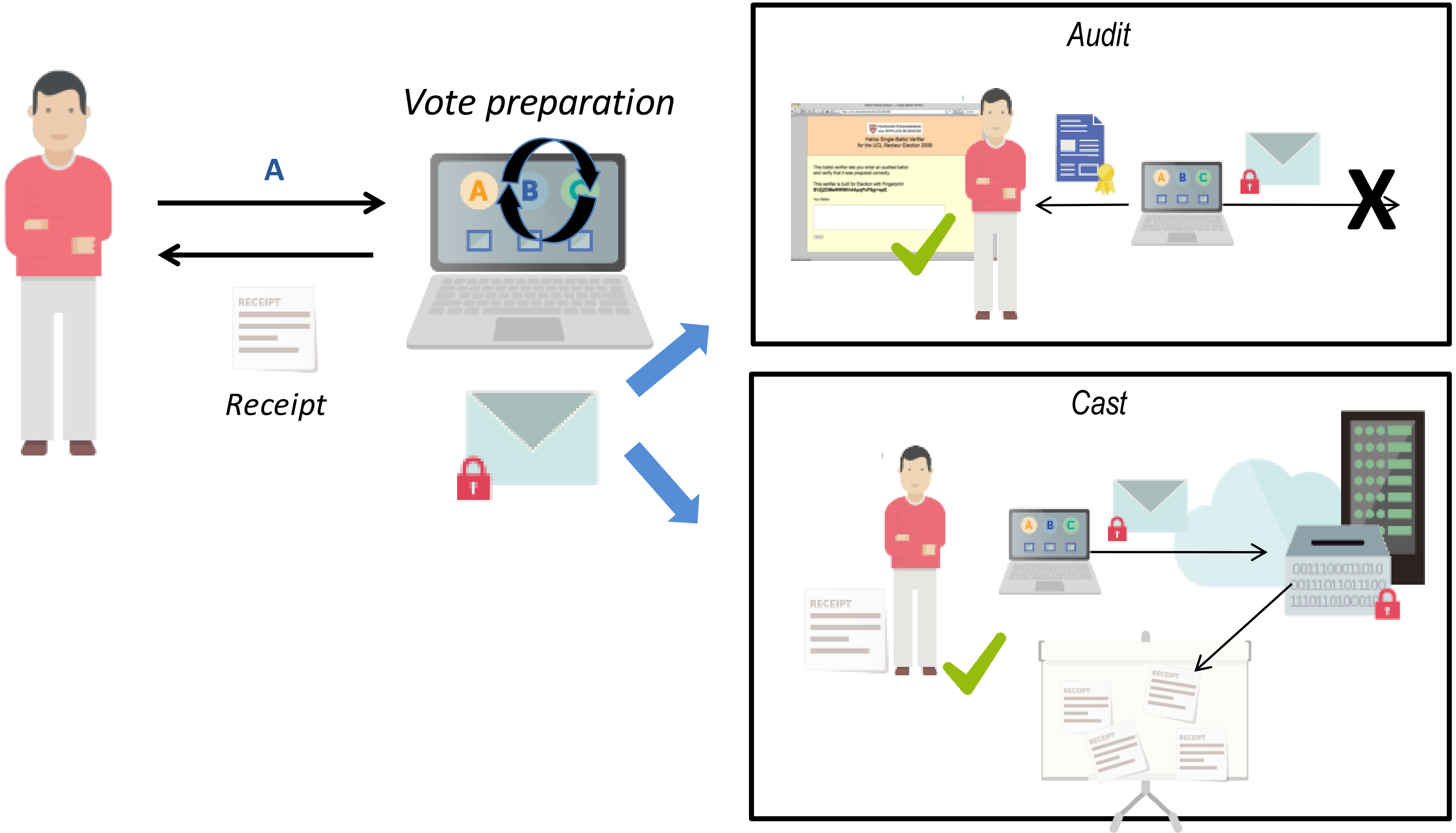
(1) Return codes

Voters use a previously received reference on paper to verify their vote after it has been cast



