

Usability of Verifiability in Helios



Maina Olembo, Fatih Karayumak, Michaela Kauer, Melanie Volkamer

8th August, 2011



Overview



-
- Why usability of verifiability in remote EVoting

 - Review of Helios
 - Vote Casting Process
 - Sample Interfaces

 - Improving Helios Interfaces
 - Cognitive Walkthrough
 - Improved Interfaces
 - User Study

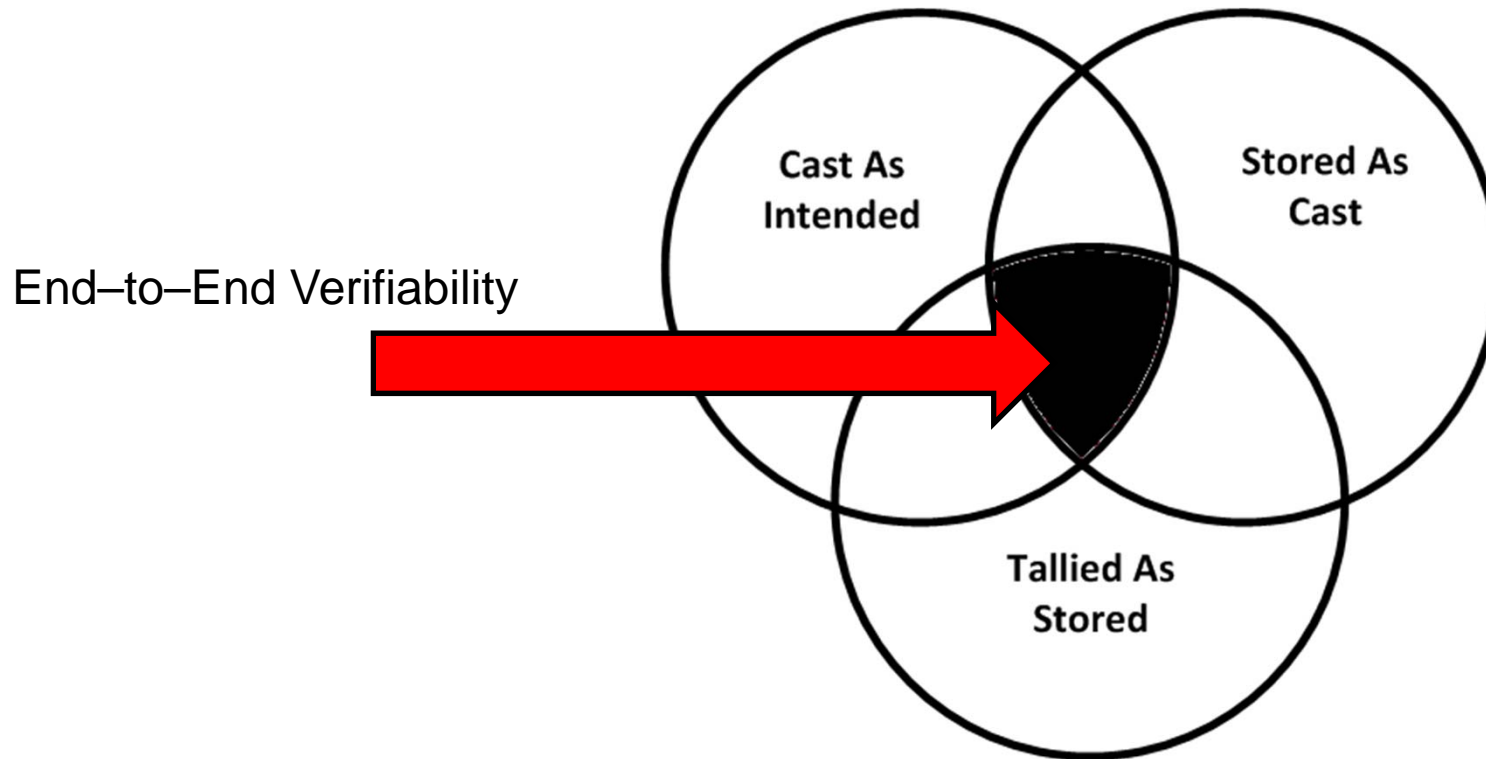
 - Future Work and Conclusion

Overview



-
- **Why usability of verifiability in remote EVoting**

Verifiability (Definition)



