

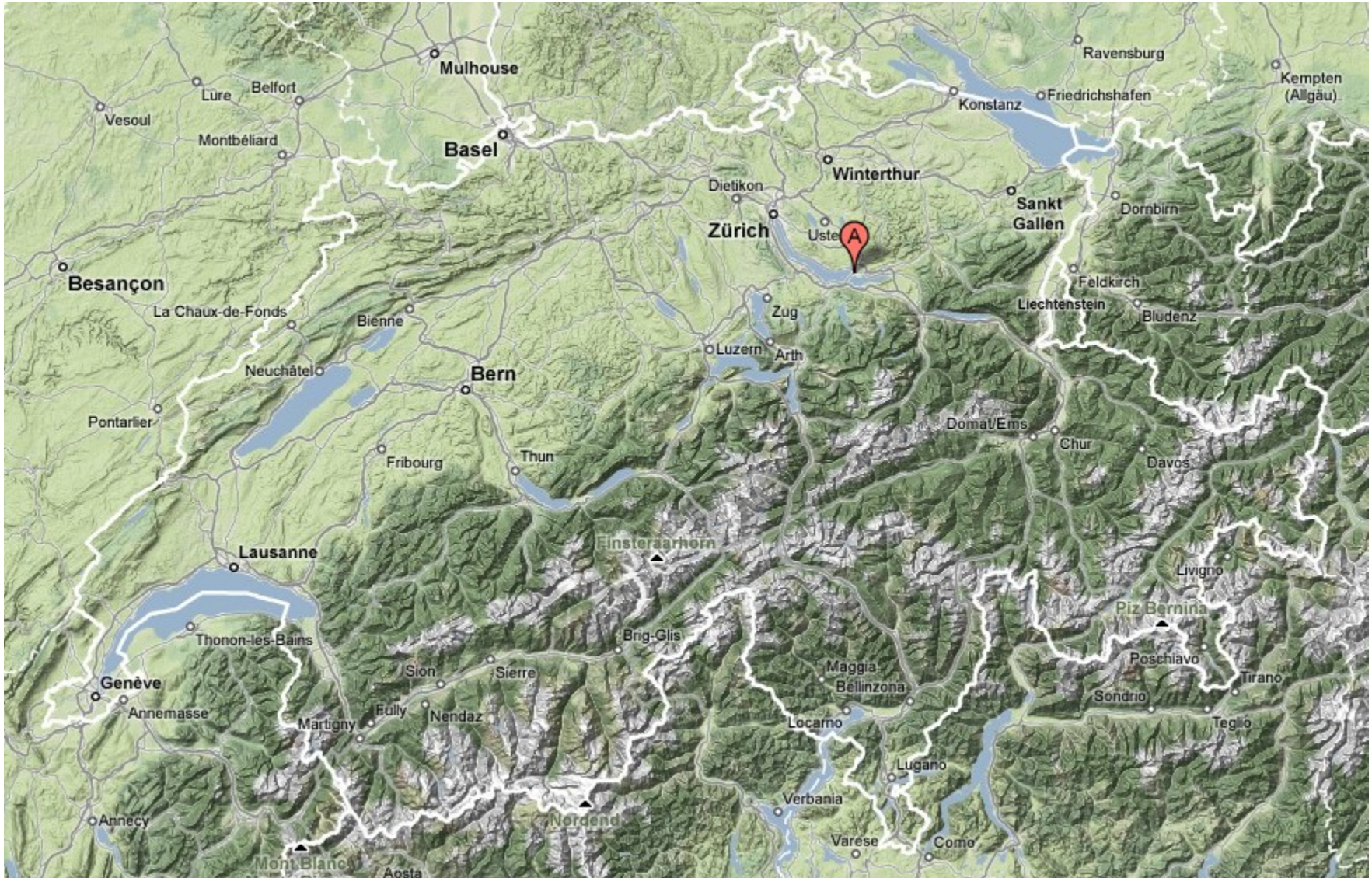
# Verifiable E-Voting with Open Source

Prof. Dr. Andreas Steffen

Hochschule für Technik Rapperswil

[andreas.steffen@hsr.ch](mailto:andreas.steffen@hsr.ch)

# Where the heck is Rapperswil?



- University of Applied Sciences with about 1000 students
- Faculty of Information Technology (300-400 students)
- Bachelor Course (3 years), Master Course (+1.5 years)



## Summary of my talk:

- Due to repeated failures and detected vulnerabilities in both electro-mechanical and electronic voting machines, voters have somehow lost faith that the outcome of a poll always represents the true will of the electorate.
- Manual counting of paper ballots is not really an option in the 21<sup>st</sup> century and is not free from tampering either.
- Modern cryptographic voting systems allow true end-to-end verification of the complete voting process by any individual voter, without sacrificing secrecy and privacy.

