Usable Verifiable Remote Electronic Voting case study HELIOS

05.09.2012

Bern

Comments

- Based on research results from the project "Usable Verifiability in Remote Electronic Voting"
  - Project funded by MICROMATA Erfolg ist programmierbar!
  - Research conducted by M. Maina Olembo

- Assumptions:
  - voter cast vote from trustworthy environment
  - voter receives authentication tokens (PWD) over secure channel
- Focus on individual verifiability
  - Cast as intended

Overview

1. Why Helios and how Helios works?
2. Helios version 1.0 interfaces
3. Cognitive Walkthrough (KOKV2011)
    1. Findings
    2. Improved Interfaces
4. User study (KKOVV2011)
    1. Design
    2. Findings
5. Online survey
    1. Design
    2. Findings
6. Next steps

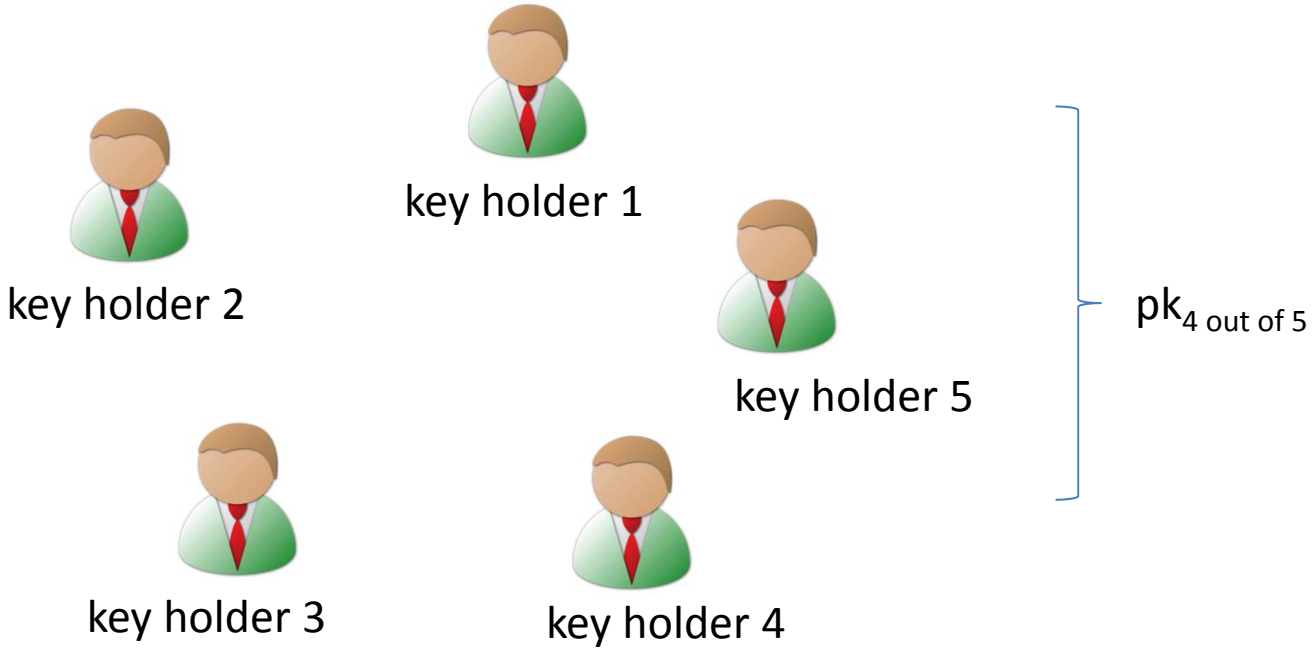
Why helios ?

- Proposed by Ben Adida in 2008: http://heliosvoting.org/

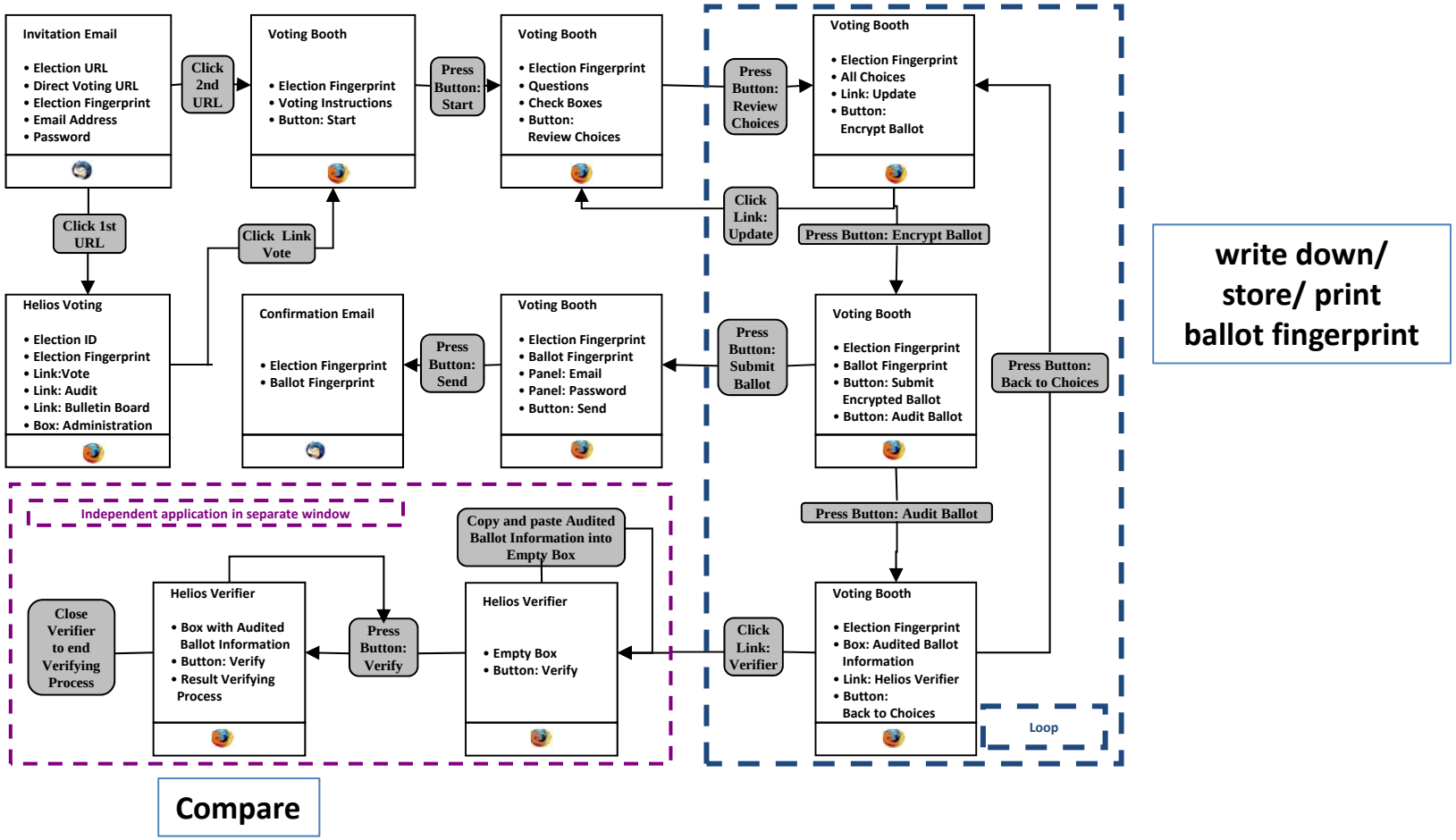
- Implemented verifiable electronic voting protocol
  - User interface
  - Open-source system
  - Well studied from security point of view

- Has been used in legally binding elections
  - in academic contexts: UCL, Princeton, IACR, …

How Helios works?



How Helios works?