→ Verifiability requires extra effort from voters

Usability Challenge



'Not every voter needs to verify'

True, but:

Any voter who wants to verify should be able to

&

Voters should not be confused by the option to verify

Objective



Analysing and improving usability of

Helios E2E verifiable remote EVoting system

while focusing on voter verifiability

Overview



- **Review of Helios**
 - Vote Casting Process
 - Sample Interfaces

About Helios

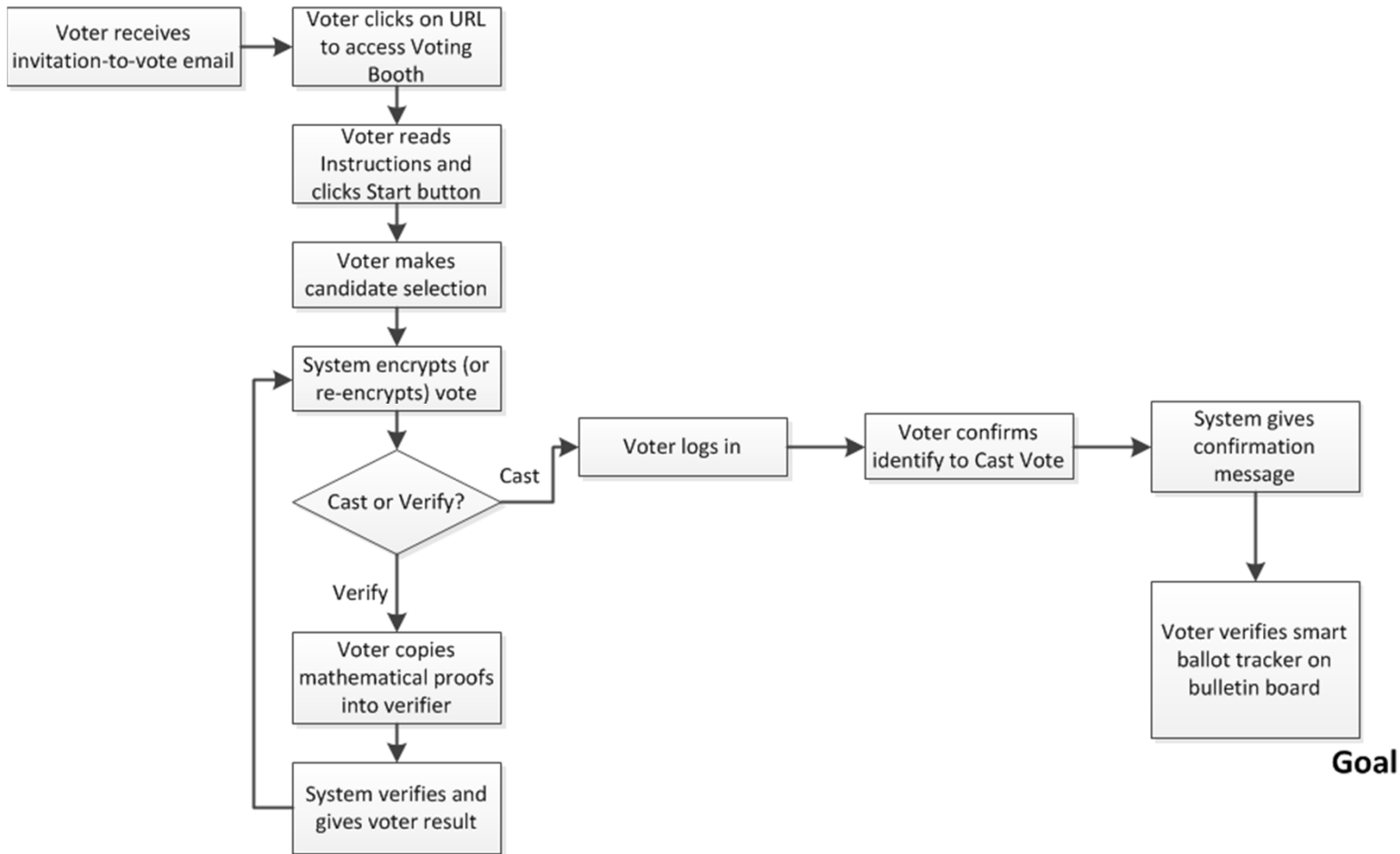


-
- Proposed by Ben Adida
 - Open-source system
 - Applies Benaloh's simple verifiable voting protocol for voter verifiability
 - Used in legally binding elections
 - in academic contexts: UCL, Princeton
 - election for IACR

Helios Vote Casting Process



Trigger



Overview



- Sample Interfaces

Sample Helios Interfaces (1)



Helios Voting Booth [\[exit\]](#)

Presidential Election of University

Presidential Election of University

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

Your ballot was successfully encrypted

Please **keep a record** of your smart ballot tracker [\[print\]](#) [\[email\]](#):

CqnEYxjq44rk+U6h+feiYnQsVvI2IF/Jsx1QsQhJa44

To protect your privacy:

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

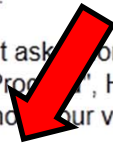
Audit [optional]

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.

Election Fingerprint: **2IsihDEFZKjeXk//Ip2vdgYGNcpDq1x4fig3F/Z2Fc4** [help!](#)

Voter selects whether to cast or verify



Sample Helios Interfaces (2)



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.

[Select your ballot audit info](#), copy it to your clipboard, then use the [ballot verifier](#) to verify it.
Once you are satisfied, click the "back to voting" button to re-encrypt and cast your ballot.

```