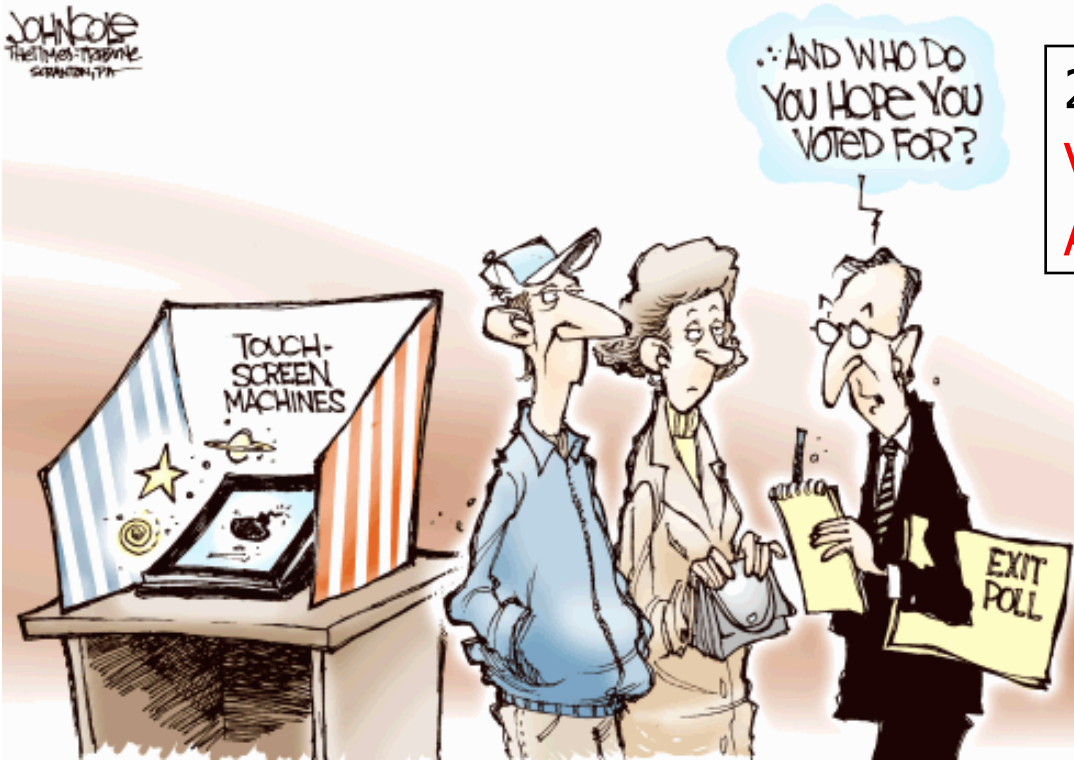
- In the 2006 mid-term federal elections, **one third** of registered U.S. voters used Direct Recording Electronic (DRE) voting machines.
- In the 2008 federal elections, many states returned to paper ballots with optical scanning but six states used 100% DREs **without** a Voter-Verified Paper Audit Trail (VVPAT).



Diebold Elections System DRE voting machine with a VVPAT attachment.

# Losing Trust in Electronic Voting Systems

John Cole  
The Times Magazine  
September 4, 2006



2006 - The Morning Call:  
**Voter smashes DRE in Allentown with metal cat**



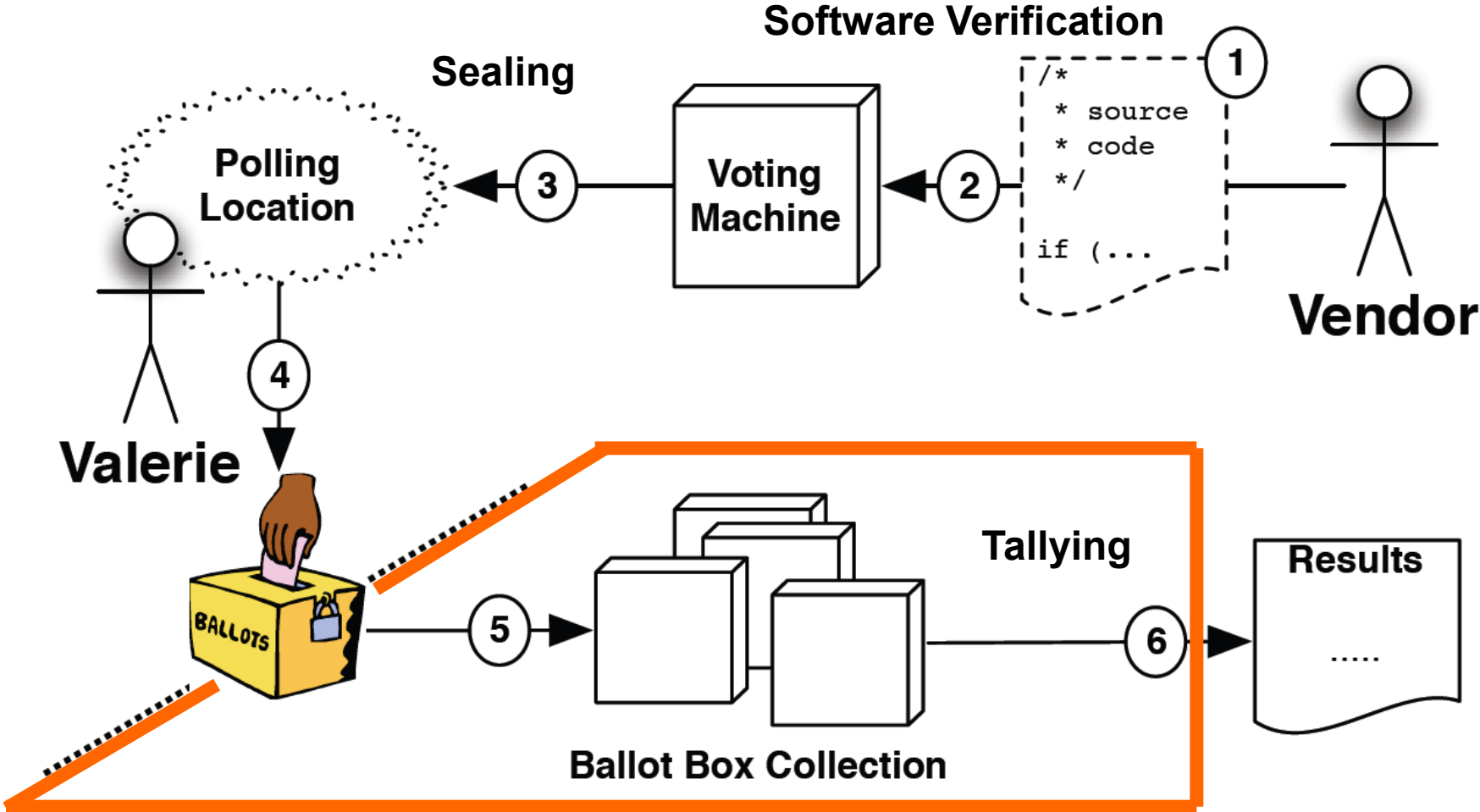
2006 - Princeton study on Diebold DRE:  
**Hack the vote? No problem**

