Usability of Verifiability in Helios

Maina Olembo, Fatih Karayumak, Michaela Kauer, Melanie Volkamer

8th August, 2011

Overview

CASED

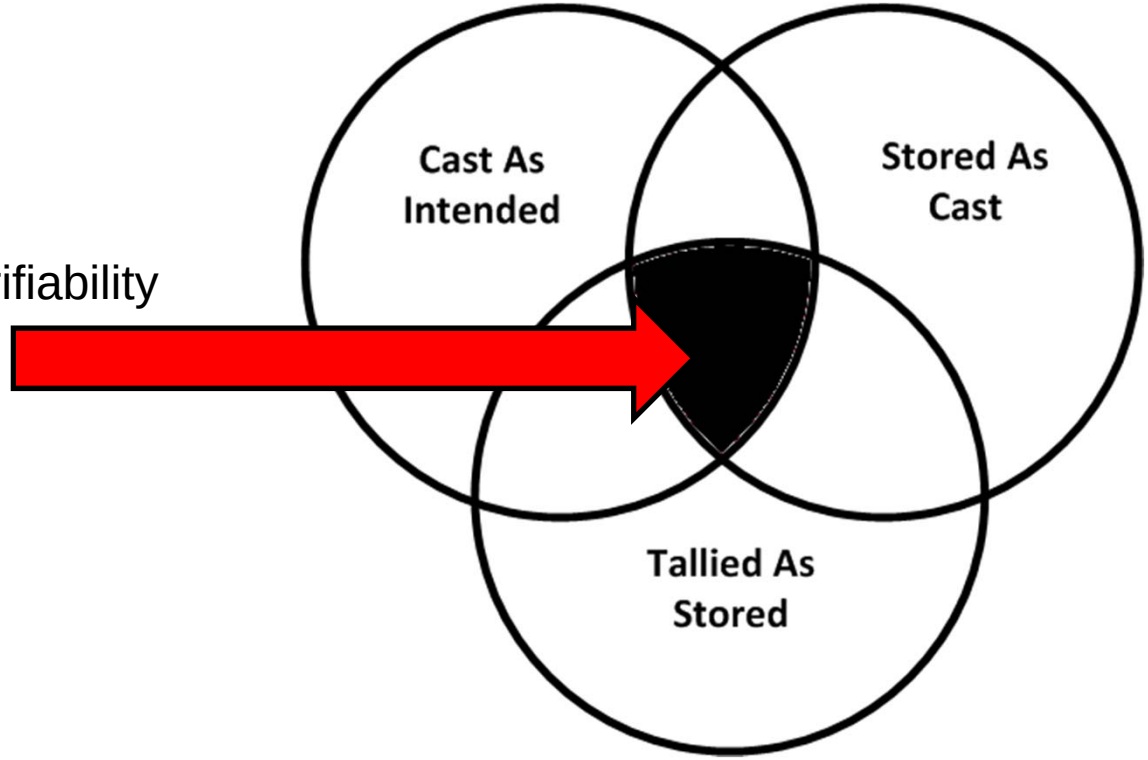
- Why usability of verifiability in remote EVoting
- Review of Helios
  - Vote Casting Process
  - Sample Interfaces
- Improving Helios Interfaces
  - Cognitive Walkthrough
  - Improved Interfaces
  - User Study
- Future Work and Conclusion

Overview

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

Verifiability (Definition)