Bulletin Board

Pseudonym/Voter's ID_1 - ballot $fingerprint_1$	
Pseudonym/Voter's ID_2 - ballot $fingerprint_2$	
…… …..	….
Pseudonym/Voter's ID_n - ballot $fingerprint_n$	

Important aspects

- Separation of vote preparation/encryption and vote casting
  → Everyone, including auditors or election observers can verify cast as intended

- Software commits to its encryption by displaying a hash of the ciphertext = ballot fingerprint
  → To ensure that the software provides the same ciphertext for verification and vote casting

Important aspects

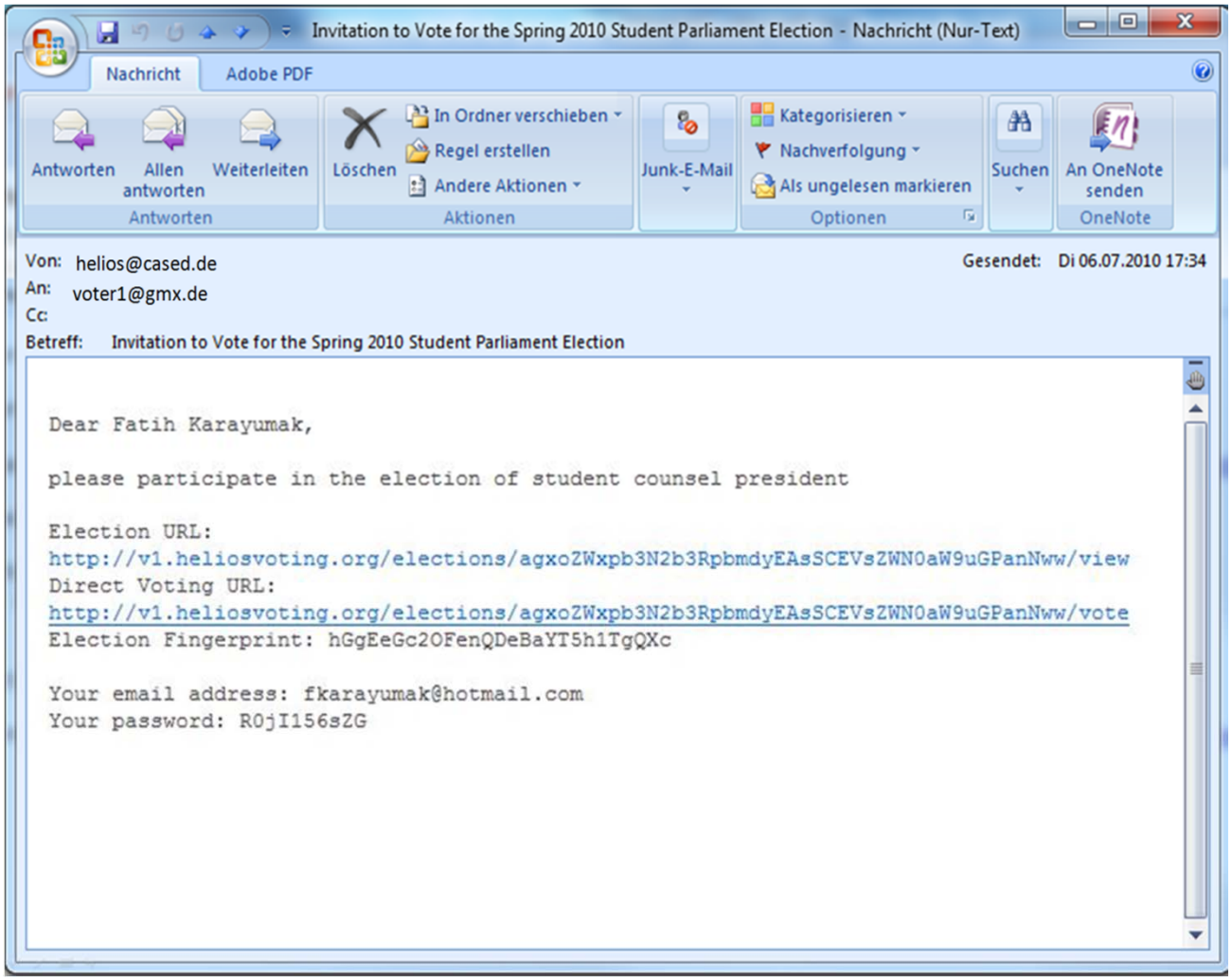
- Voter can verify as many (test) ballots as he/she wants
  → From the software's perspective, it cannot encrypt the wrong candidate with a sufficiently high probability of not being detected

- In order to ensure the secrecy of the vote, it is not possible to first verify and then cast this ballot but needs first to be re-encrypted
  → New ballot fingerprint

→ The voter cannot verify the encrypted ballot he finally casts but must trust the system due to previous checks.

Helios version 1.0

Helios version 1.0



Helios Voting

Elections you can audit

HELIOS-TEST

Election ID

agxoZWxpb3N2b3RpbmdyEAsSCEVsZWN0aW9uGPanNww

Election Fingerprint

hGgEeGc2OFenQDeBaYT5h1TgQXc

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]

Helios Voting Booth

HELIOS-TEST

Fingerprint: hGgEeGc2OFenQDeBaYT5h1TgQXc

(1) Select	(2) Encrypt	(3) Submit	(4) Done

Question #1

Please vote for the student counsel President. (select 1 answer)

- ☐ Rojan
- ☐ Melanie
- ☐ Fatih

Review all Choices

Helios Voting Booth

HELIOS-TEST

Fingerprint: hGgEeGc2OFenQDeBaYT5h1TgQXc

(1) Select	**(2) Encrypt**	(3) Submit	(4) Done

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

x0Q/CdXVBz7aTppOXhnLNg7qP3c [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

HELIOS-TEST

Fingerprint: hGgEeGc2OFenQDeBaYT5h1TgQXc

(1) Select	**(2) Encrypt**	(3) Submit	(4) Done

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":
"154335114613037429553266259127815799647940557730029411988543666967843119925275362141 2
"beta":
"119218028827576121325613754800910662880768788967973296125221846908150510426045429638 1
{"alpha":
"887461990616747633067301532435345531901542071982455046954622419547209597187651251376 8
"beta":
"295107140736624140854454666232741249374203948868977661423739419392384197411513633410 4
{"alpha":
"675301388412484813862572623899504421022221816231983514071656764092923227720659831952 2
"beta":
"623106292468999097348695236456325525563488406665053522212505204496521676294092467177 8
"individual_proofs": [[{"commitment": {"A":
"107594923803544242715367125986219432824657322767006152324733808985542956232870659263 6
```


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:

Verify

Cognitive Walkthrough [KOKV11]

Cognitive Walkthrough [KOKV11]

- Carried out on Helios version 1.0 and later on version 3.0
  - Interfaces evaluated from voter perspective
    - How usable is it to cast and verify a vote?
  - Five experts from security, e-voting and psychology
  - Fictitious university president election

Helios Voting Booth

HELIOS-TEST

Fingerprint: hGgEeGc2OFenQDeBaYT5h1TgQXc

(1) Select	**(2) Encrypt**	(3) Submit	(4) Done

?

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

O/0?

x0Q/CdXVBz7aTppOXhnLNg7qP3c [Your Receipt] ?

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

might be scary

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

What to do with the ballot fingerprint / receipt

Helios Voting Booth

HELIOS-TEST

Fingerprint: hGgEeGc2OFenQDeBaYT5h1TgQXc

(1) Select	**(2) Encrypt**	(3) Submit	(4) Done

Your audited ballot

You have chosen to audit your encrypted ballot.

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


```
{"answers": [{"choices": [{"alpha":
"154335114613037429553266259127815799647940557730029411988543666967843119925275362141 2
"beta":
"119218028827576121325613754800910662880768788967973296125221846908150510426045429638 1
{"alpha":
"887461990616747633067301532435345531901542071982455046954622419547209597187651251376 8
"beta":
"295107140736624140854454666232741249374203948868977661423739419392384197411513633410 4
{"alpha":
"675301388412484813862572623899504421022221816231983514071656764092923227720659831952 2
"beta":
"623106292468999097348695236456325525563488406665053522212505204496521676294092467177 8
"individual_proofs": [[{"commitment": {"A":
"107594923803544242715367125986219432824657322767006152324733808985542956232870659263 6
```


Copy the content above (select it). **verify/audit?**

Visit the Helios Ballot Verifier to ensure it was properly formed. **“ … how your options where encrypted”?**

Go Back to Choices

How to continue verifying / casting a ballot?

Independent?

Helios Single-Ballot Verifier

?

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

" … how your options where encrypted"?

?

Your Ballot:


```
006712190928293017047440634447262736047991277694199450337485661566689235360569 13
4442442824281698421546839630079113268065712569927707179379719877358 98",
"677610752156231266512845281272893852118882219443381748263925243963207846931541 0
4442917434395735226242591227515186733652047720551500045504467899728973220500412 3
6794544977691859939761241502815692582971527426022755524565634189069056977262092 7
3435943103478165202228566875551519542918487511576517122629647634043 16"]}],
"election_hash": "hGgEeGc2OFenQDeBaYT5h1TgQXc", "election_id":
"agxoZWxpb3N2b3RpbmdyEAsSCEVsZWN0aW9uGPanNww"}
```


C&P is error prone

Verify

election fingerprint is hGgEeGc2OFenQDeBaYT5h1TgQXc
ballot fingerprint is x0Q/CdXVBz7aTppOXhnLNg7qP3c
election fingerprint matches ballot
Ballot Contents:
Question #0 - President? : Rojan
Encryption Verified
Proofs ok.

how to continue?/
vote cast?

anything to verify? what to do if it does not match?

Cognitive Walkthrough [KOKV11]

- Carried out on Helios version 1.0 and later on version **3.0**
  - Interfaces evaluated from voter perspective
    - How usable is it to cast and verify a vote?
  - Five experts from security, e-voting and psychology
  - Fictitious university president election

Helios Voting Booth [exit]

Presidential Election of University

Presidential Election of University

(1) Select	(2) Encrypt	(3) Submit

Review your Ballot

Question #1: Please vote for the new president of University.

Prof. Zaphod Beeblebrox [update] ?

Confirm Choices and Encrypt Ballot

Election Fingerprint: **2IsihDEFZKjeXk//Ip2vdgYGNcpDq1x4fig3F/Z2Fc4** help!

Helios Voting Booth [exit]

Presidential Election of University

Presidential Election of Univers

(1) Select | (2) Encrypt | (3)

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.

Your ballot was successfully encrypted

! ? Missing instruction: comparison

Please **keep a record** of your smart ballot tracker [print] [email]:

CqnEYxjq44rk+U6h+feiYnQsVvI2IF/JsxlQsQhJa44

To protect your privacy: new: trust?

- Helios has not yet asked for your identity.
- Once you click "Proceed", Helios will remember only your encrypted vote.
- Thus, only you know your vote.

Proceed to Cast

Audit [optional]

If you choose, you can audit your ballot and reveal how your choices were encrypted.

You will then be guided to re-encrypt your choices for final casting.

Verify Encryption

Election Fingerprint: **2IsihDEFZKjeXk//Ip2vdgYGNcpDq1x4fig3F/Z2Fc4** help!

Helios Voting Booth [exit]

Presidential Election of University

Presidential Election of University

(1) Select | (2) Encrypt | **(3) Submit**

Your audited ballot

?

IMPORTANT: this ballot, now that it has been audited, *will not be tallied*.
To cast a ballot, you must click the "Back to Voting" button below, re-encrypt it, and choose "cast" instead of "audit."

Why? Helios prevents you from auditing and casting the same ballot to provide you with some protection against coercion.

?

Now what? Select your ballot audit info, copy it to your clipboard, then use the ballot verifier to verify it. new
Once you're satisfied, click the "back to voting" button to re-encrypt and cast your ballot.

? verify again?


```
{"answers": [{"choices": [{"alpha":
"215514226200839244919396721584348982099528536696983252874004045570107717097088 0
070842305883706282126475183471422680410325734813243743999099311166479344875227 04
237181864010344076761147322819413796788408672991511068643166210220420531239907 68
183902741575060518627343050422617724337155782153820408110448977890196481353313 22
518979743651083812082983897425903763892191457261132734143886960501909961748517 54
010997571252399522540810295802171956706017574177034975933970480808947172541920 23
838138434900116572791632684593193872370801399769513732887286621617996765167781 21
936703524904932161872693756883591824772226260640998170282", "beta":
"840795688665352843558387189898176361360374454870018552224018322413990188905733 4
966197233785940566829643932744390020625685039976099778254211938527813435167834 20
```


Before going back to voting,
?
you can post this audited ballot to the Helios tracking center so that others might double-check the verification of this ballot.

Even if you post your audited ballot, you must go back to voting and choose "cast" if you want your vote to count.

post audited ballot to tracking center | back to voting

Election Fingerprint: **2IsihDEFZKjeXk//Ip2vdgYGNcpDq1x4fig3F/Z2Fc4** help!

Independent?

Helios Single-Ballot Verifier

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

Enter the Election URL: /helios/elections/e355bcd2-6054-11e0-96ef-12313f0 ?

Your Ballot:


```
{"answers": [{"choices": [{"alpha":
"215514226200839244919396721584348982099528536696983252874004045570107717097088 0
0708423058837062821264751834714226804103257348132437439990993111664793448752270 4
2371818640103440767611473228194137967884086729915110686431662102204205312399076 8
1839027415750605186273430504226177243371557821538204081104489778901964813533132 2
5189797436510838120829838974259037638921914572611327341438869605019099617485175 4
0109975712523995225408102958021719567060175741770349759339704808089471725419202 3
8381384349001165727916326845931938723708013997695137328872866216179967651677812 1
```


Verify

loading election...
election fingerprint is 2IsihDEFZKjeXk//Ip2vdgYGNcpDq1x4fig3F/Z2Fc4
smart ballot tracker is CqnEYxjq44rk+U6h+feiYnQsVvl2IF/JsxlQsQhJa44
election fingerprint matches ballot
Ballot Contents:
Question #1 - Please vote for the new president of University. : Prof. Zaphod Beeblebrox
Encryption Verified
Proofs ok.

SUCCESSFUL VERIFICATION, DONE! **even worse!**

Findings

Missing: clear terminology and clear instructions

Complicate (many steps) and error prone verifiability

Same design for verification and main voting interface

Irritation to authenticate at the end of the voting process

Improved Interfaces (1)

Dear ...

You are registered on the electoral roll. For this election you will use a secure online voting system that uses verification codes. These codes will help you understand the correctness of this election.
You can vote on the election web-page www.election.university.com on 27 March 2011 between 9:00 a.m. and 6:00 p.m. Here you can also get further information about the execution of this election.
To check your eligibility to vote, you will be required to authenticate yourself with a username and a password.

Your username: <User-Name>
Your password: <Password>

Please don't share this information with anyone.

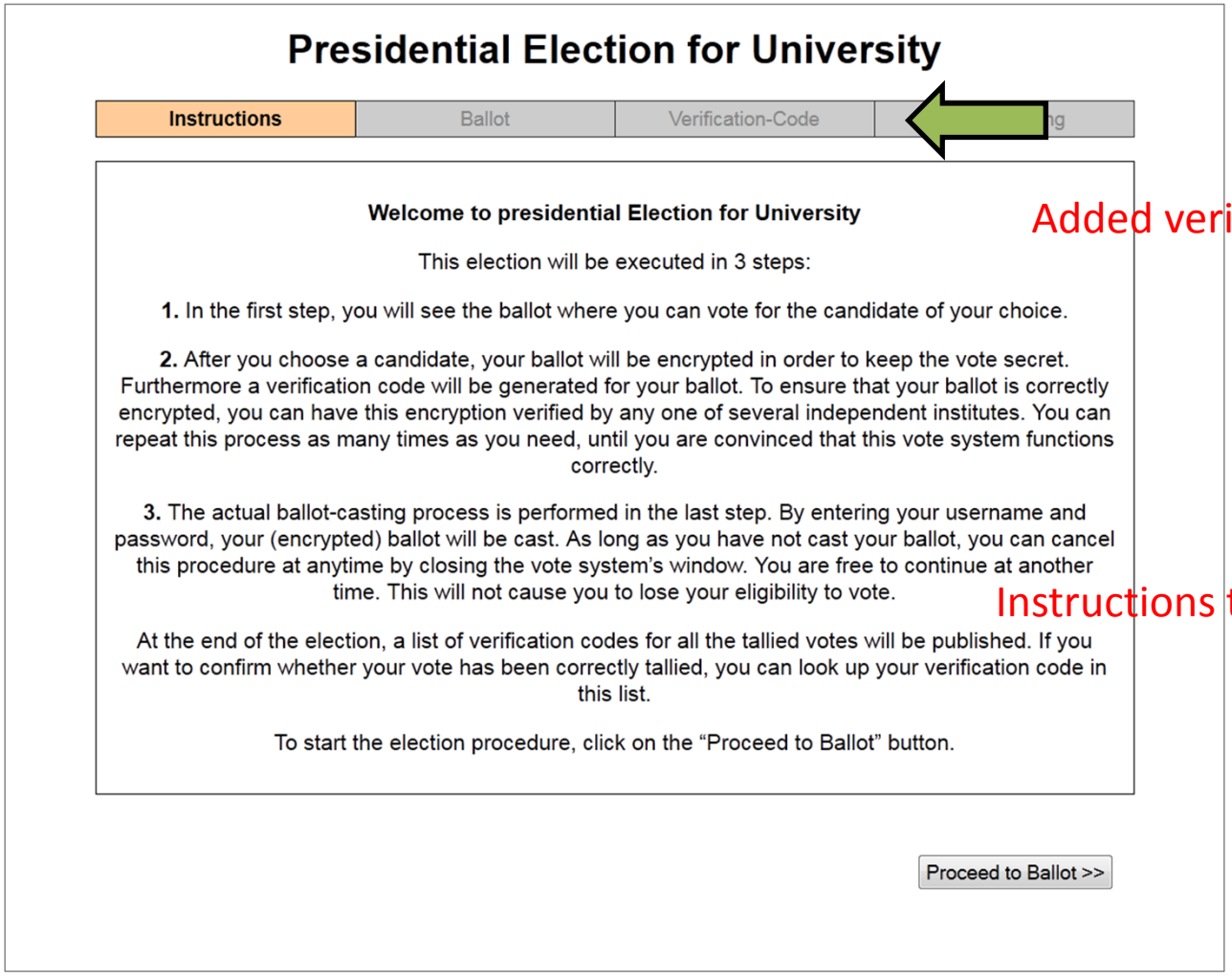
Best Regards
Election Officer

Clear instructions

SHA1-Fingerprint:	95:C3:19:DF:FF:93:F4:49:EB:C6:80:92:F6:E0:78:DF:22:A4:06:35
MD5-Fingerprint:	40:ED:BF:B6:76:B6:5A:AE:43:B2:FD:6C:C4:AF:44:76

To authenticate servers

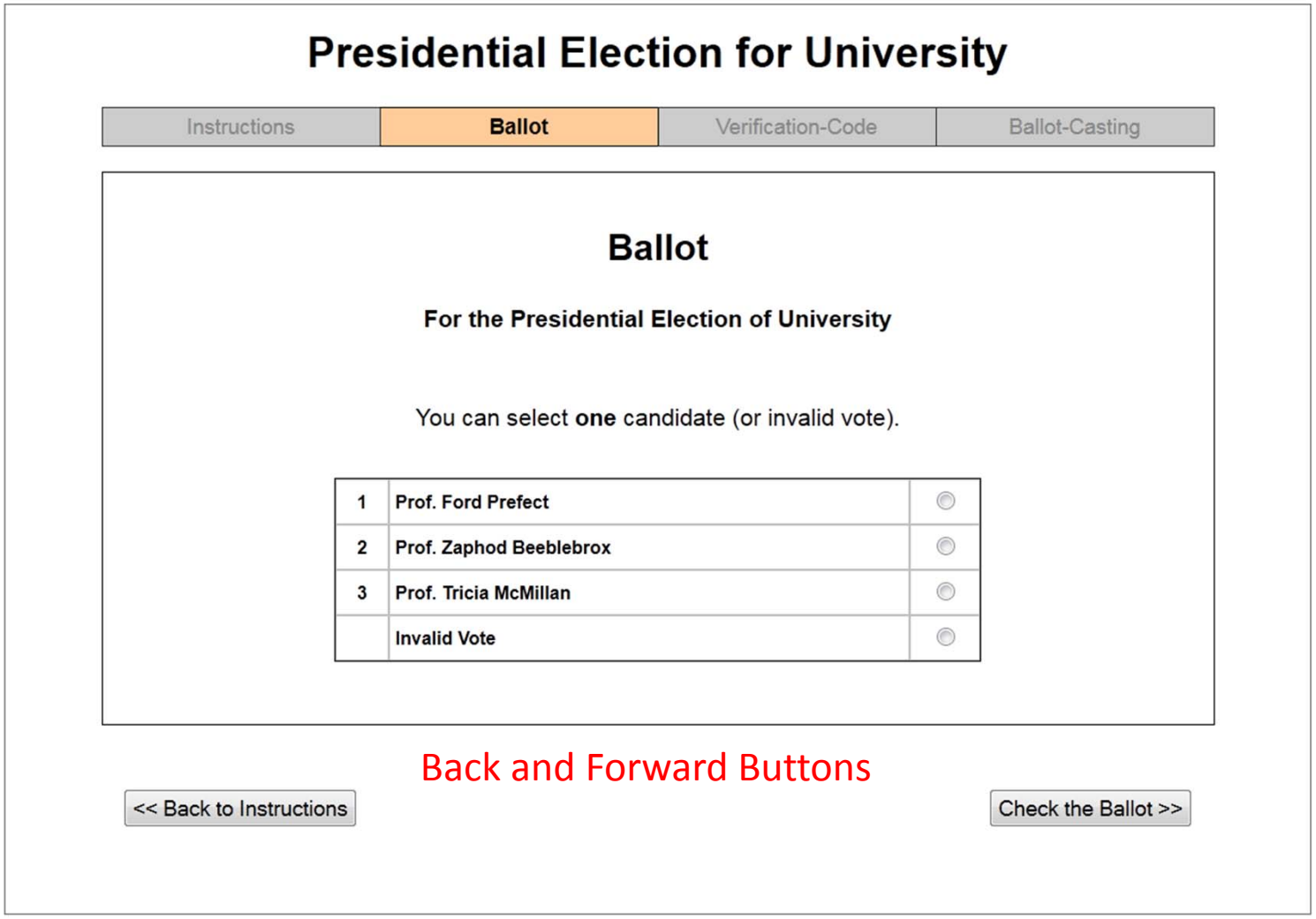
Improved Interfaces (2)



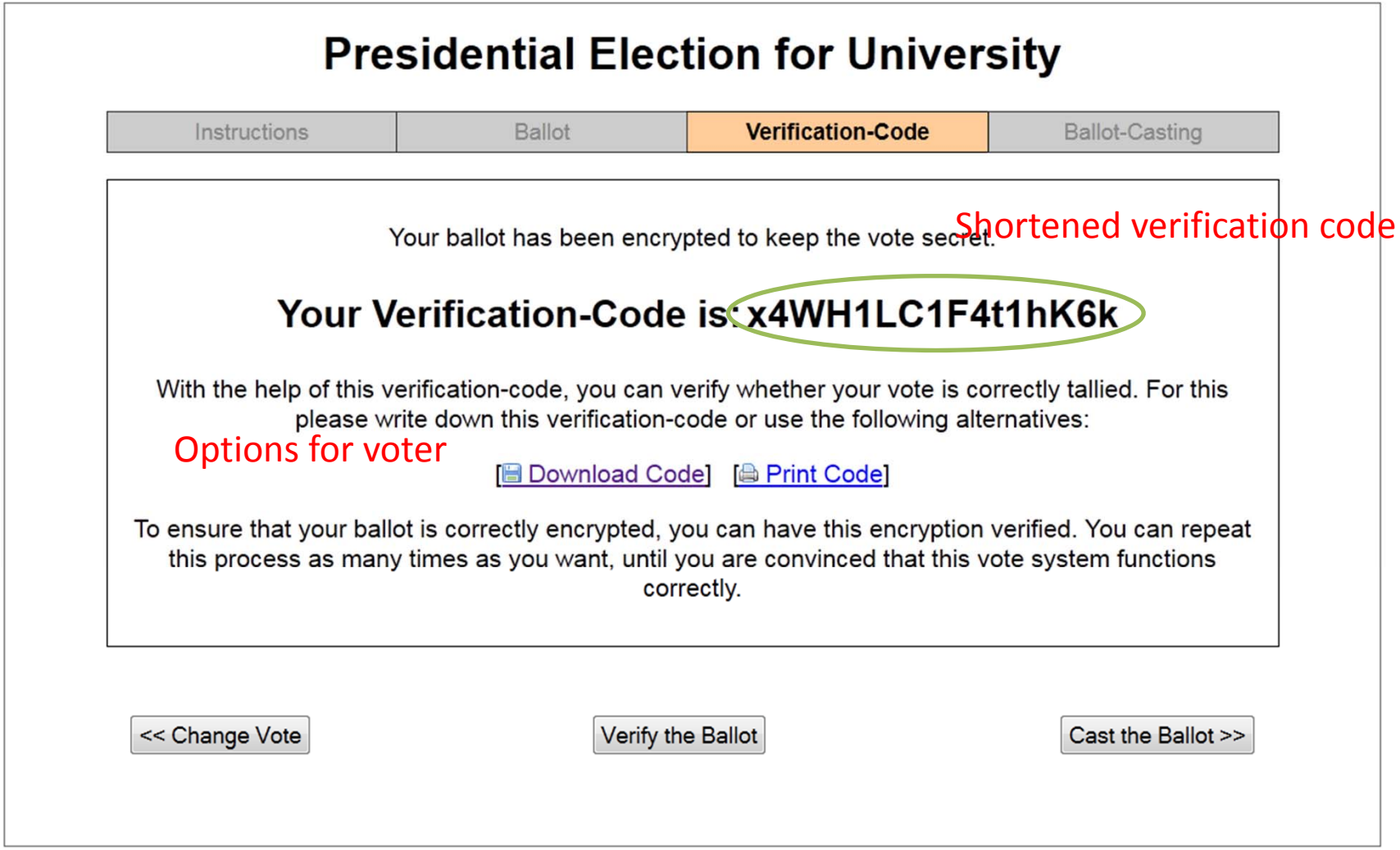
Added verifiability step

Instructions to voters

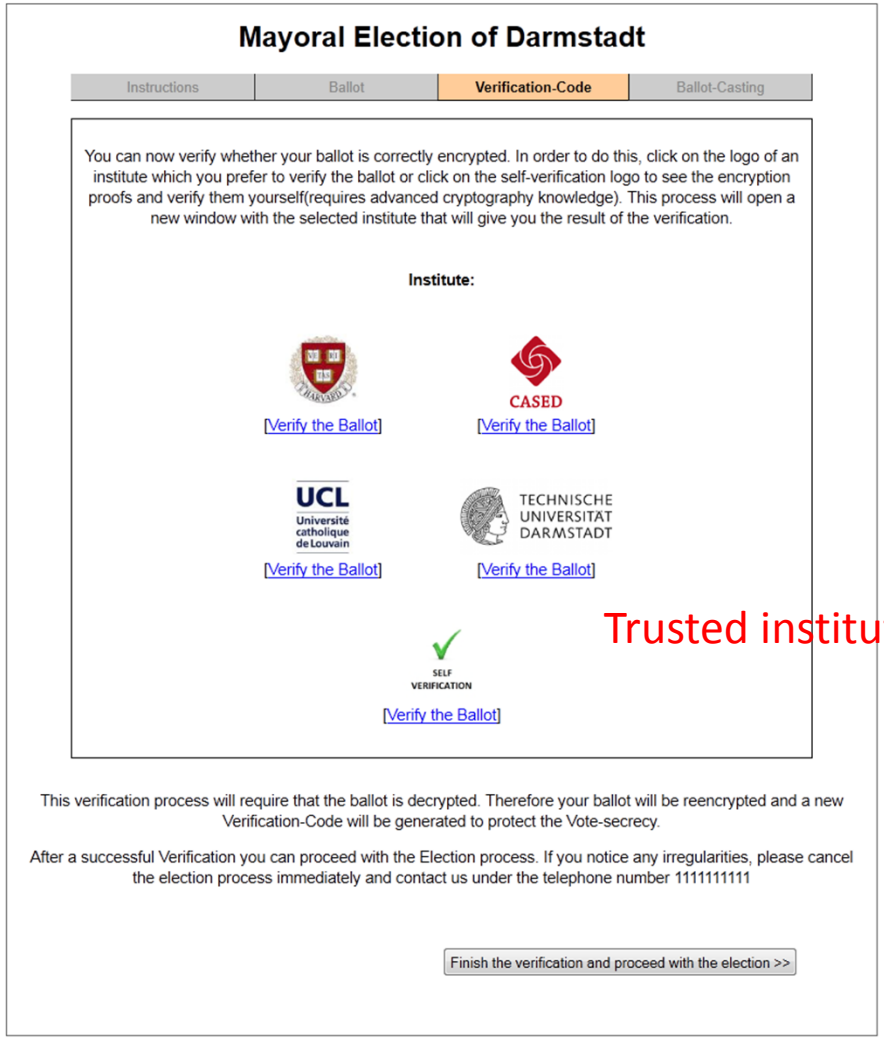