2006 - Dutch ES3B voting machines:  
**Hacked to play chess**



March 3 2009 - Germany:  
**Bundesverfassungsgericht bans e-voting machines**

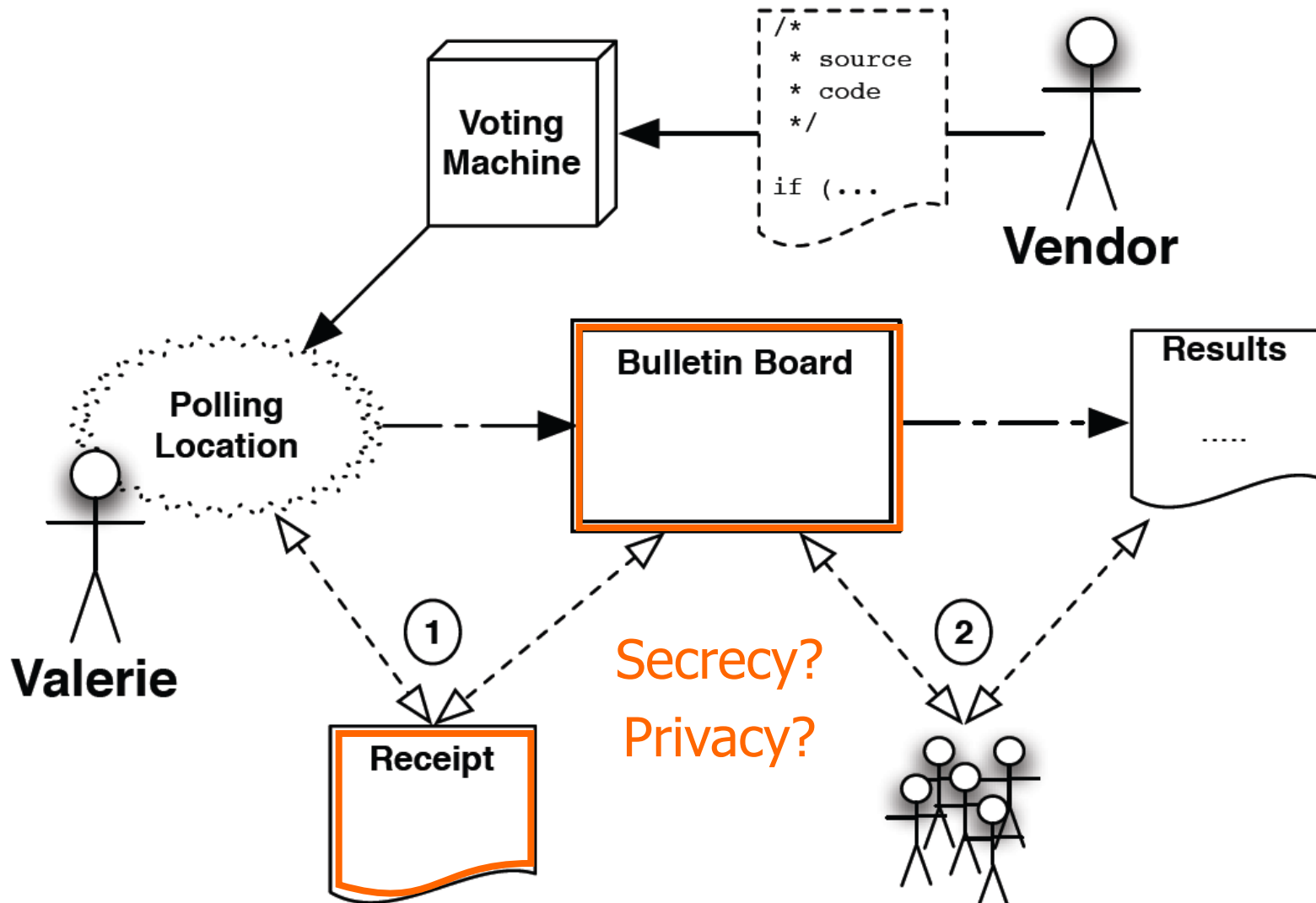
# Traditional Chain-of-Custody Security



**Verification by proxy only**

Source: Ben Adida, Ph.D. Thesis 2006

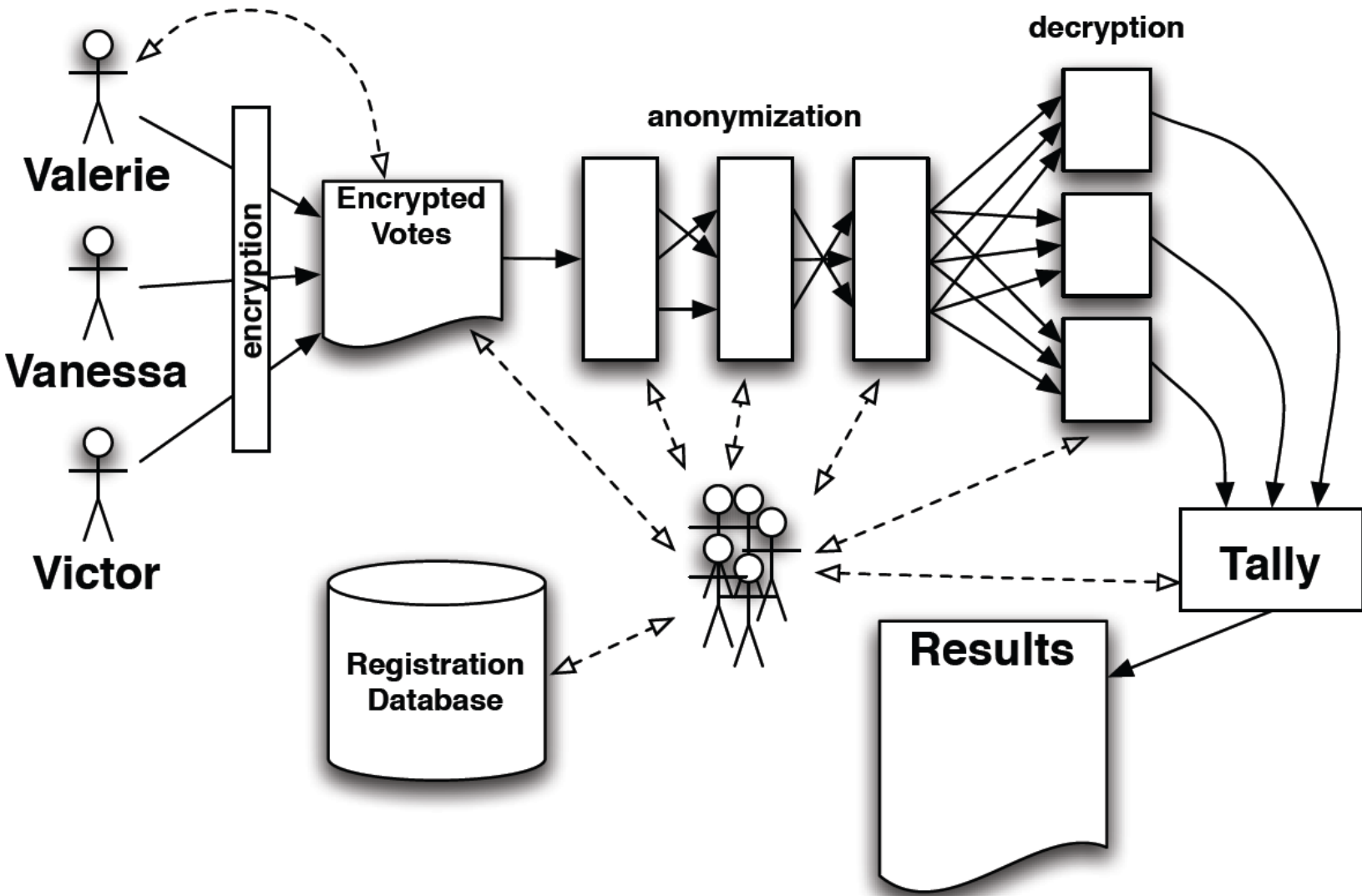
# Desirable: End-to-End Verification by Voter





- Any voter can verify that his or her ballot is included unmodified in a collection of ballots.
- Any voter (and typically any independent party additionally) can verify [with high probability] that the collection of ballots produces the correct final tally.
- No voter can demonstrate how he or she voted to any third party (thus preventing vote-selling and coercion).

# Solution: Cryptographic Voting Systems



Source: Ben Adida, Ph.D. Thesis 2006

## Proposed E2E Systems

- **Punchscan** by David Chaum.
- **Prêt à Voter** by Peter Ryan.
- **Scratch & Vote** by Ben Adida and Ron Rivest.
- **ThreeBallot** by Ron Rivest (paper-based without cryptography)
- **Scantegrity II** by David Chaum, Ron Rivest, Peter Ryan et al.  
(add-on to optical scan voting systems using Invisible Ink)
- **Helios** by Ben Adida (<http://www.heliosvoting.org/>)

# Helios Voting

## Elections you can audit

If my vote is supposed to stay secret, how can I verify that it was counted correctly?