End–to–End Verifiability



→ Verifiability requires extra effort from voters

Usability Challenge

CASED

`*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

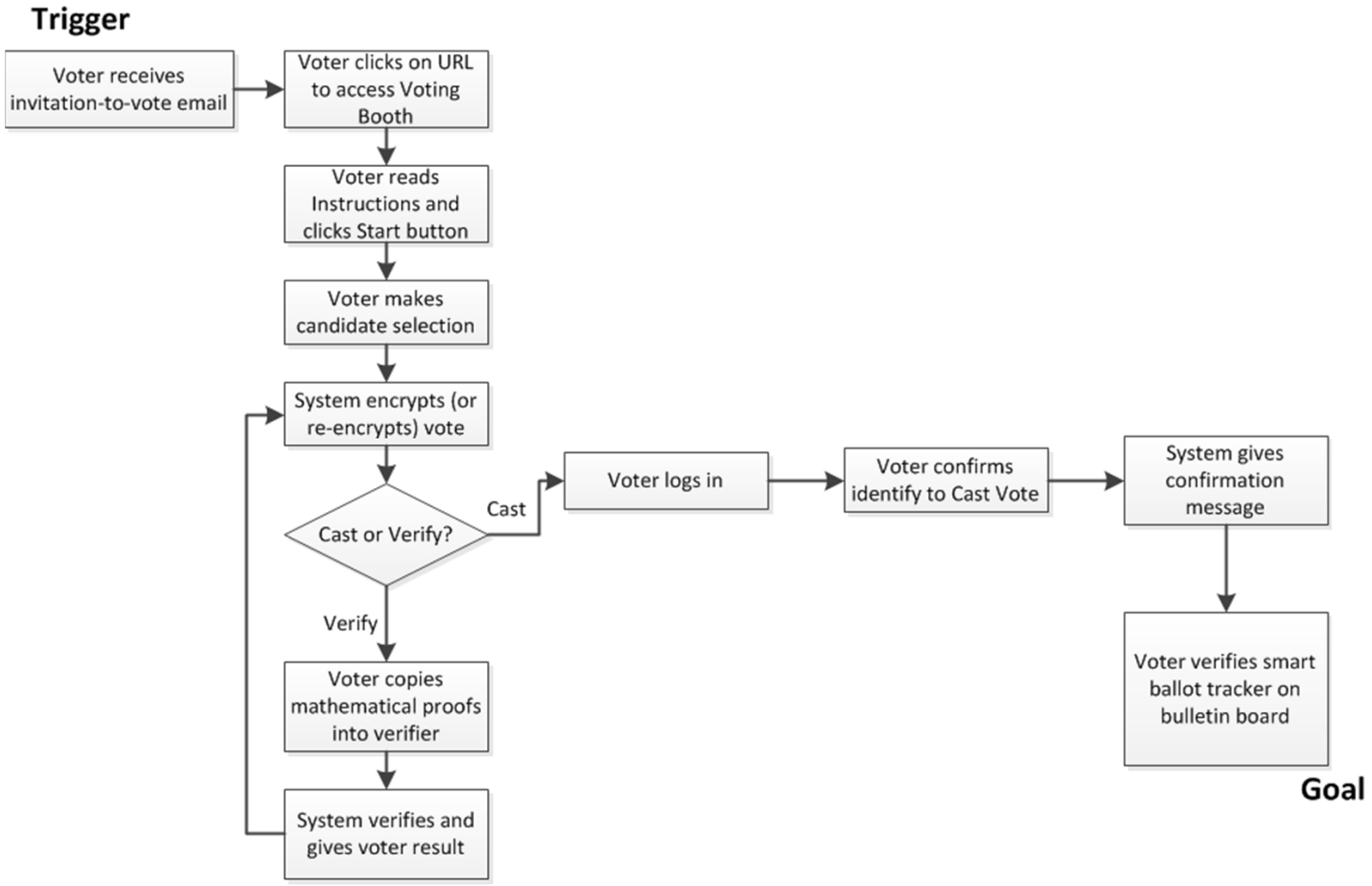
Overview