(2) Cast or audit

Voters use an audit application
to verify before casting



Vote preparation

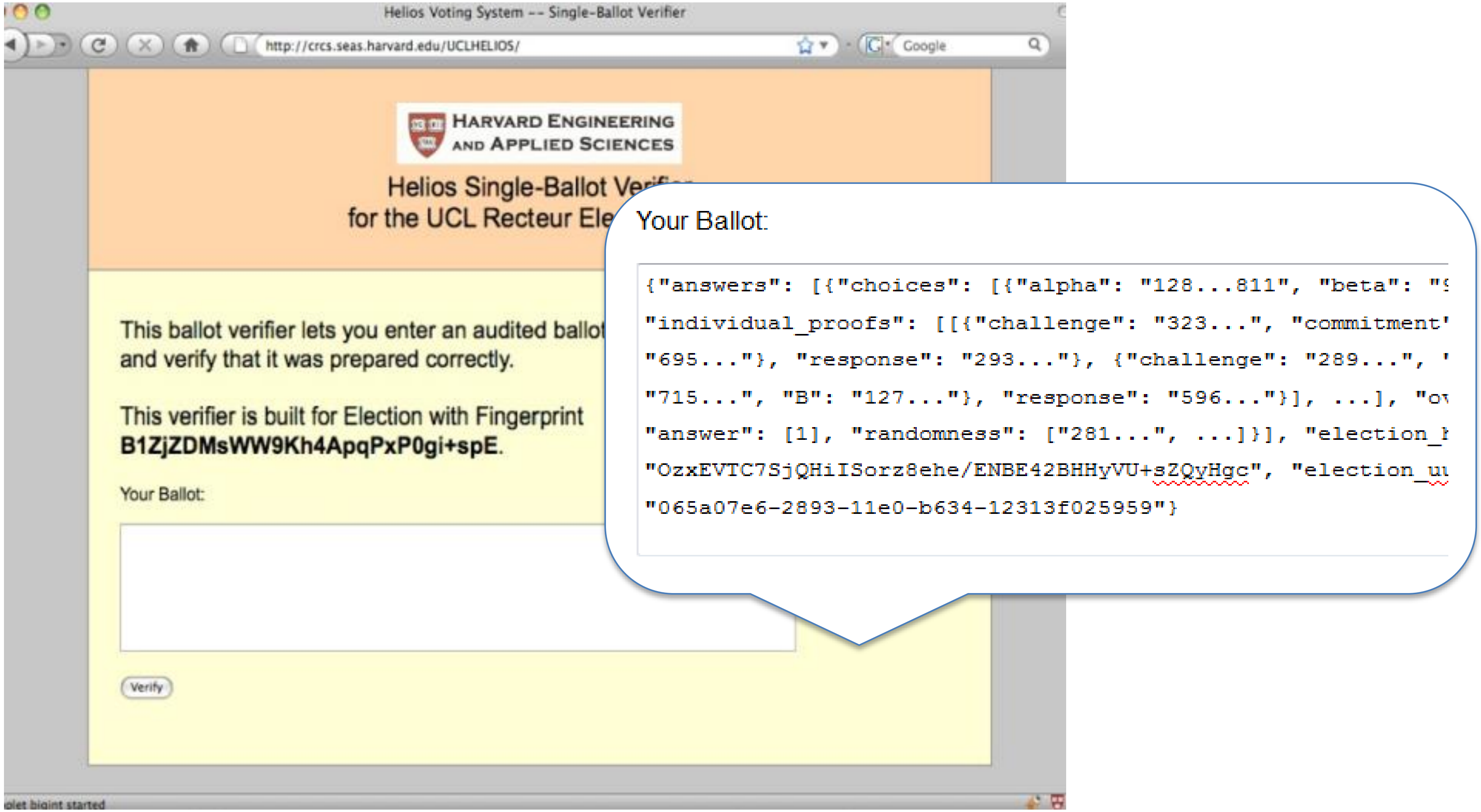
A

Receipt

Audit

Cast

(2) Cast or audit



Helios Voting System -- Single-Ballot Verifier
http://crcs.seas.harvard.edu/UCLHELIOS/
Google
Harvard Engineering and Applied Sciences

Helios Single-Ballot Ver
for the UCL Recteur Ele

This ballot verifier lets you enter an audited ballot
and verify that it was prepared correctly.

This verifier is built for Election with Fingerprint
B1ZjZDMsWW9Kh4ApqPxP0gi+spE.

Your Ballot:

Verify
olet bigint started

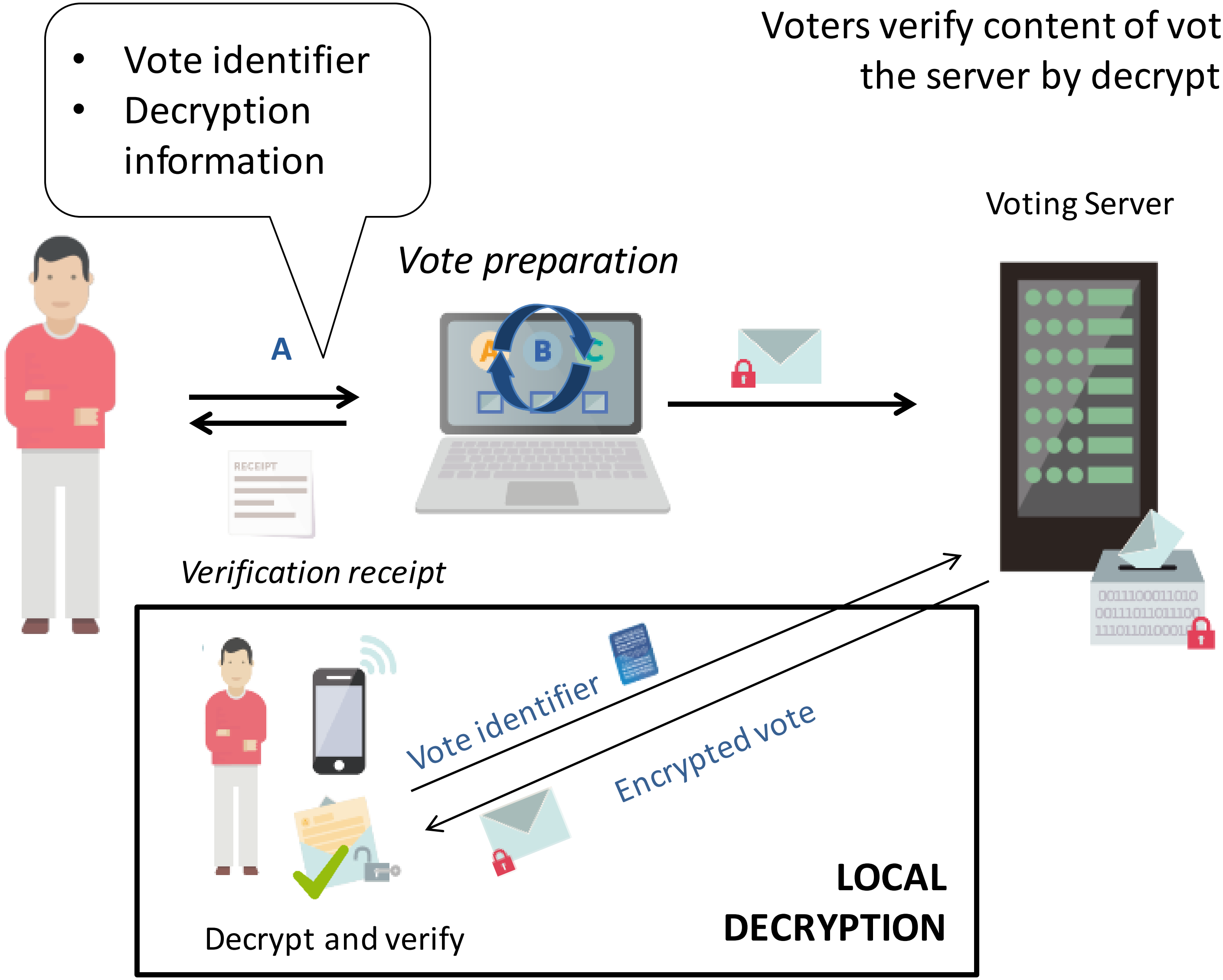
Your Ballot:

```
{"answers": [{"choices": [{"alpha": "128...811", "beta": "
"individual_proofs": [[{"challenge": "323...", "commitment"
"695..."}, "response": "293..."}, {"challenge": "289...", "
"715...", "B": "127..."}, "response": "596..."}], ...], "o
"answer": [1], "randomness": ["281...", ...]}], "election_
"OzxEVTC7SjQHiISorz8ehe/ENBE42BHHyVU+sZQyHgc", "election_u
"065a07e6-2893-11e0-b634-12313f025959"}
```