The Helios Voting System implements advanced cryptographic techniques to maintain ballot secrecy while providing a mathematical proof that the election tally was correctly computed.

We call this an *open-audit election*, because you or anyone else can audit it.

Check out our [Frequently Asked Questions](#).



Create an Open-Audit Election

[\[Home\]](#) [\[My Elections\]](#) [\[Learn\]](#) [\[Blog/Updates\]](#)

All content on this site is licensed under a Creative Commons License.  
If you redistribute this content, you should give credit to Ben Adida and Harvard University.

## Helios Voting

### Elections you can audit

#### Create a New Election

Name:

- Helios administers your election
- You administer your election
- Multiple trustees administer your election

[\[Home\]](#) [\[My Elections\]](#) [\[Learn\]](#) [\[Blog/Updates\]](#)

All content on this site is licensed under a Creative Commons License.  
If you redistribute this content, you should give credit to Ben Adida and Harvard University.

## Helios Voting Elections you can audit

### Create a New Election: LinuxTag 2010

An election managed by Helios.

Generate Election Keys

[\[Home\]](#) [\[My Elections\]](#) [\[Learn\]](#) [\[Blog/Updates\]](#)

All content on this site is licensed under a Creative Commons License.  
If you redistribute this content, you should give credit to Ben Adida and Harvard University.

## Helios Voting

### Elections you can audit

#### LinuxTag 2010

Election ID

agxoZWxpb3N2b3RpbmdyEAsSCEVsZWN0aW9uGJ2QBww

Election Fingerprint

1qWpc8zsJ9K0z1o4R8mJxsp0uNM

[Vote in this election](#) [[Audit a Single Ballot](#)] [[Bulletin Board of Cast Votes](#)]

Administration

Election in Progress

- [voters](#)
- [compute tally](#)
- [archive election](#)

[\[Home\]](#) [\[My Elections\]](#) [\[Learn\]](#) [\[Blog/Updates\]](#)

All content on this site is licensed under a Creative Commons License.  
If you redistribute this content, you should give credit to Ben Adida and Harvard University.

## Helios Voting Elections you can audit

### Freeze Election: LinuxTag 2010

Once frozen, an election's questions can no longer be modified.

Since you have set up your election with **closed registration**, you will also *not* be able to modify the voter list once you freeze the election, nor will you be able to switch your election to open registration.

You must freeze an election before you can contact voters.

freeze!

never mind

---

[\[Home\]](#) [\[My Elections\]](#) [\[Learn\]](#) [\[Blog/Updates\]](#)

All content on this site is licensed under a Creative Commons License.  
If you redistribute this content, you should give credit to Ben Adida and Harvard University.



## Helios Voting Elections you can audit

### LinuxTag 2010 — Voters [done]

This election is configured with **closed voter registration**, which means that all voters must be listed before the election is frozen, and thus before the election begins.