{ "answers": [{"choices": [{"alpha": "21551422620083924491939672158434889820995285366969832528740040455701077170970880070842305883706282126475183471422680410325734813243743999099311166479344875227042371818640103440767611473228194137967884086729915110686431662102204205312399076818390274157506051862734305042261772433715578215382040811044897789019648135331322518979743651083812082983897425903763892191457261132734143886960501909967448517540109975712523995225408102958021719567060175741770349759339704808089848381384349001165727916326845931938723708013997695137328872866216179967848775121936703524904932161872693756883591824772226260640998170282", "beta": "840795688665352843558387189898176361360374454870018552224018322413990188905733496619723378594056682964393274439002062568503997609977825421193852781343516783420"}]}]}
```

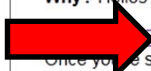
Before going back to voting, you can post this audited ballot to the Helios tracking center so that others might double-check the verification of this ballot.

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!](#)

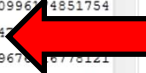
Select audit info



Open verifier window



Copy information



Sample Helios Interfaces (3)



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:

Your Ballot:

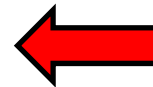
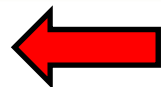
```
{ "answers": [ { "choices": [ { "alpha":  
"2155142262008392449193967215843489820995285366969832528740040455701077170970880  
5084230588370628212647518347142268041032573481324374399909931116647934487522704  
23718186401034407676114732281941379678840867299151106864316621022042053123990768  
18390274157506051862734305042261772433715578215382040811044897789019648135331322  
51897974365108381208298389742590376389219145726113273414388696050190996174851754  
01099757125239952254081029580217195670601757417703497593397048080894717254192023  
83813843490011657279163268459319387237080139976951373288728662161799676516778121
```

Verify

loading election...
election fingerprint is 2lsihDEFZKjeXk//lp2vdgYGNcpDq1x4fig3F/Z2Fc4
smart ballot tracker is CqnEYxjq44rk+U6h+feiYnQsVvl2IF/JsxIQsQhJa44
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!