Example: **UCL student elections with Helios**

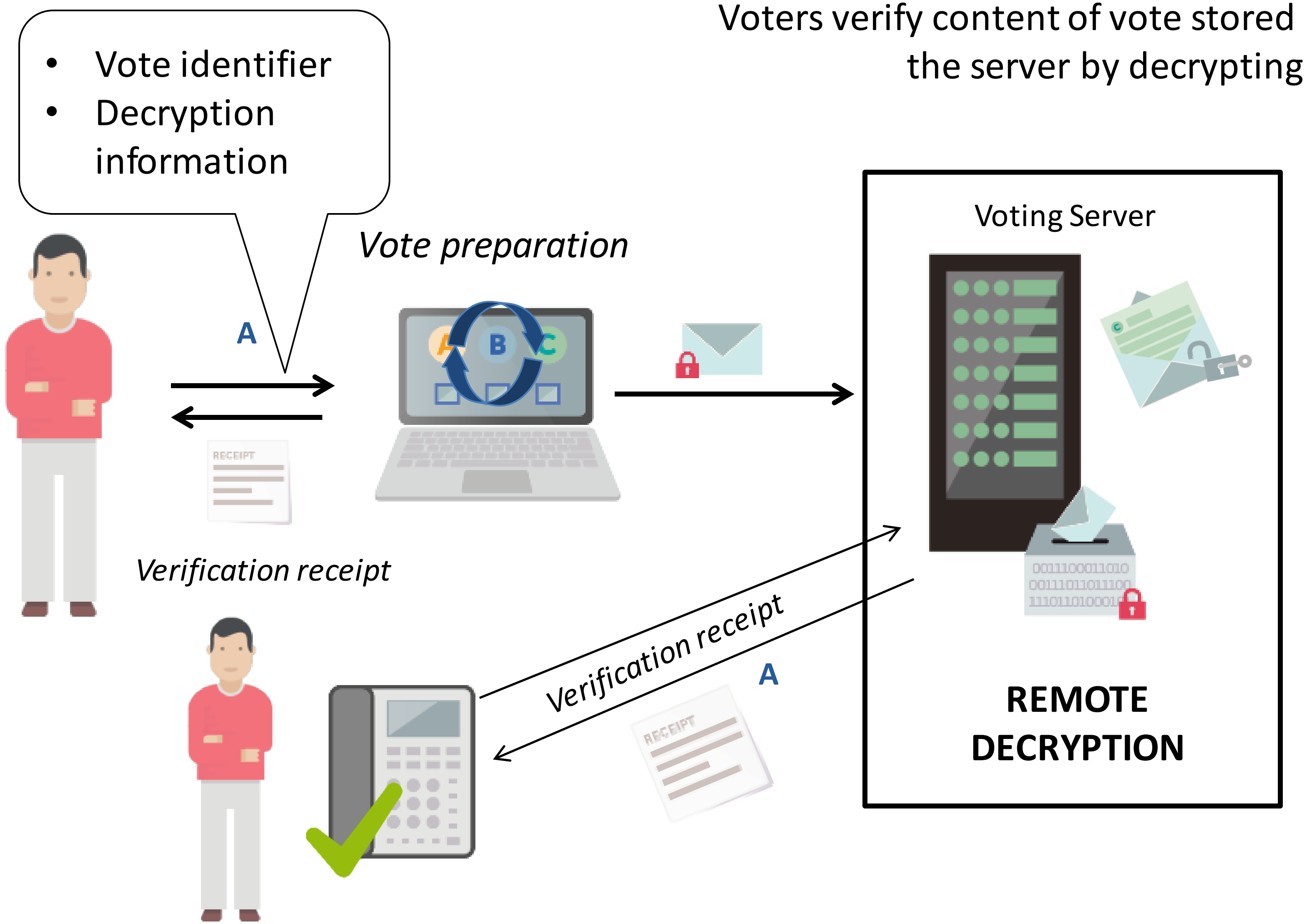
(3) Decrypt cast vote

Voters verify content of vote stored in the server by decrypting it

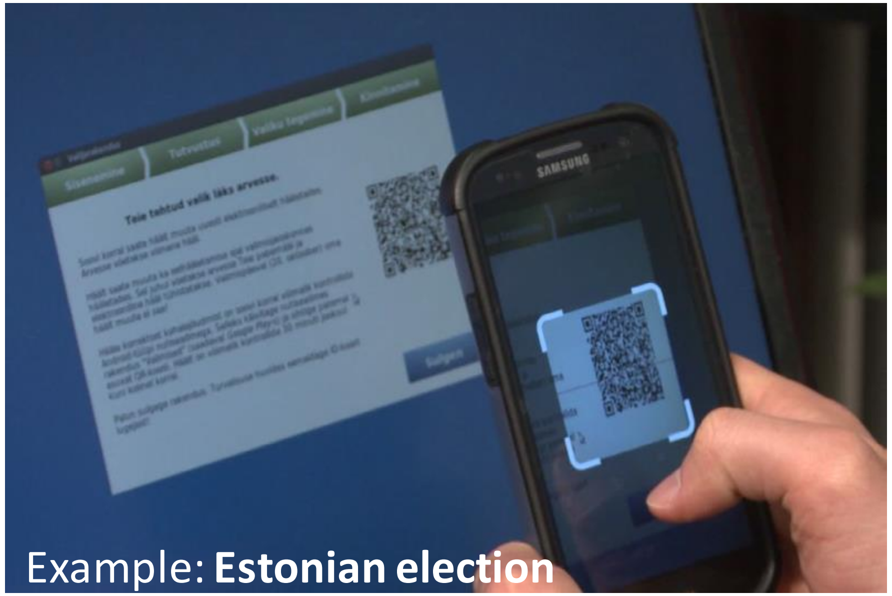


(3) Decrypt cast vote

Voters verify content of vote stored in the server by decrypting it

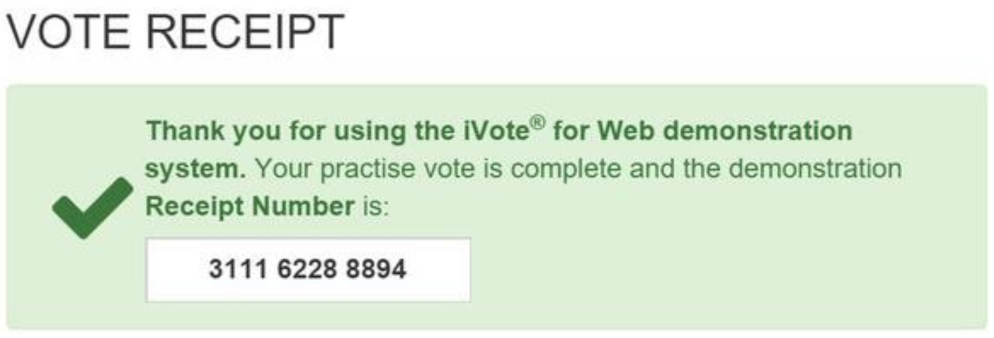


(3) Decrypt cast vote



Example: **Estonian election**

LOCAL
DECRYPTION



VOTE RECEIPT

✓ **Thank you for using the iVote® for Web demonstration system.** Your practise vote is complete and the demonstration **Receipt Number** is:

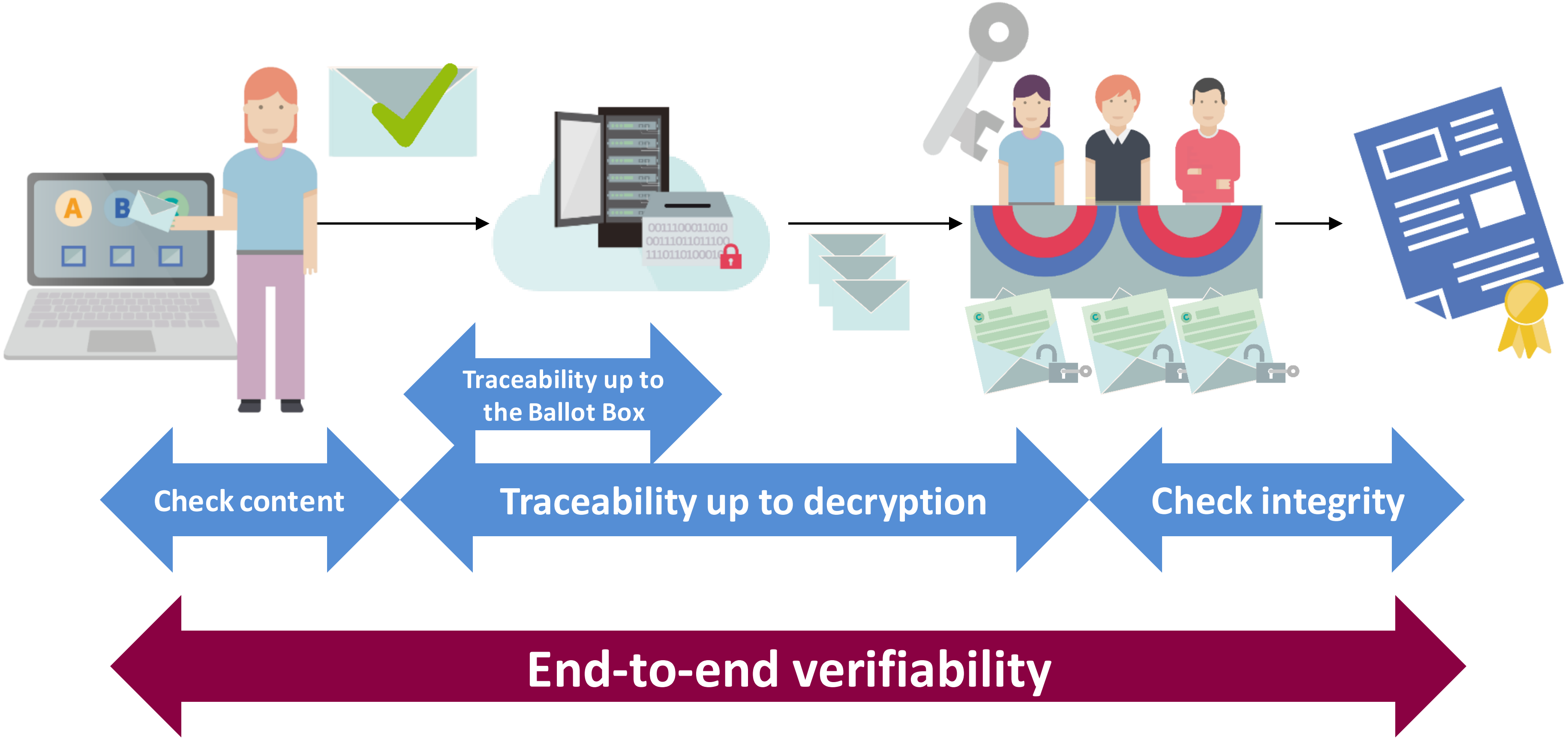
3111 6228 8894

Example: **New South Wales iVote system**

REMOTE
DECRYPTION

Scytl
Innovating Democracy

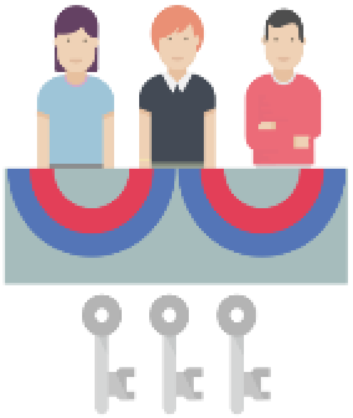
End-to-end verifiability



A private company can control the election!!!!

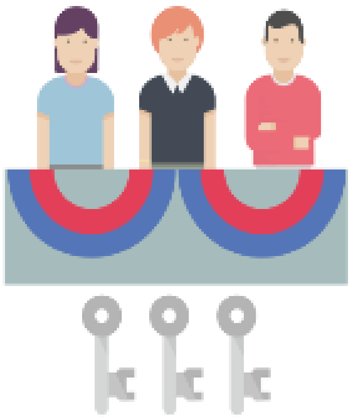
Administration vs Electoral Board

Electoral Board



- Preserves Election privacy
- Decryption keys

Administration Board



- Preserves Election configuration integrity
- Signing keys

Administration and Electoral Board

- Secret keys split in **“shares”**.
- Shamir Secret Sharing Scheme.
- Shares stored in **smartcards** or any other hardware token.
- Owned by the **board members.**
- Protected by a **PIN code** selected by them.

Administration and Electoral Board