Improved Interfaces (3)



Improved Interfaces (4)

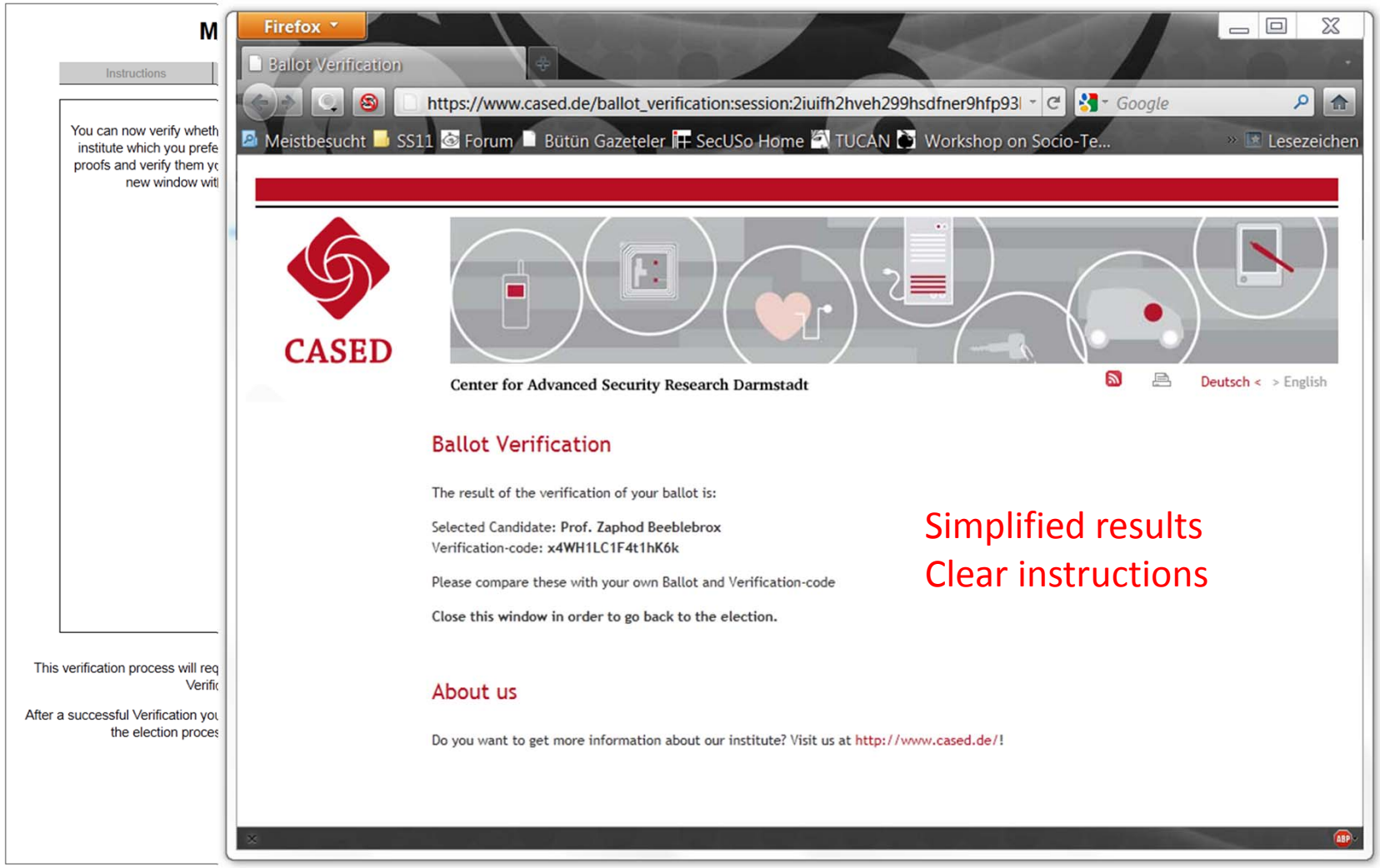


Improved Interfaces (5)



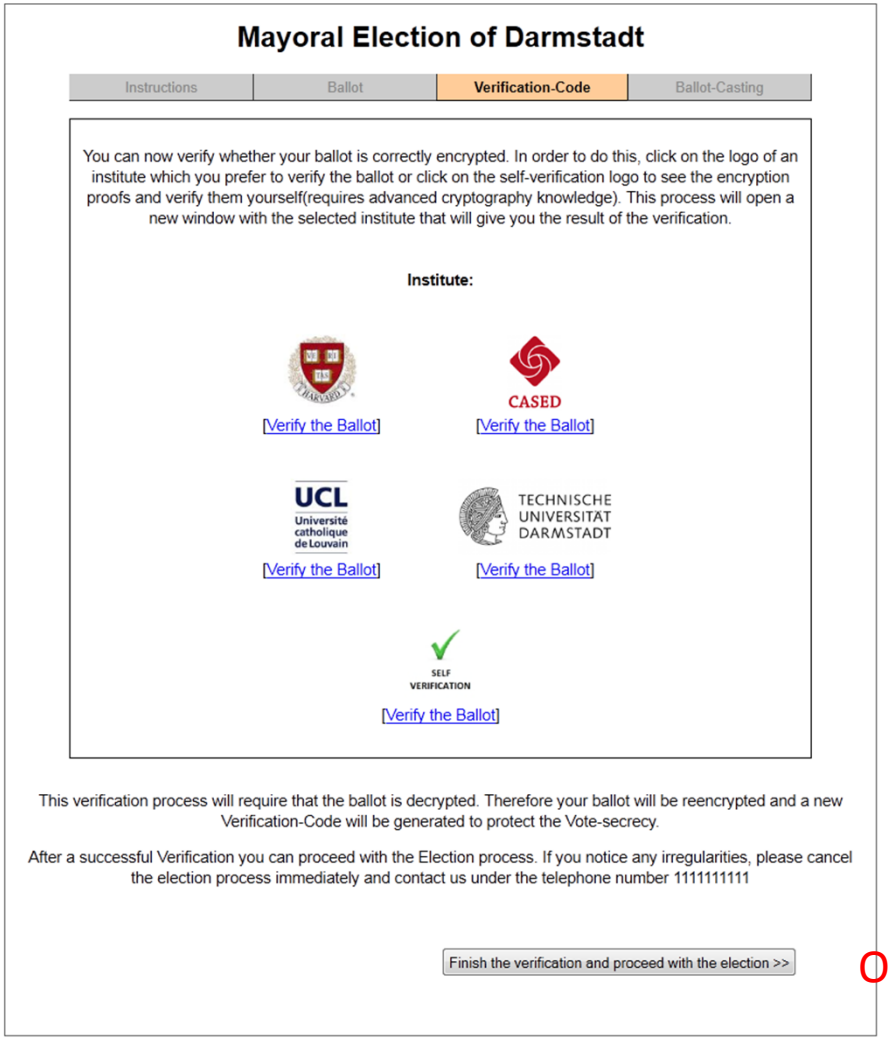
Trusted institutions for verification

Improved Interfaces (6)



Simplified results
Clear instructions

Improved Interfaces (5)

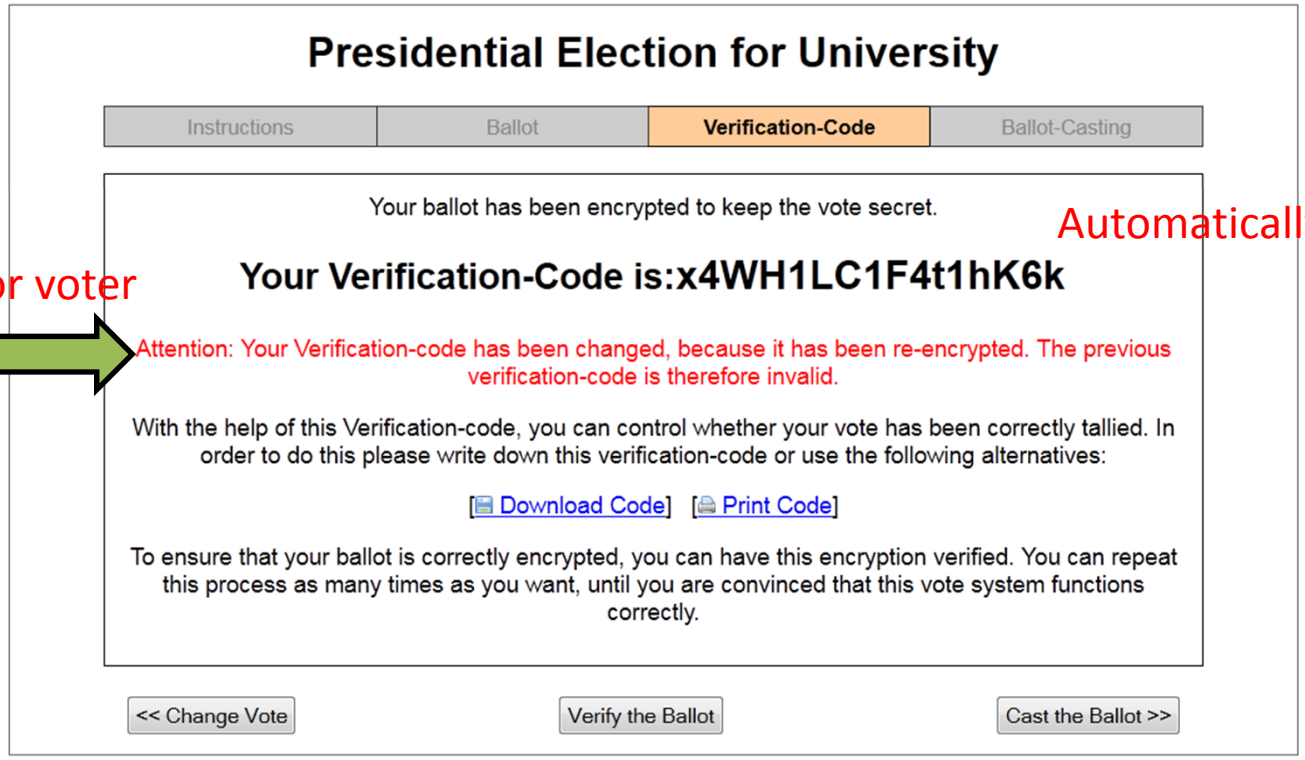


Only button

Improved Interfaces (7)

Explanation for voter

Automatically re-encrypted



Comparison

Old	New
Click Audit (Drops down to give more information)	
Click Verify Encryption	Click verify the ballot
Click link to select information	
Right-click and copy	
Click Ballot Verifier link	Click on verifying institute
Paste information in ballot verifier window	
Click Verify	
Close window	Click close window (as in PPT)
Click Back to Voting	Click enter new vote button (as in PPT)
Click Confirm button to re-encrypt or Update to change vote	[automatic]

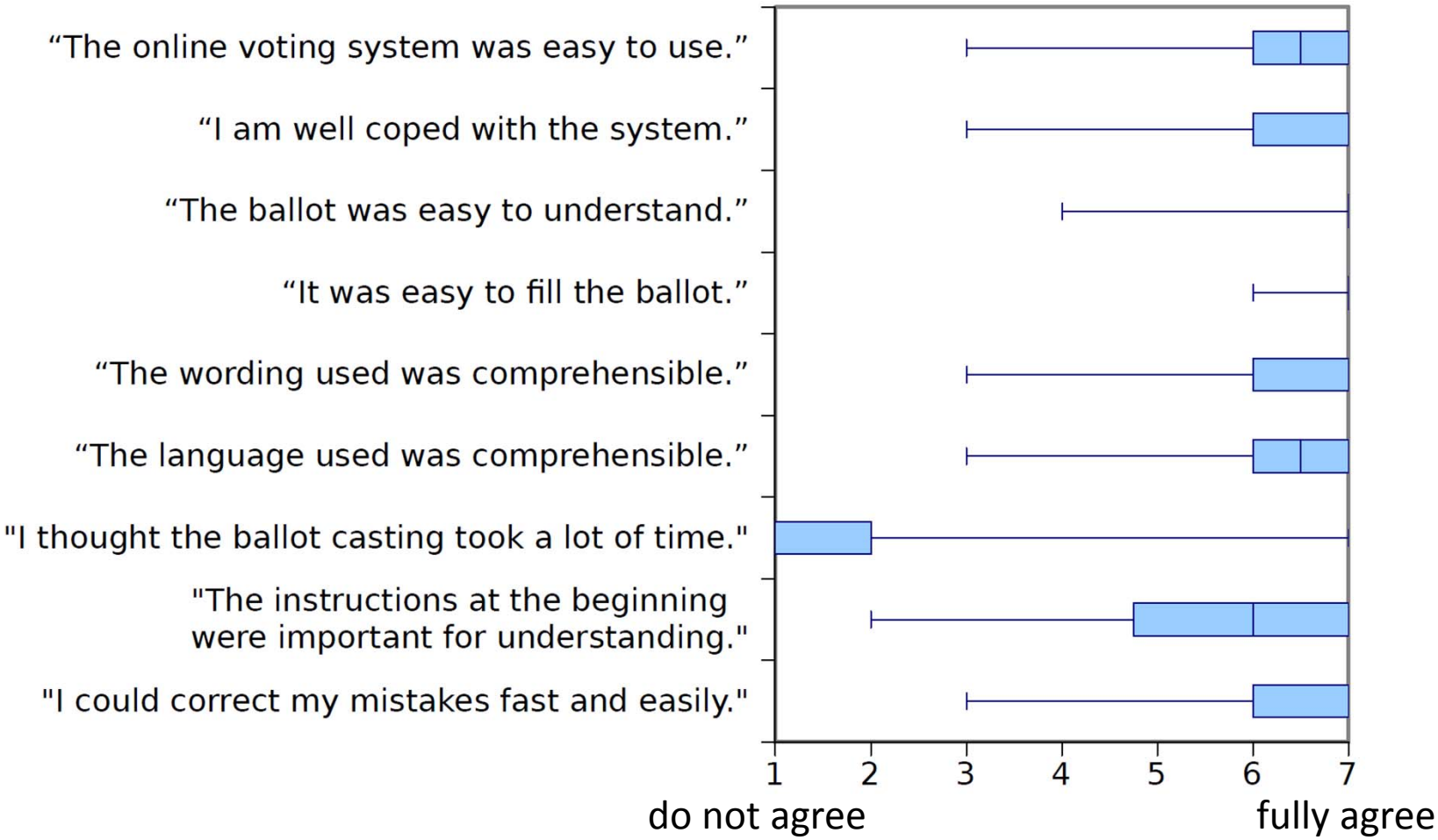
User Study [KKOVV2011]

Design of the user study (lab study)

- Mock mayoral election in Darmstadt
- Material/Interface in German
- 34 participants
- Asked to put on a modified bicycle helmet with a video camera and eye-tracking
- Participants cast a vote w/o instructions (2 rounds)
  - Would people verify? How?
  - Can people verify if we tell them to do so?
  - Instructions emphasized verifying with different techniques, different votes
- 3 questionnaires

Note: hard for participants to take it serious as it is not a secret election due to eye tracker and log files

General Usability (after round 1)



General Usability

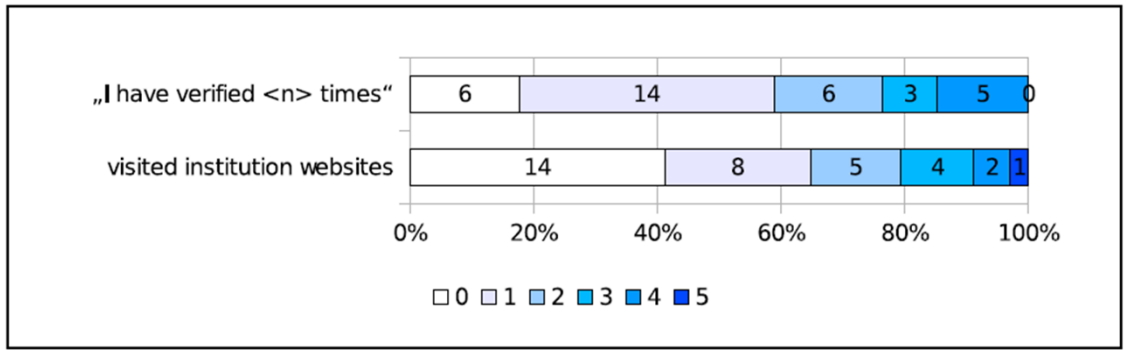
- 1 of 20 who answered that they verified further stated not having noticed that the code changed (round 1)
- 1 of the remaining 14 stated this in round 2

→Most of participates noticed it

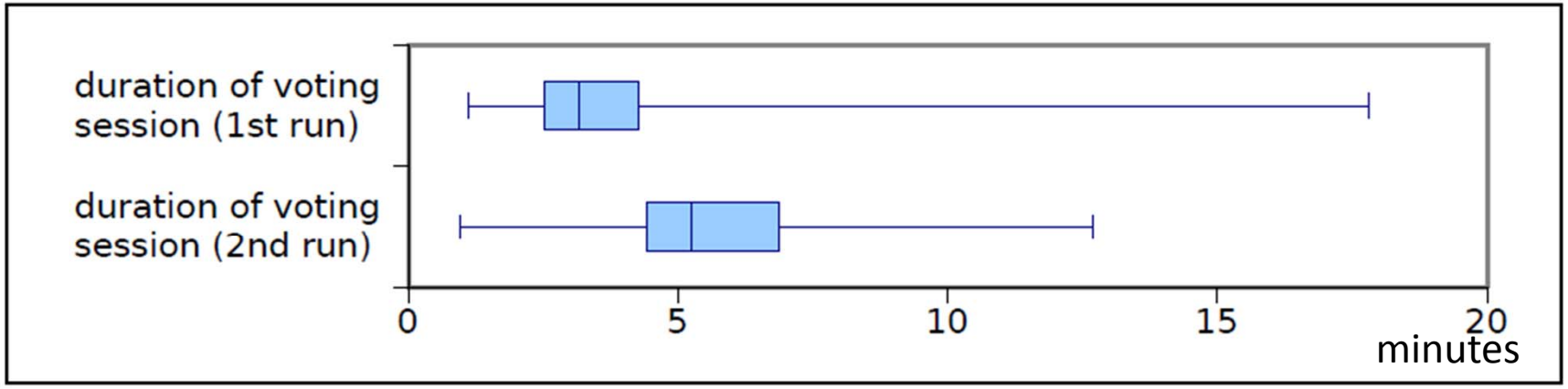
- After round 2
  - 8 of 34 participants stated that it was not clear to them that they had to compare the verification codes or/and the candidates
  - All stated that it was clear to them that their vote was not cast after having verified

How many people verified?

- 20 of 34 participants (58%) verified in the **first** run (log files)
  - 10 with technical background verified
  - 10 without technical background verified
  - → No correlation between technical background and interest in verifying