- **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

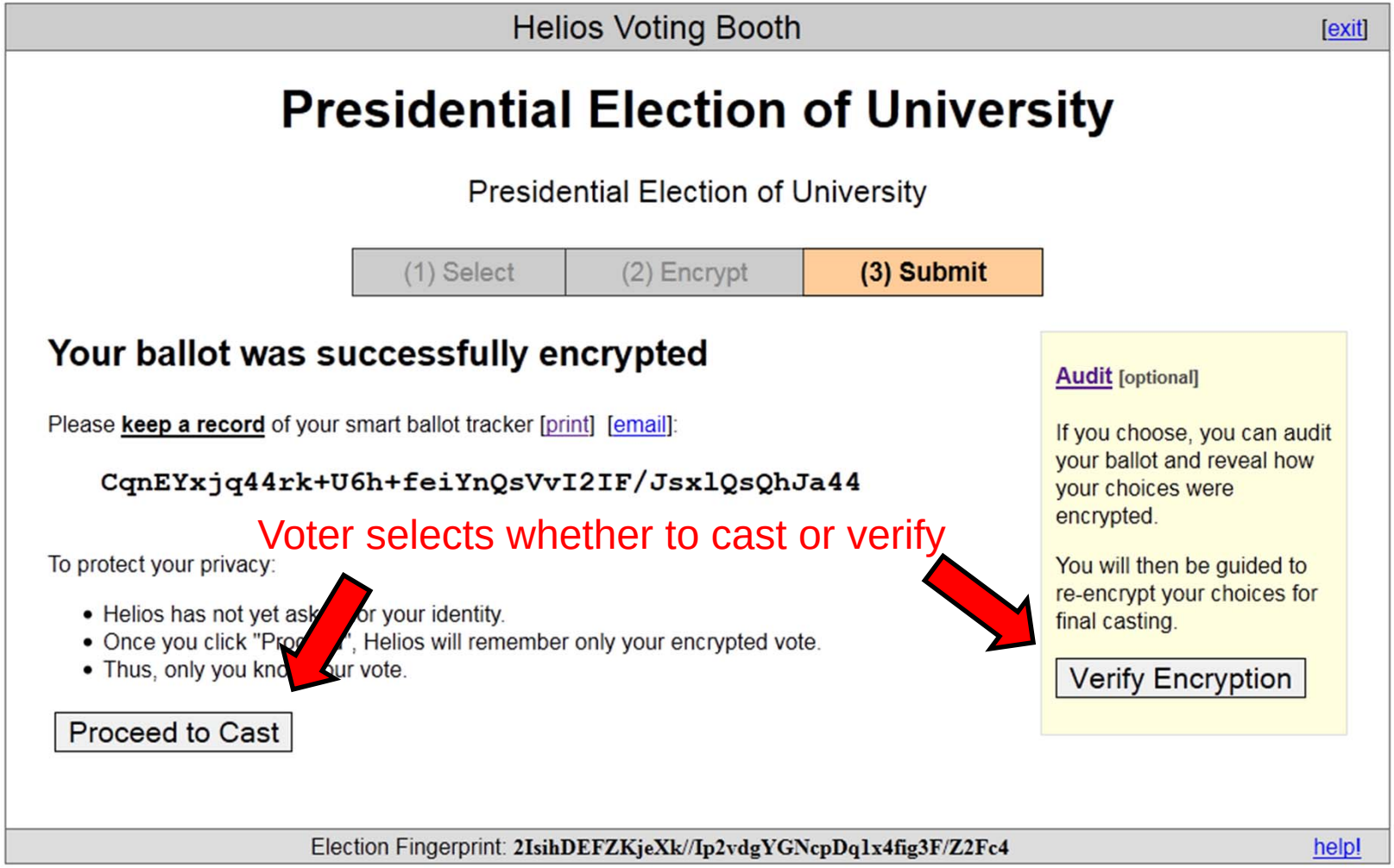
Helios Vote Casting Process



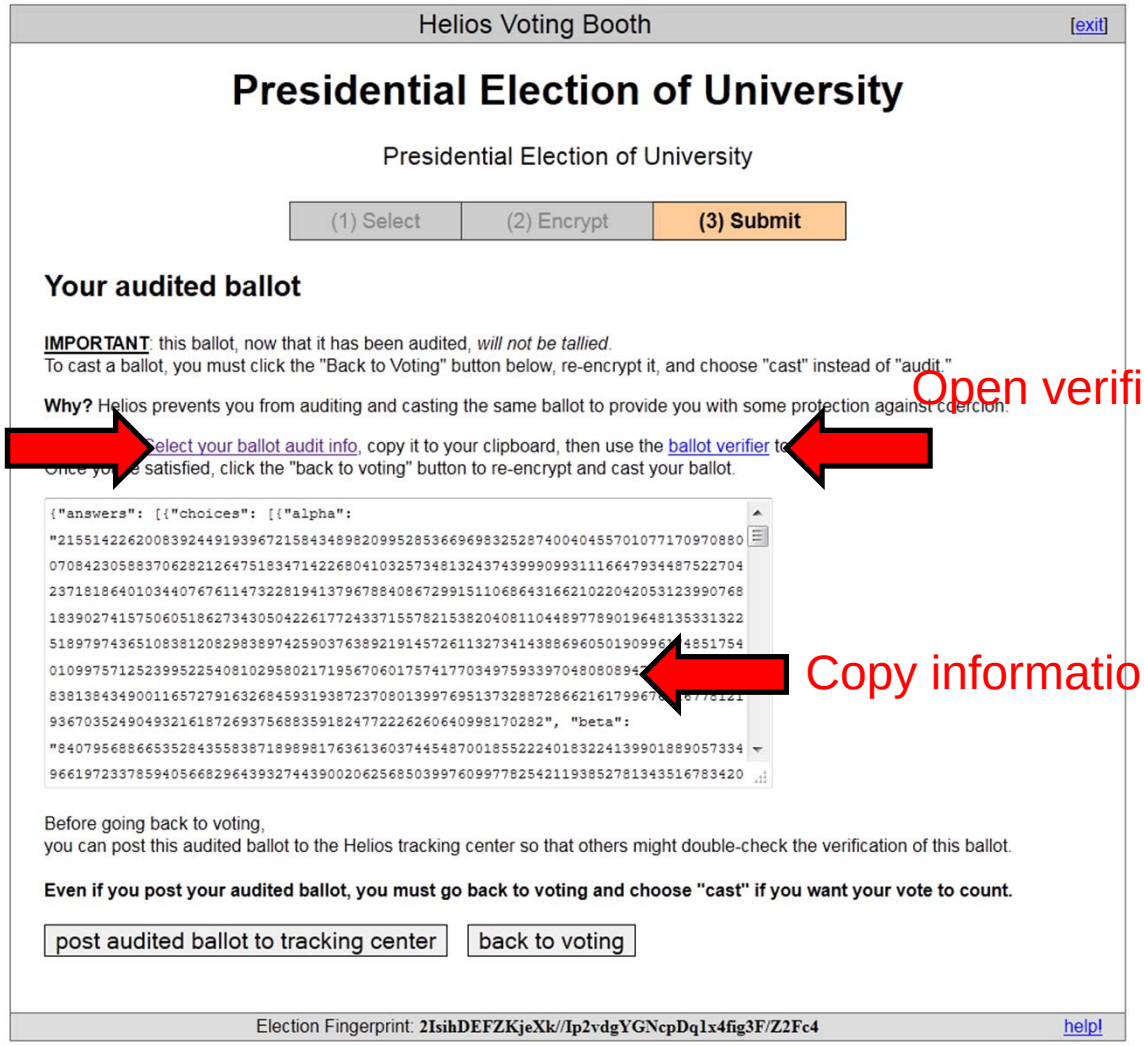
Overview

- Sample Interfaces

Sample Helios Interfaces (1)



Sample Helios Interfaces (2)