- **Cryptographic keys** can be created in **isolated / air-gap** computers, that have been properly hardened and protected.

- It takes place during official ceremonies with local **authorities, auditors, observers, politics, media**…

- You can **generate only the shares** and then reconstruct the public key, so the private key does not exist until the election end.

One single person cannot…

- ✗ Decrypt the votes
- ✗ Modify the electoral roll
- ✗ Generate fake results
- ✗ Modify or add votes

Trust relies on the Electoral and Administration

Boards, auditors, and observers

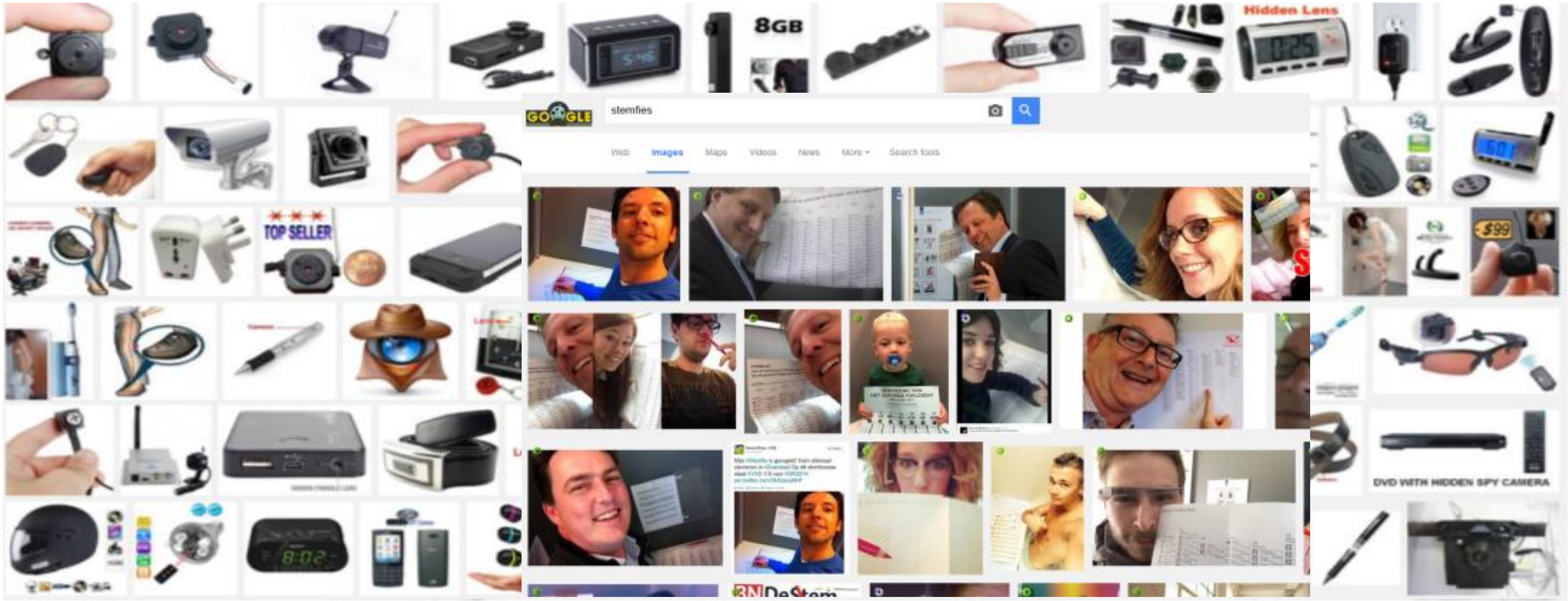
SERIES 2003 A
JK 432
K11
106285
FEDERAL RESERVE SYSTEM
NOTE IS LEGAL TENDER DEBTS, PUBLIC AND P
Treasurer of the United States.
LEGAL TENDER PUBLIC AND PRIVATE
THIS NOTE IS L FOR ALL DEBTS, PU
NOVUS ORDO SECLORUM
THE GREAT SEAL

But voters might be coerced or bought!!!