  - All did some comparison, some only very quick (eye tracking)
- 28 of 34 (82%) claimed to have verified at least once
  - Some participants confused "verifying" with double checking that their ballot was correctly filled.
  - 2 went to the verification page but then back without having verifieid



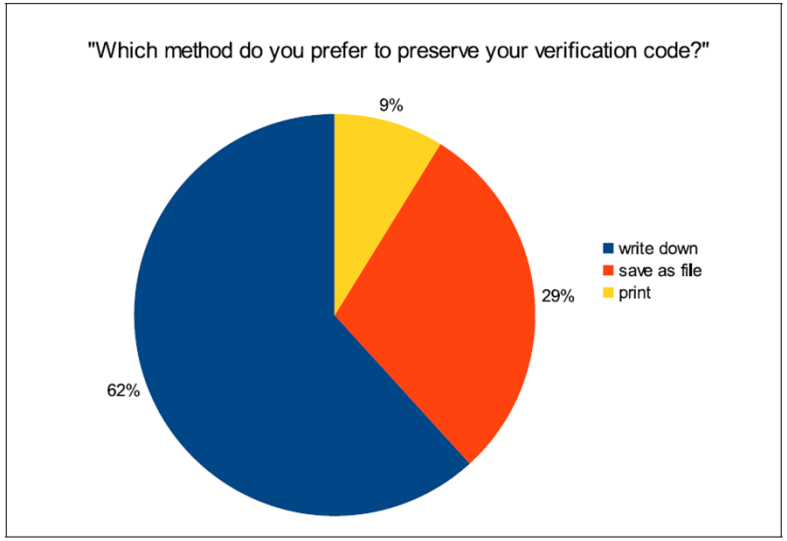
Duration for vote casting



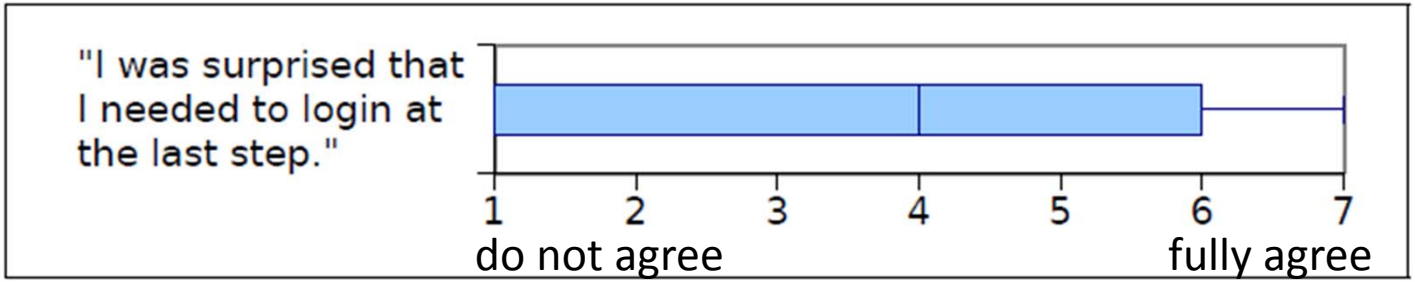
From enter URL/ press enter and cast vote / entered correct credentials

Preferred method of verification of the security code

- Round 1:
  - 17 wrote down, 9 saved, 4 printed
  - none compared with displayed commitment if printed or stored



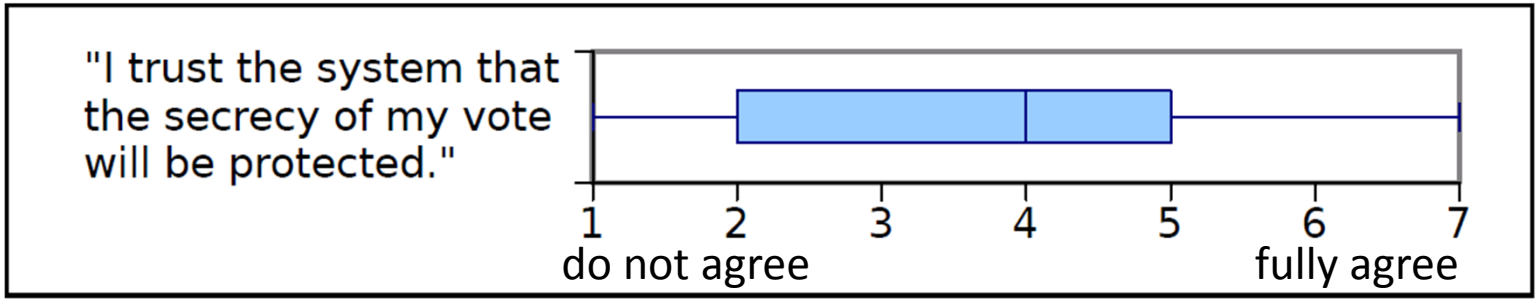
Is the authentication at the end of the voting process irritating?



Do people have enough information to properly verify and cast their vote?

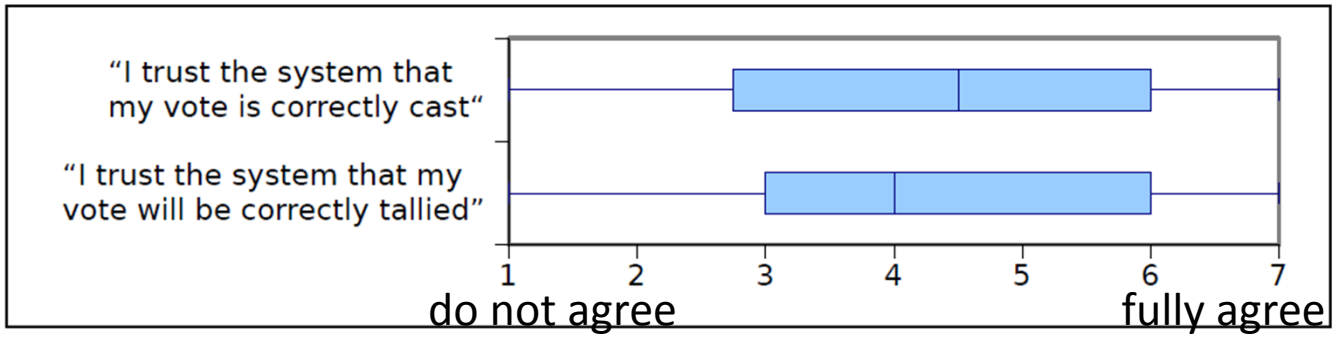
- 16 of 34 participants (47%): not enough information
  - Participants without technical background complained that the first page (with the instructions) contained too much information at once (some didn't even read it)
  - Participants with technical background wanted more information about the security of the system (papers, security proofs, statements from other institutions regarding the level of security etc.)
- 31 of 34 participants (91%): concept of verifiability needs to be introduced before using this kind of voting system

Trust regarding ballot secrecy



- Concerns about their vote secrecy….
  - "The institutions can see my vote!" "… but they have strong privacy policies"
  - "derive vote from verification code is possible for institutes for whom else?
  - 26 participants (76%) answered that they were irritated by the changing verification code
  - 2 out of 20 in first round modified vote after having verified
- Possible reason
  - Idea behind re-encrypting the ballot after verification unclear
  - Concept of test vote unclear

Trust in correct vote casting & tallying



- Participants were not able to verify the proper tallying at all
  → Trust level in the proper tallying was expected to be lower than in correct vote casting
- Possible reason: People were not aware that these are two different concepts

General comments

- “Normal people will find it too complicated.” (with technical background)