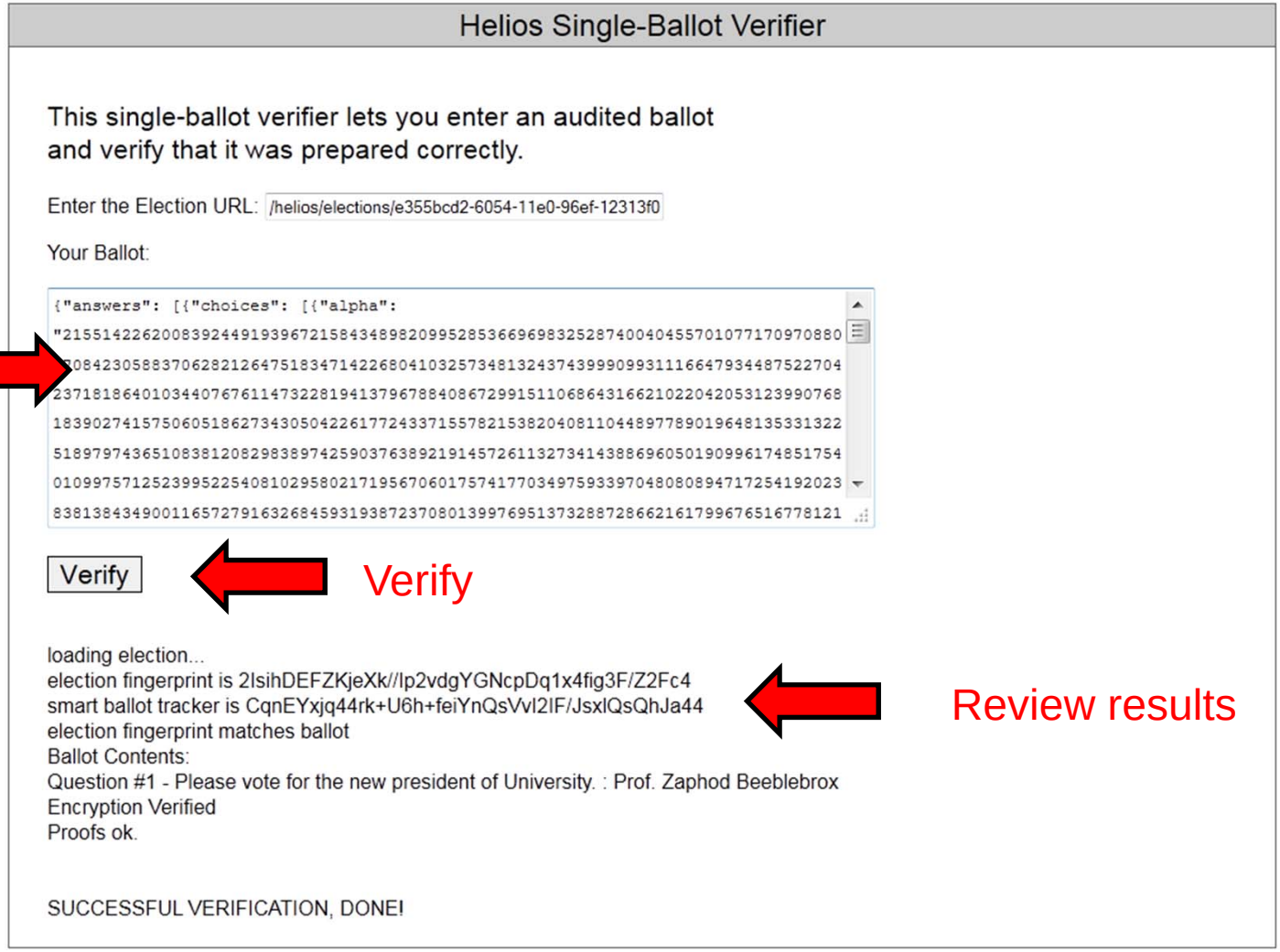


Select audit info

Open verifier window

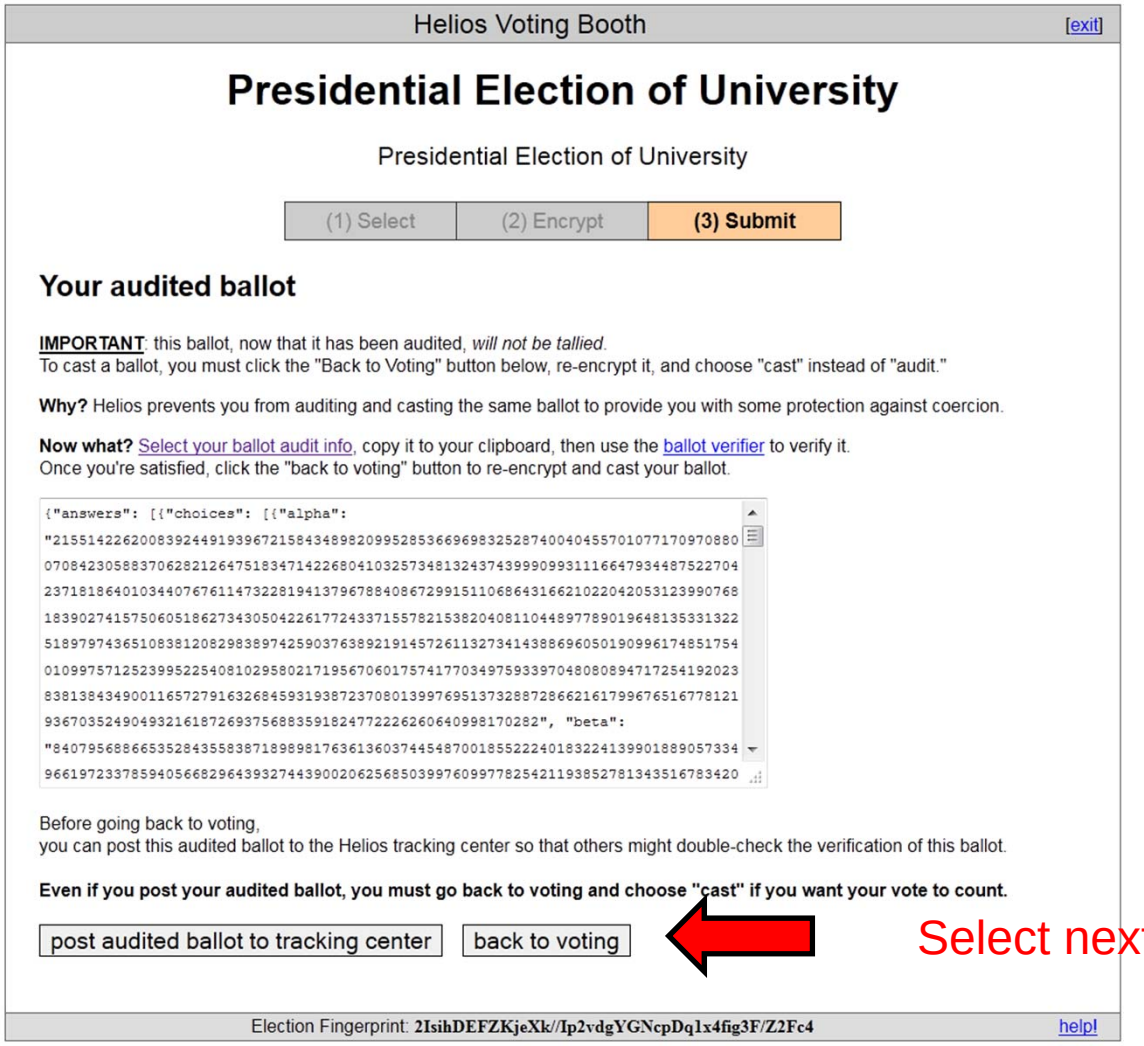
Copy information

Sample Helios Interfaces (3)