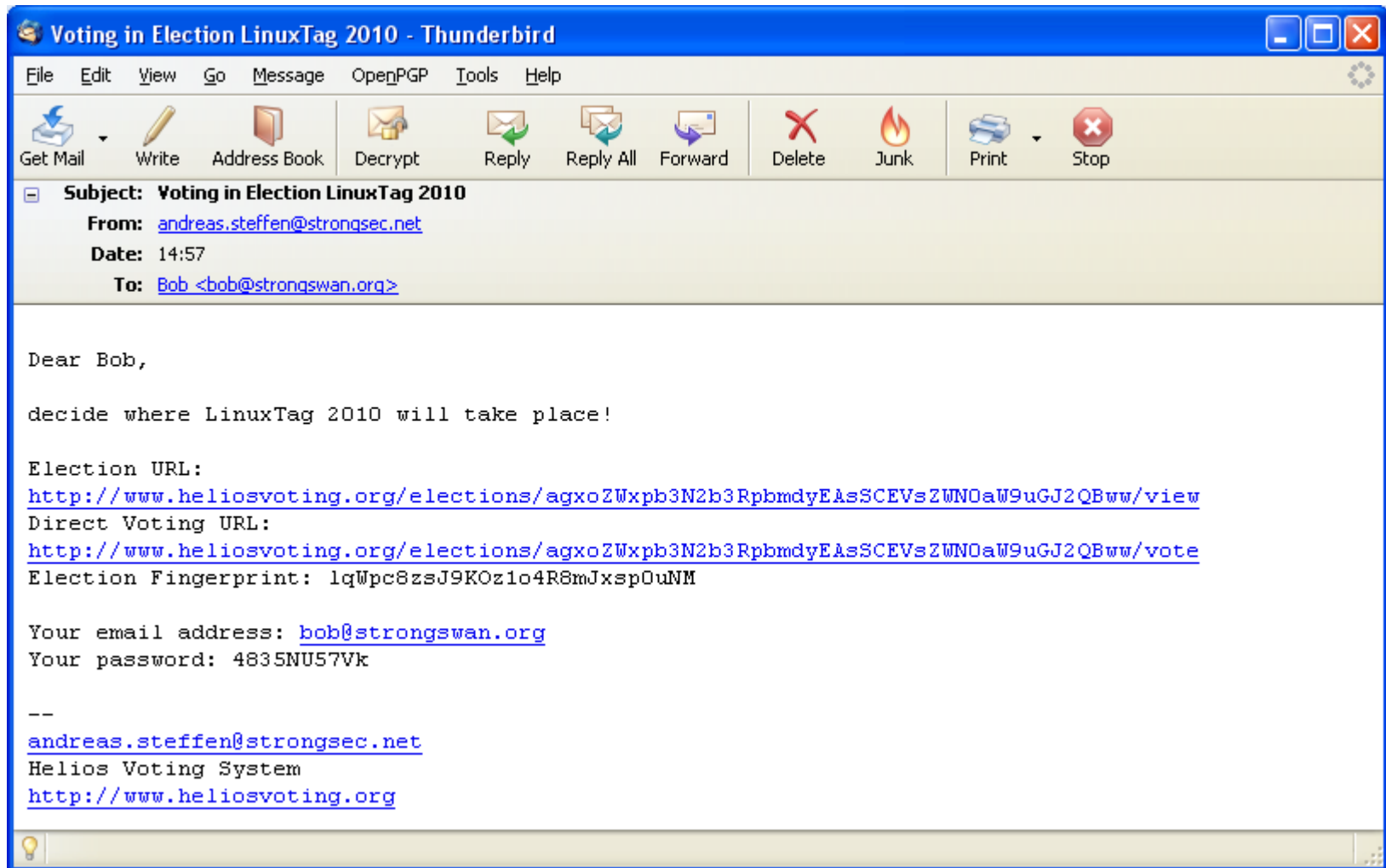
all  none  voted  not voted

Name	Email	Category	
Bob	bob@strongswan.org		<input checked="" type="checkbox"/>
Carol	carol@strongswan.org		<input checked="" type="checkbox"/>
Dave	dave@strongswan.org		<input checked="" type="checkbox"/>
Alice	alice@strongswan.org		<input checked="" type="checkbox"/>

Act on those voters you have selected above:

email

# Invite Voters per Email



## Helios Voting Booth

# LinuxTag 2010

Fingerprint: lqWpc8zsJ9KOz1o4R8mJxsp0uNM

Welcome to the **LinuxTag 2010** election.

To cast a vote, you will be led through the following steps:

1. **Select** your options.  
Answer every question, and review your choices.
2. **Encrypt** your selection.  
Your selection is encrypted safely inside in your browser. At this point, you are not yet logged in: anyone can create an encrypted ballot and verify that it was encrypted correctly.
3. **Submit** your encrypted ballot.  
Authenticate and submit your encrypted ballot for tallying.

Start

## Helios Voting Booth

# LinuxTag 2010

Fingerprint: lqWpc8zsJ9KOz1o4R8mJxsp0uNM

**(1) Select**

(2) Encrypt

(3) Submit

(4) Done

### Question #1

---

*Which is your preferred location for LinuxTag 2010? (select 1 answer)*

- Berlin
- Karlsruhe
- Don't care

Review all Choices

# Encrypt Ballot

## Helios Voting Booth

# LinuxTag 2010

Fingerprint: lqWpc8zsJ9KOz1o4R8mJxsp0uNM

**(1) Select**

(2) Encrypt

(3) Submit

(4) Done

### Confirmation of your Choices

---

**Question #1 — Venue of LinuxTag 2010:**

Karlsruhe [\[update\]](#)

Encrypt Ballot

# Optionally Audit Ballot

**Helios Voting Booth**

## LinuxTag 2010

Fingerprint: **lqWpc8zsJ9KOz1o4R8mJxsp0uNM**

(1) Select	<b>(2) Encrypt</b>	(3) Submit	(4) Done
------------	--------------------	------------	----------

Your ballot has now been encrypted. Your ballot fingerprint is:

**zg027/r0oCzhG4BMpK8qwNK1JSI** [\[Your Receipt\]](#)

If you choose to submit this ballot, all plaintext information will be deleted from your browser's memory.

Submit Encrypted Ballot

Audit Ballot

# Documented Ballot Format

## Your audited ballot

You have chosen to audit your encrypted ballot.

Here is the fully audited ballot information, which you can copy and paste.

```
{ "answers": [{" choices": [{" alpha":
"33398817026391415638238481826354899256896707754747432902619289095584912133199095138510698167682285814575018704737
"beta"
"33587085857865267803259625055883321258940763281875716602924657831446573525495228262322482803154919202622112425610
"alpha"
"10585148594409549563588417140322568138013647588696255073414017466663780215674722252030977480568044925290029447682
"beta"
"13490506802361055980412103284909969381894532798109332284579603638072468752715576439670194100881231746142541172139
"alpha"
"83341242281020051056164560419292602564587257259663061159868267397995482006555639226207157538894534212524327897811
"beta"
"83014648049271414938336009798583537726387034233428600472041126214015011535482130325303196653253694144563530703467
"individual_proofs": [{" commitment": {" A":
"14972438579272447903639108466019967877948163188265751336298710490721522661775783836200166188520276117412139365893
"B"
"38365185885711149525990902056291735739689815800071593736606429139507938540809248328983052221016504456707723936053
"challenge"
"6138023295988014080583479272363859382377817691791566408784445976065113053086617484062958757224090738618745141781987
```

Copy the content above [\(select it\)](#).  
Visit the [Helios Ballot Verifier](#) to ensure it was properly formed.