You can show your vote in remote voting

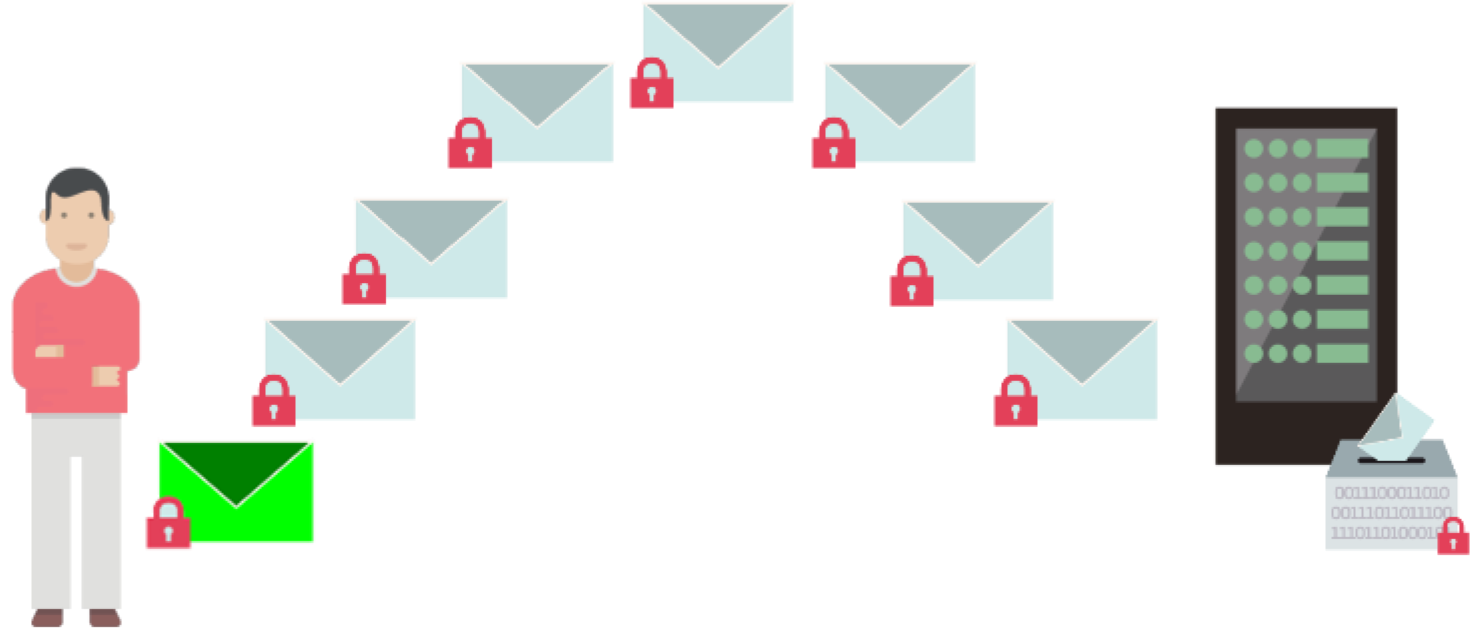
Yes… ⏺ ▶ ⏸ ⏹

But also in traditional voting…



What can you do to prevent coercion or vote-buying

Cheating the coercer / vote buyer



1] Allow multiple voting (last vote counts)

Make the attack expensive at large-scale

2] OTP sent to the phone of the registered voter

Any system in the wild wild web can be hacked…

Reduce the surface

- Isolated / offline servers for critical activities
- Just a few of endpoints
- Short timeframe
- Last patched versions of any software
- Hardened and appropriately tested

OK but…
what if an attacker were to be finally successful, and …

Sysadmins always have access to everything…

(1) Split of responsibilities

The voting terminal

The **Servers**

Isolated computers

(2) We have discussed…

- END-TO-END ENCRYPTION
- MIXNETS
- SECRET SHARING SCHEMES
- ELECTORAL BOARDS
- ZERO KNOWLEDGE PROOFS
- END-TO-END VERIFIABILITY

(3) One single person cannot…

- ✗ Decrypt the votes
- ✗ Modify the electoral roll
- ✗ Generate fake results
- ✗ Modify or add votes

Trust relies on the Electoral and Administration Boards, auditors, and observers

What could a sysadmin do wrong?