Sample Helios Interfaces (4)

CASED



Overview

CASED

- 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

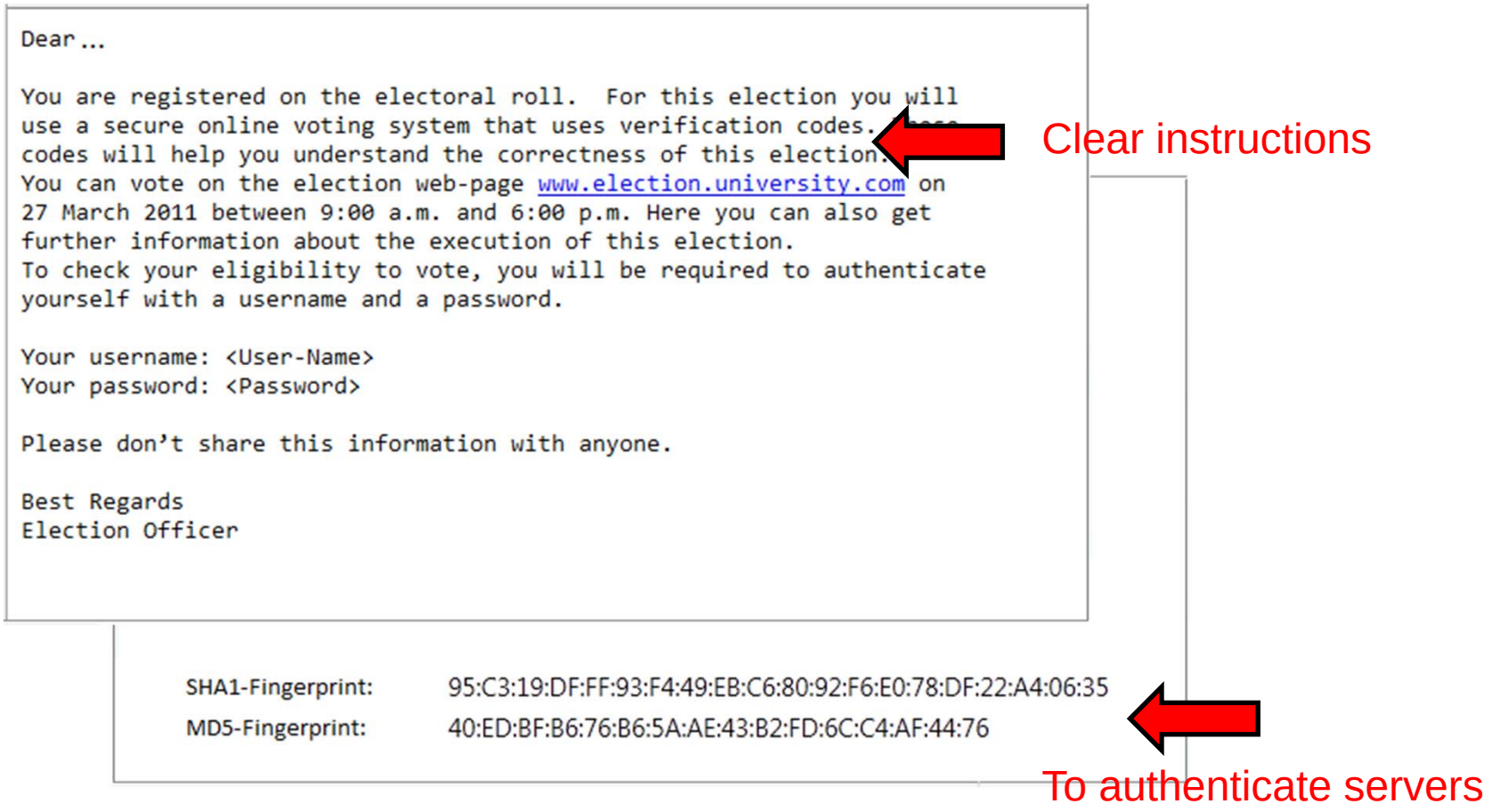
Smart ballot tracker long, difficult to compare