**Go Back to Choices**

## Helios Single-Ballot Verifier

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

Your Ballot:

```
{ "answers": [ { "choices": [ { "alpha":  
"3339881702639141563823848182635489925689670775474743290261928909558491213319909  
"beta":  
"3358708585786526780325962505588332125894076328187571660292465783144657352549522  
{ "alpha":  
"1058514859440954956358841714032256813801364758869625507341401746666378021567472  
"beta":
```

**Verify**

election fingerprint is lqWpc8zsJ9KOz1o4R8mJxsp0uNM  
ballot fingerprint is zg027/r0oCzhG4BMpk8qwNK1JSI  
election fingerprint matches ballot  
Ballot Contents:  
Question #0 - Venue of LinuxTag 2010 : Karlsruhe  
Encryption Verified  
Proofs ok.



## Helios Voting Booth

# LinuxTag 2010

Fingerprint: `lqWpc8zsJ9KOz1o4R8mJxsp0uNM`

(1) Select

**(2) Encrypt**

(3) Submit

(4) Done

Your ballot has now been encrypted. Your ballot fingerprint is:

**6oAgbsjJSuhfhjHm4XNjWkVL6IO** [[Your Receipt](#)]

If you choose to submit this ballot, all plaintext information will be deleted from your browser's memory.

**Submit Encrypted Ballot**

You can choose to audit your ballot, which will show you how your options were encrypted. You will then have to re-seal your ballot if you wish to cast it.

**Audit Ballot**

## Helios Voting Booth

# LinuxTag 2010

Fingerprint: lqWpc8zsJ9KOz1o4R8mJxsp0uNM

(1) Select

(2) Encrypt

**(3) Submit**

(4) Done

### Submit Your Encrypted Ballot

Your encrypted ballot is ready for submission.  
All plaintext information has been removed from memory: all that remains is the encrypted vote.

Your encrypted vote fingerprint is:

**6oAgbsjJSuhfhjHm4XNjWkVL6IO**

To submit your encrypted vote, enter your login information below.  
(Notice how we only ask for your login once your ballot plaintext has been discarded.)

**IF YOU DO NOT HAVE YOUR ELECTION PASSWORD:** enter your email address in the email field, then click "get password", and wait a few seconds for a notification.

Email:  [\[get password\]](#)

Password:

## Helios Voting Booth

# LinuxTag 2010

Fingerprint: lqWpc8zsJ9KOz1o4R8mJxsp0uNM

(1) Select

(2) Encrypt

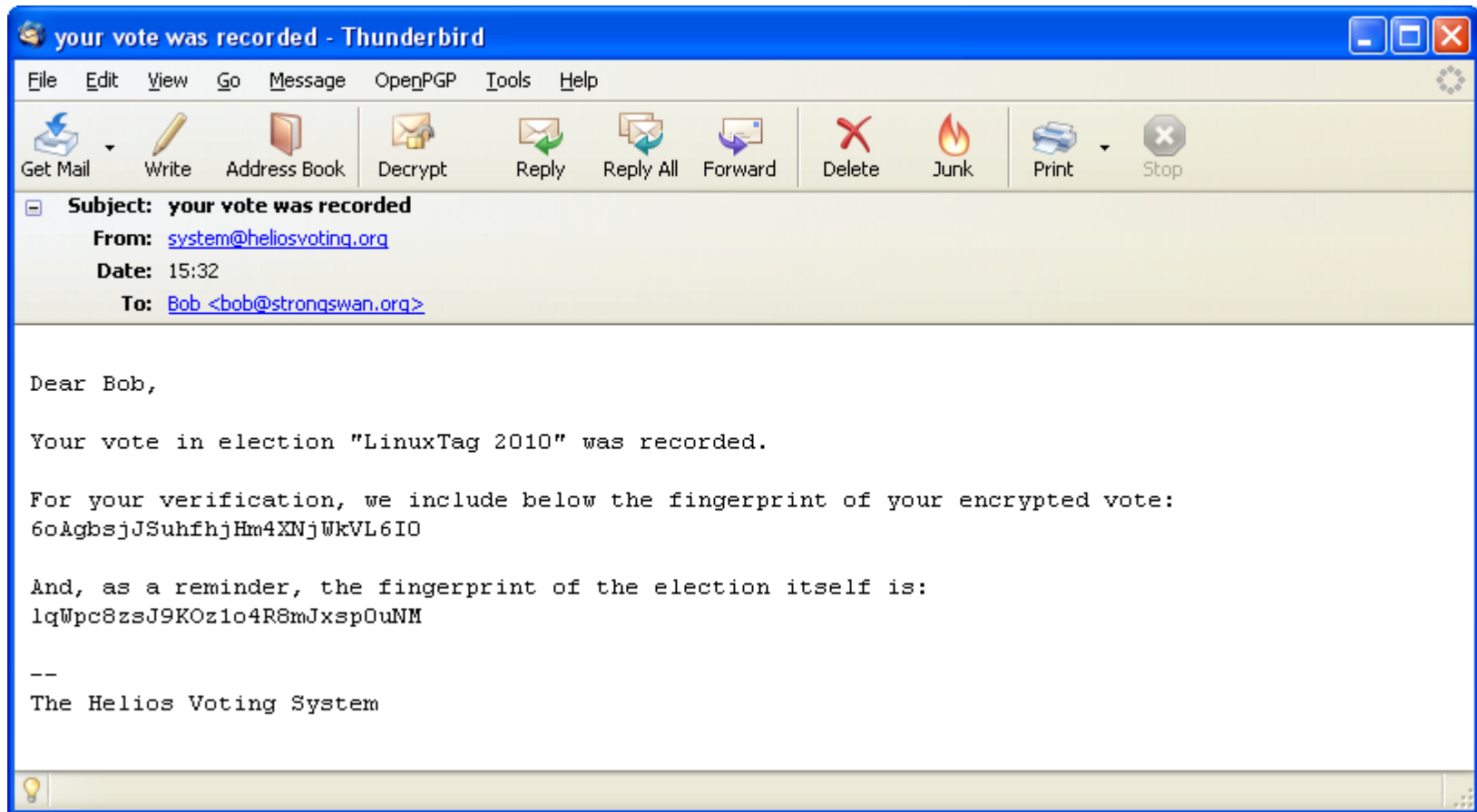
(3) Submit

**(4) Done**

### **Vote Submitted!**

Congratulations, your vote has been correctly submitted and recorded.

# Receipt per Email



## Helios Voting Elections you can audit

### LinuxTag 2010 — Bulletin Board [\[done\]](#)

#### Search

Voter Email:

Voters 1 - 20

Name	Ballot Fingerprint
Bob	6oAgbsjJSuhfhjHm4XNjWkVL6IO
Carol	kIkXXjAH21b0+B6tIqz8QUeGYig
Dave	h1LxcNC+Jz zaa4jsIkOIjcyq718
Alice	dI6n5yzY4jH3q1i/DEkgrpLbnQA

[\[Home\]](#) [\[My Elections\]](#) [\[Learn\]](#) [\[Blog/Updates\]](#)

All content on this site is licensed under a Creative Commons License.  
If you redistribute this content, you should give credit to Ben Adida and Harvard University.

## Helios Voting Elections you can audit

### LinuxTag 2010 -- Drive Tally

This page will drive the tallying process in chunks, from JavaScript.

0 tallied.

**Start Tally!**

---

[\[Home\]](#) [\[My Elections\]](#) [\[Learn\]](#) [\[Blog/Updates\]](#)

All content on this site is licensed under a Creative Commons License.  
If you redistribute this content, you should give credit to Ben Adida and Harvard University.

# Helios Voting

## Elections you can audit

### LinuxTag 2010

Election ID  
`agxoZWxpb3N2b3RpbmdyEAsSCEVsZWN0aW9uGJ2QBww`

Election Fingerprint  
`1qWpc8zsj9K0z1o4R8mJxsp0uNM`

[Vote in this election](#) [[Audit a Single Ballot](#)] [[Bulletin Board of Cast Votes](#)]  
(the tally has already been computed, but you can view the voting interface anyways.)


**Administration**

**Election Done**

- [voters](#)
- [archive election](#)

### Tally

**Venue of LinuxTag 2010:**

- Berlin: 1
- Karlsruhe: 2 
- Don't care: 1

[Audit the Election Tally](#)

# Public Audit of Voting Process

## Helios Election Verifier

Enter the Election ID:

J2b3RpbmdyEAsSCEVsZWN0aW9uGJ2QBww

start verification

Election: LinuxTag 2010  
Fingerprint: IqWpc8zsJ9KOz1o4R8mJxsp0uNM  
Voter - Bob - 6oAgbsjJSuhfhjHm4XNjWkVL6ID  
voter 0, ea 0, choice 0 -- VERIFIED  
voter 0, ea 0, choice 1 -- VERIFIED  
voter 0, ea 0, choice 2 -- VERIFIED  
voter 0, ea 0 OVERALL -- VERIFIED  
Voter - Carol - kIkXXjAH21b0+B6tlqz8QUeGYig  
voter 1, ea 0, choice 0 -- VERIFIED  
voter 1, ea 0, choice 1 -- VERIFIED  
voter 1, ea 0, choice 2 -- VERIFIED  
voter 1, ea 0 OVERALL -- VERIFIED  
Voter - Dave - h1LxcNC+Jzzaa4jslkOljcyq718  
voter 2, ea 0, choice 0 -- VERIFIED  
voter 2, ea 0, choice 1 -- VERIFIED  
voter 2, ea 0, choice 2 -- VERIFIED  
voter 2, ea 0 OVERALL -- VERIFIED  
Voter - Alice - dl6n5yzY4jh3q1i/DEkgrpLbnQA  
voter 3, ea 0, choice 0 -- VERIFIED  
voter 3, ea 0, choice 1 -- VERIFIED  
voter 3, ea 0, choice 2 -- VERIFIED  
voter 3, ea 0 OVERALL -- VERIFIED  
Question #0: Venue of LinuxTag 2010  
- Berlin - 1 -- VERIFIED  
- Karlsruhe - 2 -- VERIFIED  
- Don't care - 1 -- VERIFIED  
ELECTION VERIFIED!



- Modern Cryptographic Voting Systems allow true end-to-end verification of the whole voting process by anyone while maintaining a very high level of secrecy.
- Due to the advanced mathematical principles they are based on, Cryptographic Voting Systems are not easy to understand and are therefore not readily accepted by authorities and the electorate.
- But let's give Cryptographic Voting Systems a chance!  
They can give democracy a new meaning in the 21<sup>st</sup> century!

<http://security.hsr.ch/msevot/>