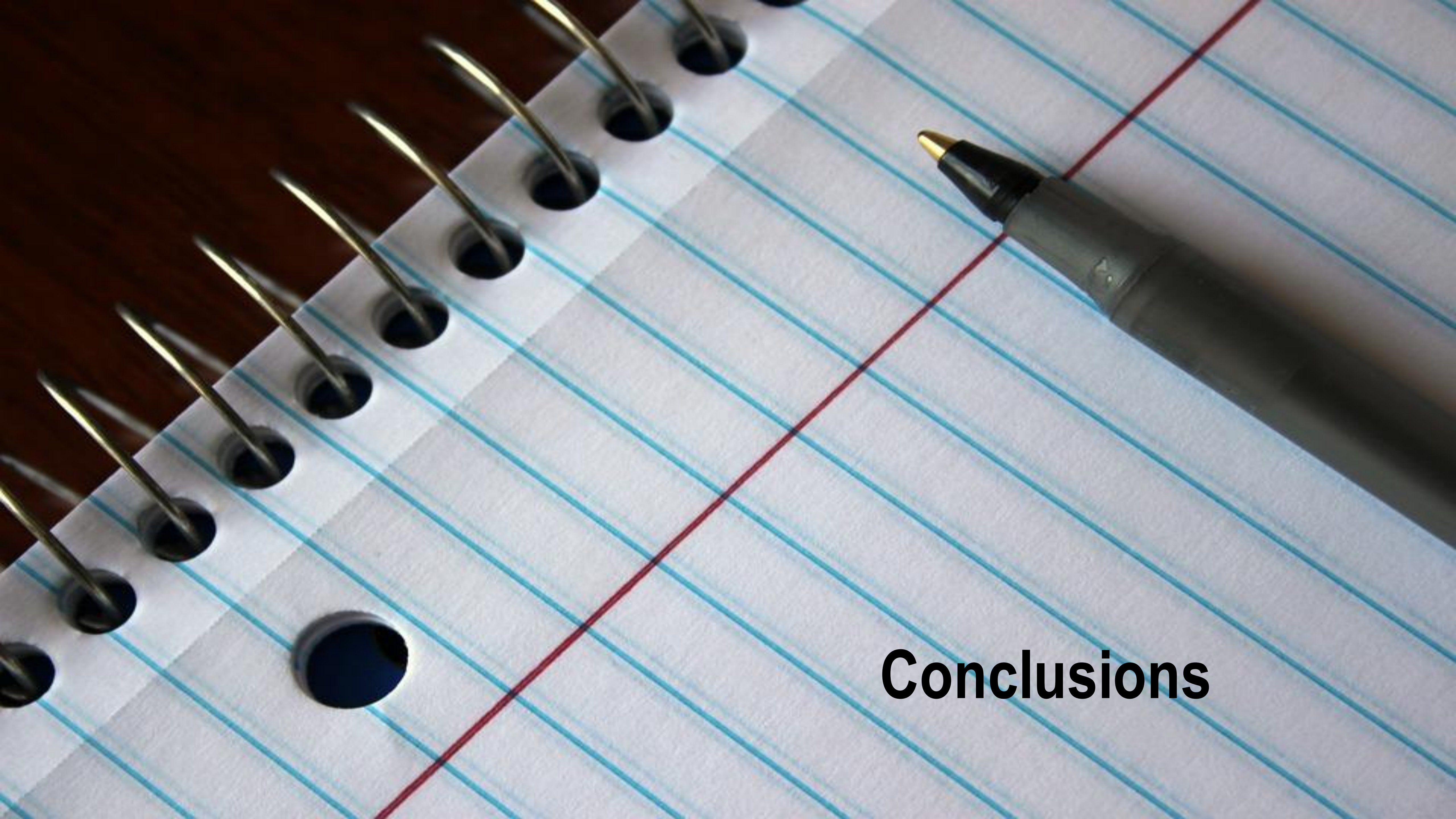
Boycott / Vandalism?

But there are **backups and Disaster Recovery Plans**

…which are even more complex in traditional elections

Replace the software for a malicious one?

But you can use **end-to-end verifiability**



Conclusions

Conclusions

Summary of main cryptographic measures:

- **End-to-end encryption** starting on the **voters' device**
- The Electoral Boards and **secret sharing schemes**
- **Sensitive operations** performed in ceremonies, on **isolated computers**
- **Cast as intended** verifiability and **Return Codes**
- Vote **traceability** and voting **receipts**
- Verifiable **mix-nets** and decryption using **ZKPs**