Overview

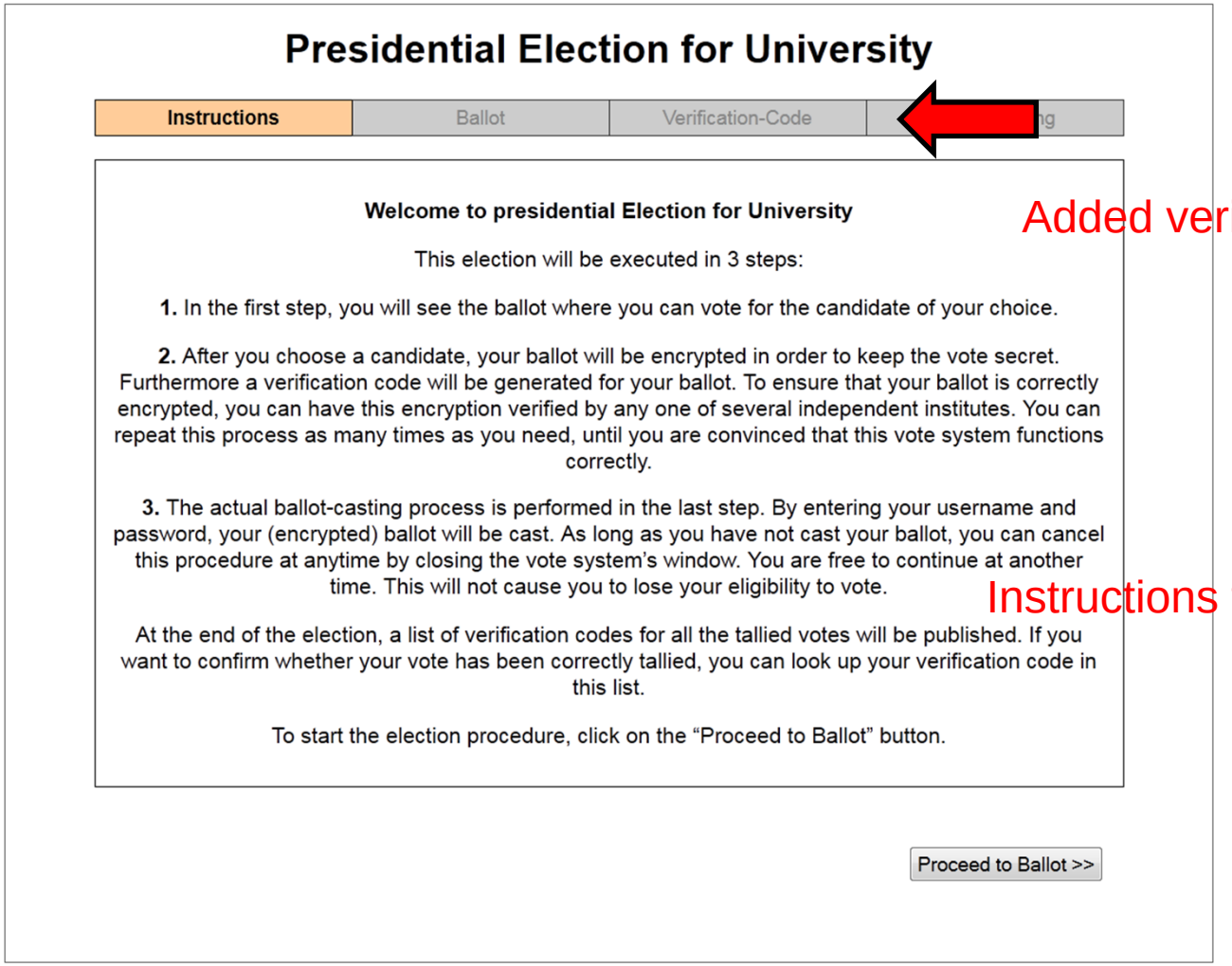
CASED

- Improved Interfaces

Improved Interfaces (1)