Paste



Sample Helios Interfaces (4)



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.
Once you're satisfied, click the "back to voting" button to re-encrypt and cast your ballot.

```
{"answers": [{"choices": [{"alpha":  
"2155142262008392449193967215843489820995285366969832528740040455701077170970880  
07084230588370628212647518347142268041032573481324374399909931116647934487522704  
23718186401034407676114732281941379678840867299151106864316621022042053123990768  
18390274157506051862734305042261772433715578215382040811044897789019648135331322  
51897974365108381208298389742590376389219145726113273414388696050190996174851754  
01099757125239952254081029580217195670601757417703497593397048080894717254192023  
83813843490011657279163268459319387237080139976951373288728662161799676516778121  
936703524904932161872693756883591824772226260640998170282", "beta":  
"8407956886653528435583871898981763613603744548700185522240183224139901889057334  
96619723378594056682964393274439002062568503997609977825421193852781343516783420
```

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](#) [\[help\]](#)

Select next steps

Overview



- Improving Helios Interfaces
 - Cognitive Walkthrough

Cognitive Walkthrough



-
- Usability inspection method
 - A psychology, usability expert and computer scientists
 - Usability expert – no background in EVoting systems
 - Security and EVoting experts familiar with techniques employed
 - Analyzed the vote casting and verifiability procedures
 - Assessed the interfaces from voter's perspective
 - Considered
 - Actions required for vote casting and verifying a vote
 - Confusing aspects

Findings



Interchanging use of terms

Audit/verify

Inadequate emphasis placed on verifying
Voter may be confused by additional steps



Voter seeking help has to send an email

Impractical

Verifiability process is confusing

Mathematical proofs can be overwhelming to average voter

Copy and paste may be prone to error

Smart ballot tracker long, difficult to compare

Overview



- Improved Interfaces

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. 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)



Presidential Election for University

Instructions Ballot Verification-Code **Log**

Welcome to presidential Election for University

This election will be executed in 3 steps:

1. In the first step, you will see the ballot where you can vote for the candidate of your choice.
2. After you choose a candidate, your ballot will be encrypted in order to keep the vote secret. Furthermore a verification code will be generated for your ballot. To ensure that your ballot is correctly encrypted, you can have this encryption verified by any one of several independent institutes. You can repeat this process as many times as you need, until you are convinced that this vote system functions correctly.
3. The actual ballot-casting process is performed in the last step. By entering your username and password, your (encrypted) ballot will be cast. As long as you have not cast your ballot, you can cancel this procedure at anytime by closing the vote system's window. You are free to continue at another time. This will not cause you to lose your eligibility to vote.

At the end of the election, a list of verification codes for all the tallied votes will be published. If you want to confirm whether your vote has been correctly tallied, you can look up your verification code in this list.

To start the election procedure, click on the "Proceed to Ballot" button.

Proceed to Ballot >>

Added verifiability step

Instructions to voters

Improved Interfaces (3)



Presidential Election for University

Instructions	Ballot	Verification-Code	Ballot-Casting
--------------	--------	-------------------	----------------

Ballot

For the Presidential Election of University

You can select **one** candidate (or invalid vote).

1	Prof. Ford Prefect	<input type="radio"/>
2	Prof. Zaphod Beeblebrox	<input type="radio"/>
3	Prof. Tricia McMillan	<input type="radio"/>
	Invalid Vote	<input type="radio"/>

Provide invalid vote option

Back and Forward Buttons

<input type="button" value=" << Back to Instructions"/>		<input type="button" value=" Check the Ballo >>"/>
---	--	--

Improved Interfaces (4)



Presidential Election for University

Instructions	Ballot	Verification-Code	Ballot-Casting
--------------	--------	-------------------	----------------

Your ballot has been encrypted to keep the vote secret.

Your Verification-Code is x4WH1LC1F4t1hK6k

With the help of this verification-code, you can verify whether your vote is correctly tallied. For this please write down this verification-code or use the following alternatives:

[Download Code](#) [Print Code](#)

To ensure that your ballot is correctly encrypted, you can have this encryption verified. You can repeat this process as many times as you want, until you are convinced that this vote system functions correctly.

[<< Change Vote](#) [Verify the Ballot](#) [Cast the Ballot >>](#)

Shortened verification code

Options for voter

Improved Interfaces (5)





Mayoral Election of Darmstadt


Instructions	Ballot	Verification-Code	Ballot-Casting
--------------	--------	-------------------	----------------


You can now verify whether your ballot is correctly encrypted. In order to do this, click on the logo of an institute which you prefer to verify the ballot or click on the self-verification logo to see the encryption proofs and verify them yourself (requires advanced cryptography knowledge). This process will open a new window with the selected institute that will give you the result of the verification.