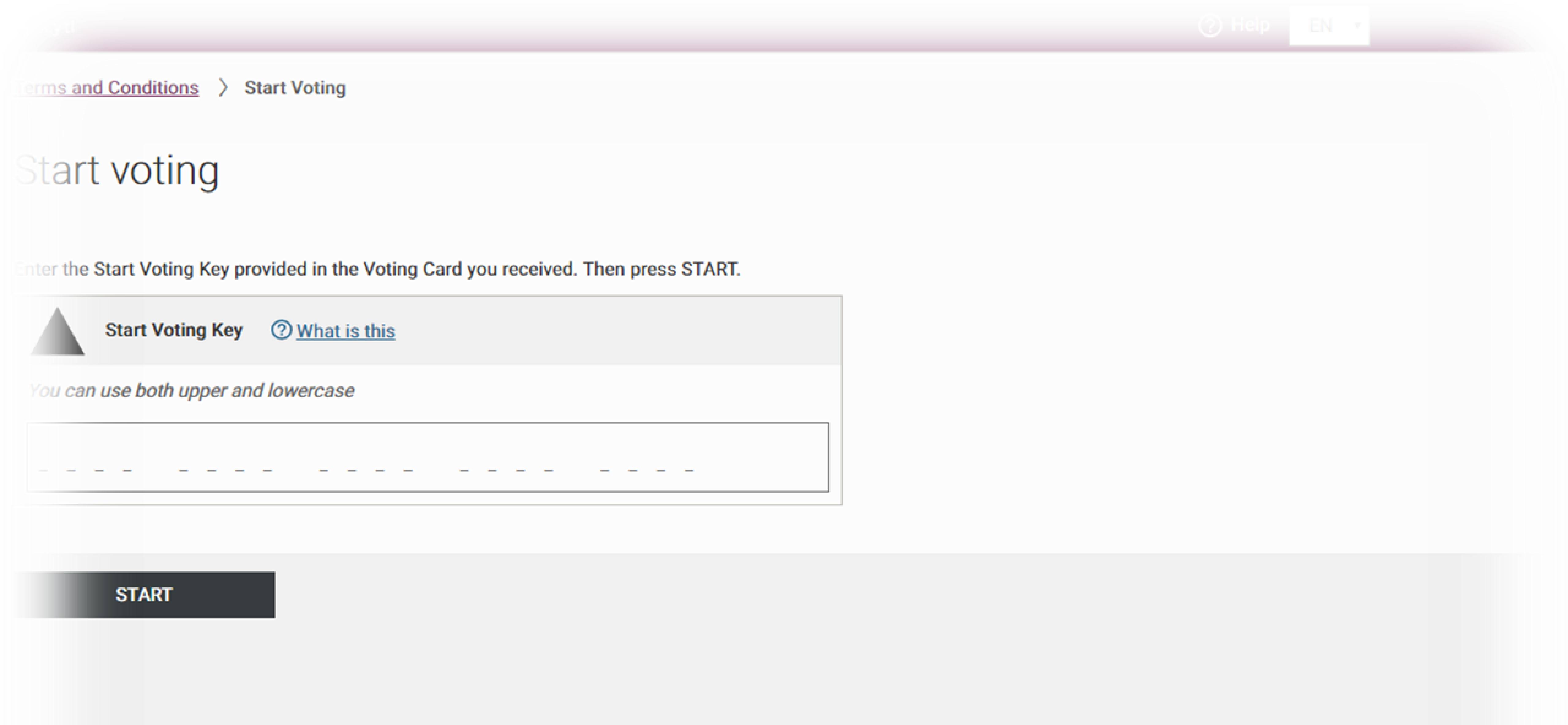
Conclusions

- There are lot of **advanced security controls on Internet Voting**, although they are not know by the general public
- Similar to **traditional elections**
- And much **better than postal voting**
- Strongest security controls rely on **cryptography**

Conclusions

Internet Voting means that some remote computers handle your vote.

But it does not mean that you need to trust on them…



Terms and Conditions > Start Voting

Start voting

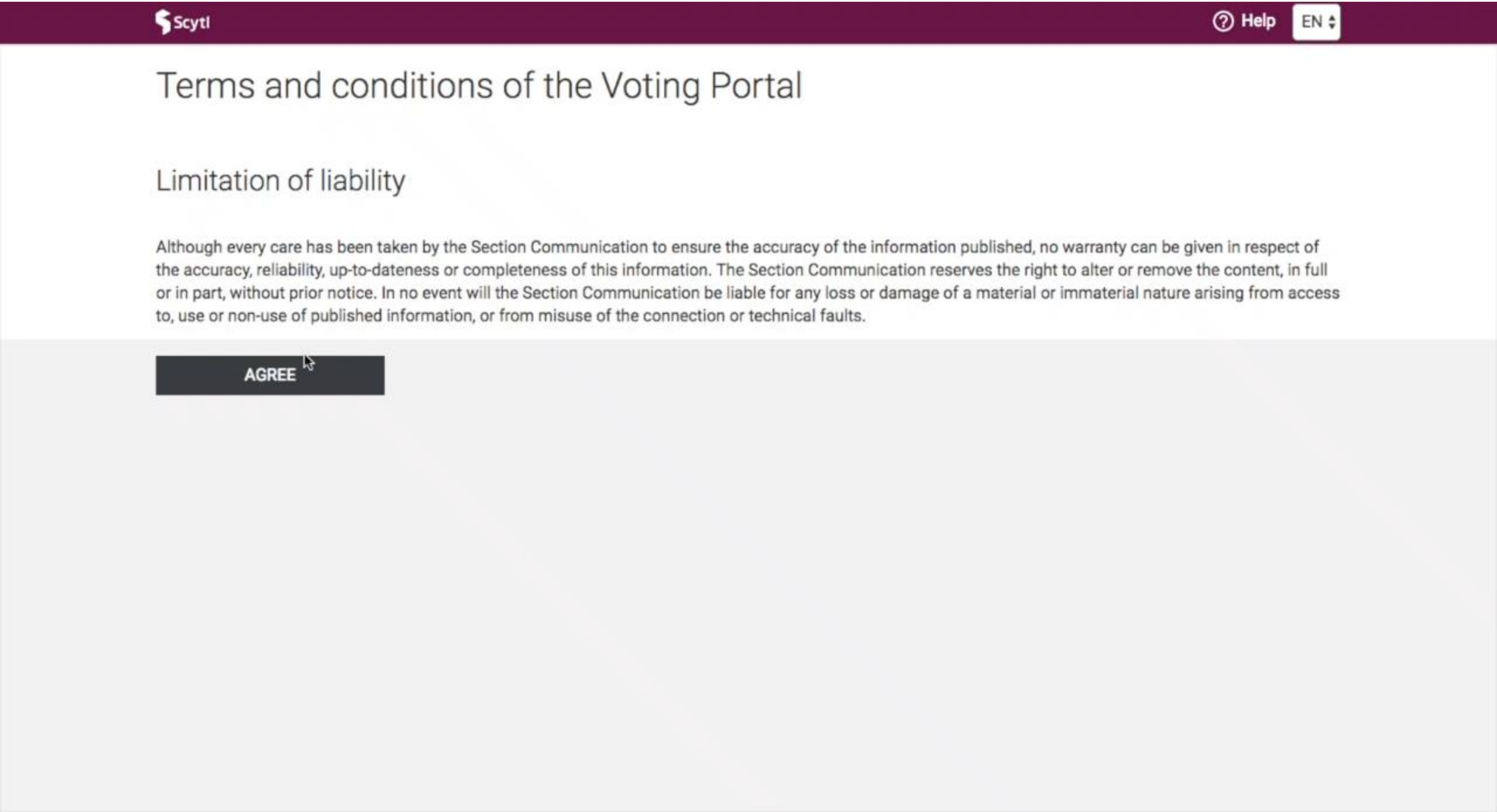
Enter the Start Voting Key provided in the Voting Card you received. Then press START.

Start Voting Key ⓘ What is this

You can use both upper and lowercase

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

DEMO TIME



Terms and conditions of the Voting Portal

Limitation of liability

Although every care has been taken by the Section Communication to ensure the accuracy of the information published, no warranty can be given in respect of the accuracy, reliability, up-to-dateness or completeness of this information. The Section Communication reserves the right to alter or remove the content, in full or in part, without prior notice. In no event will the Section Communication be liable for any loss or damage of a material or immaterial nature arising from access to, use or non-use of published information, or from misuse of the connection or technical faults.

Any questions?

Innovating Democracy