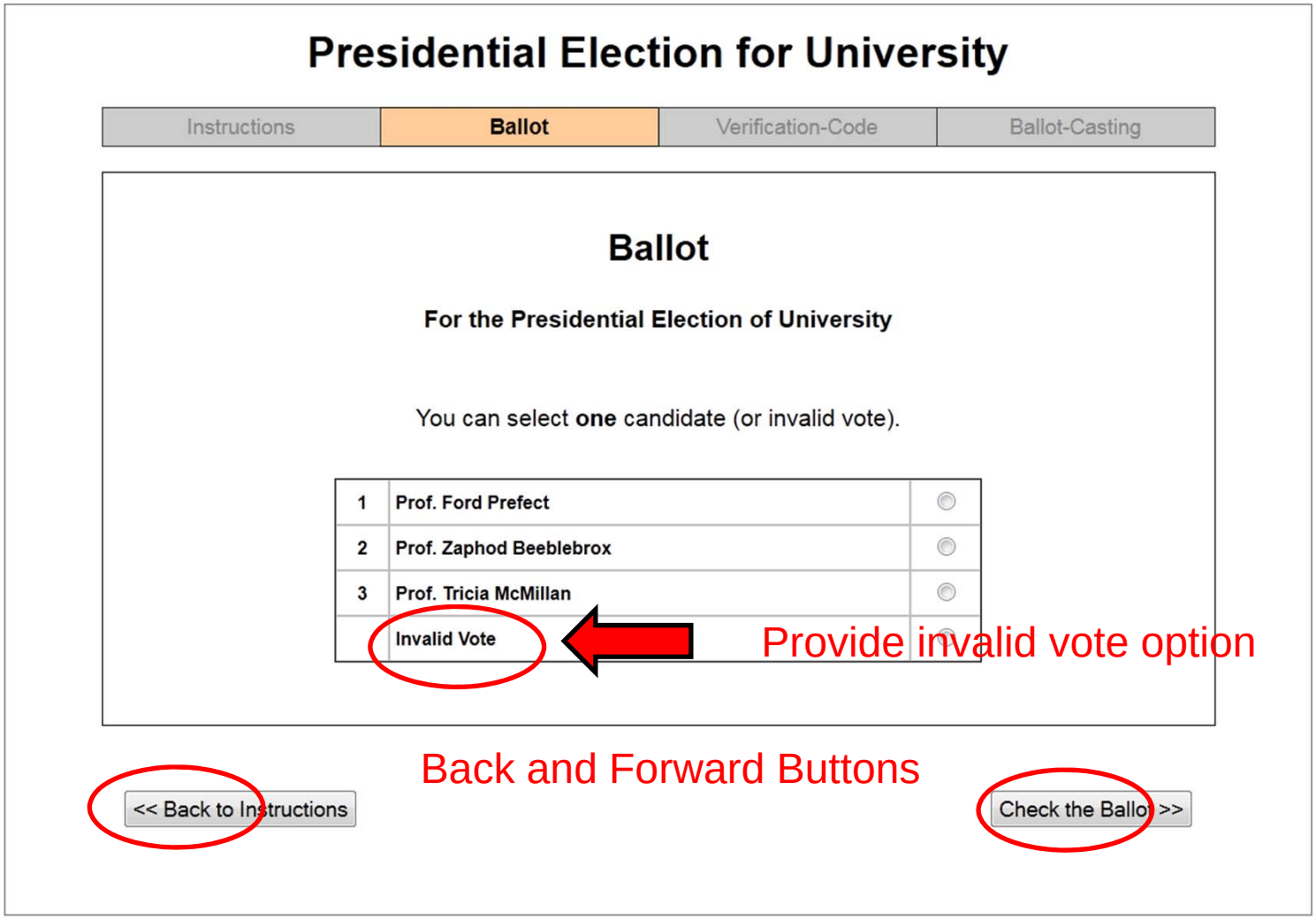
Improved Interfaces (2)