Institute:


[\[Verify the Ballot\]](#)


CASED
[\[Verify the Ballot\]](#)


UCL
Université catholique de Louvain
[\[Verify the Ballot\]](#)


TECHNISCHE UNIVERSITÄT DARMSTADT
[\[Verify the Ballot\]](#)


SELF VERIFICATION
[\[Verify the Ballot\]](#)

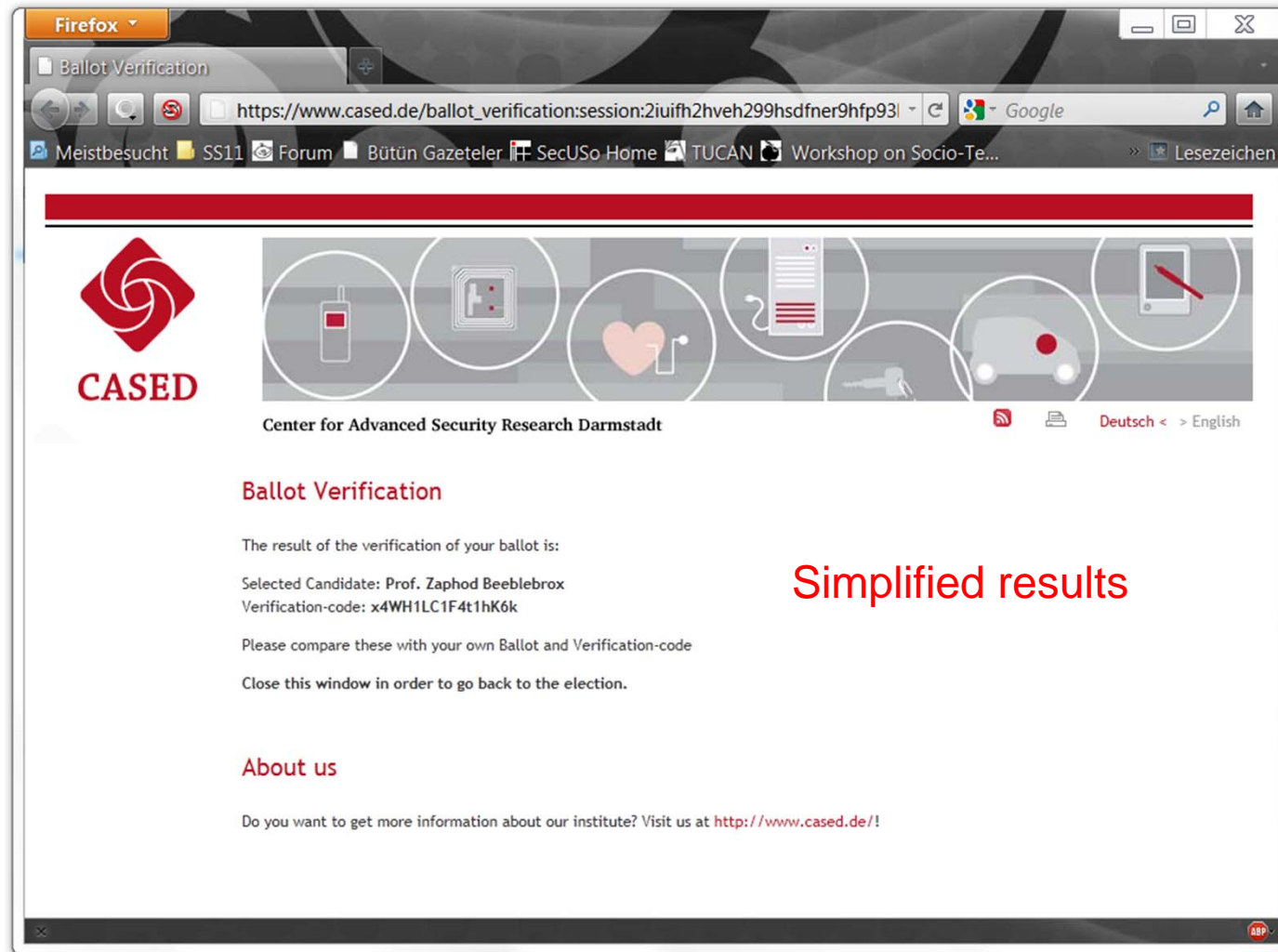
This verification process will require that the ballot is decrypted. Therefore your ballot will be reencrypted and a new Verification-Code will be generated to protect the Vote-secrecy.