- “Good to know it is encrypted” (without technical background)

- “Got confused with the different verification codes”
- “Writing down a new security code each time annoys me.”

- “I do not understand the idea behind the verification code”
- “Why should I trust the verification procedure if I should not trust the voting system”

Findings

- Most people are able to verify (at least with quick check)
- People do not get the idea of test ballots to verify
- People do not understand what they can verify and what not

Online survey

- Carried out to identify voters' mental model of verifiability
  - Are voters aware of verifiability?
  - Do they see a need to verify their votes?
  - Are there factors that are more likely to cause voters to verify?
  - What terminology is adequate to communicate verifiability to voters?

- In Kenya and Germany
  - Kenya: no postal voting, not possible to observe
  - Germany: 30% postal voting, possible to observe

Design

- Interviews carried out as a pre-test
- Refined online questionnaire

Figure 1: First Picture

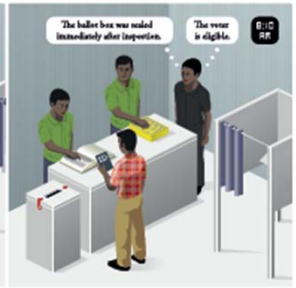


Figure 2: Second Picture

Figure 3: Third Picture

Figure 4: Fourth Picture

Figure 5: Fifth Picture

Figure 6: Sixth Picture

First Findings

- More familiar with aspects of universal verifiability
  - Match number of voters to votes cast
  - Re-count
- Not as familiar with aspects of individual verifiability
  - Seals at ballot boxes to ensure that they are not opened
  - Concerned about secrecy of the vote
- General verifiability findings
  - Some prefer delegating responsibility of verifying to others
  - More likely to verify with Internet voting than with paper based voting but only with first elections
  - Verify if unexpected result (mentioned re-count)
  - No need for traditional paper based elections because of trust in people who they know
- More familiar terms than verifiability
  - Monitor, observe

Next Steps

- Improve usability of hash value
  - Represent hash value graphically
  - Identify secure enough length for hash value
  - Analyze what are people willing to compare
- Explain concept of “test” votes better
- Changes to interface based on results
  - Adopt wording
  - Number for each hash value
  - Go back to empty ballot
  - Only ‘write down’ option
  - Distribute receipt for ‘stored as cast’ verifiability
  - Use QR code and Android app for comparison

https://www.presidentelection.university.com

UNIVERSITY PRESIDENT ELECTION

Instructions	Ballot	Verification-Code	Vote-Casting

You can now verify whether your ballot is correctly encrypted.

Click on the logo of your choice. A new window will open with the results of the verification.

Institutes:

[Verify the Ballot]

[Verify the Ballot]

[Verify the Ballot]

[Verify the Ballot]

[Verify the Ballot]

Trust in verification device or voting environment enough

In order to verify your vote, the ballot will be decrypted. Once the process is finalized, your vote will be re-encrypted and a new verification-code generated.

You can continue with the voting process upon successful verification. If you notice any irregularities, cancel the election process immediately and contact the election officials [Telephone number: 123456789]

Enter a new vote to proceed with the election

Open Discussion

- Currently: some cumbersome steps for the voter
  - Check https for voting page
  - For each verified vote:
    - Write down hash value and compare with verification page of institute(s)
    - Check https for institute's page
  - For casting: Write down hash value and compare on board
  - In addition: check on bulletin board

- Alternative: vote casting from different trusted institutions
  - Check https for voting page
  - Could forward ballot fingerprint to delegate 'stored as cast' verification

- Combination?

Questions?

Literature

Helios voting system: Adida, B. 2008. Web-based open audit voting. In Proceedings of the 17th symposium on security, pp. 335–348. Berkeley, CA, USA: USENIX Association.

[KOKV11] Usability Analysis of Helios - An Open Source Verifiable Remote Electronic Voting System by Fatih Karayumak, Maina M. Olembo, Michaela Kauer, Melanie Volkamer. In: *Proceedings of the Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE)*, 2011.

[KKOVV11] User Study of the Improved Helios Voting System Interface by Fatih Karayumak, Michaela Kauer, Maina M. Olembo, Tobias Volk, Melanie Volkamer. In: *Socio-Technical Aspects in Security and Trust (STAST), 2011 1st Workshop on* , p. 37-44, IEEE Digital Library, 2011. ISBN 1-4577-1181-7.

[SN93] Mental models: Concepts for human computer interaction research by STAGGERS, N., AND NORGIO, A. F. Int. J. Man-Machine Studies 38, 4 (1993), 587 605.