After a successful Verification you can proceed with the Election process. If you notice any irregularities, please cancel the election process immediately and contact us under the telephone number 1111111111

[Finish the verification and proceed with the election >>](#)

Trusted institutions for verification

Improved Interfaces (6)



Improved Interfaces (7)



Presidential Election for University

Instructions Ballot **Verification-Code** Ballot-Casting

1	Prof. Ford Prefect	<input type="radio"/>
2	Prof. Zaphod Beeblebrox	<input checked="" type="radio"/>
3	Prof. Tricia McMillan	<input type="radio"/>
	Invalid Vote	<input type="radio"/>

Your ballot has been encrypted to keep the vote secret.

Your Verification-Code is: x4WH1LC1F4t1hK6k

Attention: Your Verification-code has been changed, because it has been re-encrypted. The previous verification-code is therefore invalid.

With the help of this Verification-code, you can control whether your vote has been correctly tallied. In order to do this please write down this verification-code or use the following alternatives:

[Download Code](#) [Print Code](#)

To ensure that your ballot is correctly encrypted, you can have this encryption verified. You can repeat this process as many times as you want, until you are convinced that this vote system functions correctly.

[<< Change Vote](#) [Verify the Ballot](#) [Cast the Ballot >>](#)

Explanation for voter



Attention: Your Verification-code has been changed, because it has been re-encrypted. The previous verification-code is therefore invalid.

Improved Interfaces (8)



Presidential Election for University

Instructions	Ballot	Verification-Code	Ballot-Casting
--------------	--------	-------------------	-----------------------

Verification-Code of the Ballot to be cast is: **x4WH1LC1F4t1hK6k**

Please compare the shown verification-code with the one you wrote down during the previous step.

Please enter your user-name and password if you want to cast your ballot. You can find your user-name and your password in the invitation to vote letter.

Username	<input type="text"/>
Password:	<input type="password"/>

<< Back to the verification-code

Conclude the Ballot-Casting >>

Improved Interfaces (9)



Presidential Election for University

Instructions

Ballot

Verification-Code

Ballot-Casting

Your vote has been saved. Thank you very much for your participation

1 hour after the end of this election at 6:00 pm, the results and the list of verification-codes will be published at www.electionresults.university.com

Now please close this window.

Comparison



-
- Old Interfaces
 - Total # mouse clicks to *cast a vote* - 9
 - Total # mouse clicks to *verify a vote* - 8
 - New Interfaces
 - Total # mouse clicks to *cast a vote* - 7
 - Total # mouse clicks to *verify a vote* - 3

Overview



- User Study

User Study



-
- Tested usability of new interfaces with 34 users
 - Lab set up
 - Two runs; voters given instructions after first run
 - **Findings:**
 - Voters find the new interfaces usable
 - Voters need more assistance to understand concept of verifiability
 - Results in STAST2011

Overview



- Future Work and Conclusion

Future Work



-
- Adequate length for the verification code
 - More user-friendly techniques for verifiability, e.g. QR codes
 - Interview potential voters for their understanding of verifiability
 - Short video to explain concept of verifiability to voters
 - Integrate metaphors
 - Investigate how to assist voters to authenticate voting servers

Conclusion



-
- Investigated usability of verifiability in Helios
 - Analysed current interfaces using cognitive walkthrough technique
 - Developed alternative interfaces for Helios
 - Evaluated new interfaces in a user study [STAST2011]
 - Usability of verifiability processes still requires further research

The End



Thank you for your attention

Any Questions?