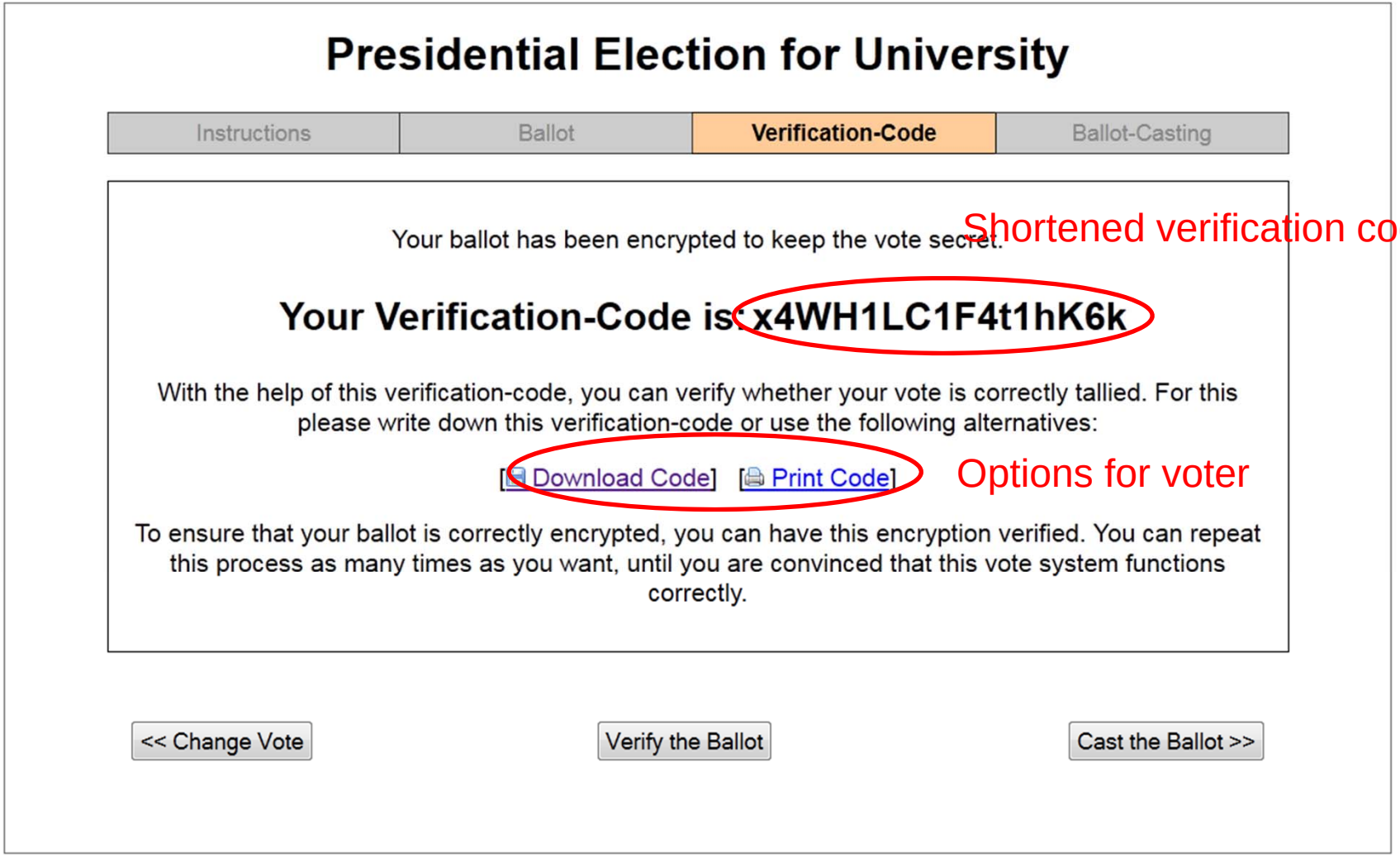
Added verifiability step

Instructions to voters

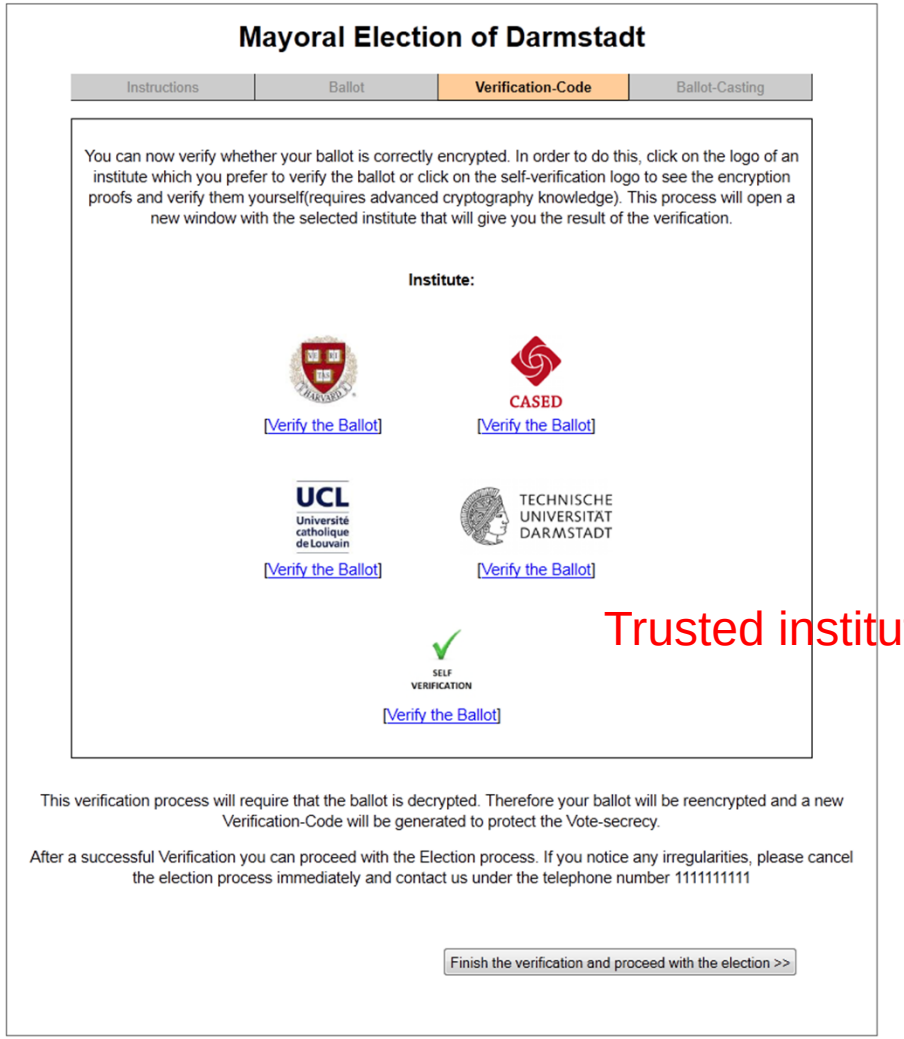
Improved Interfaces (3)



Improved Interfaces (4)

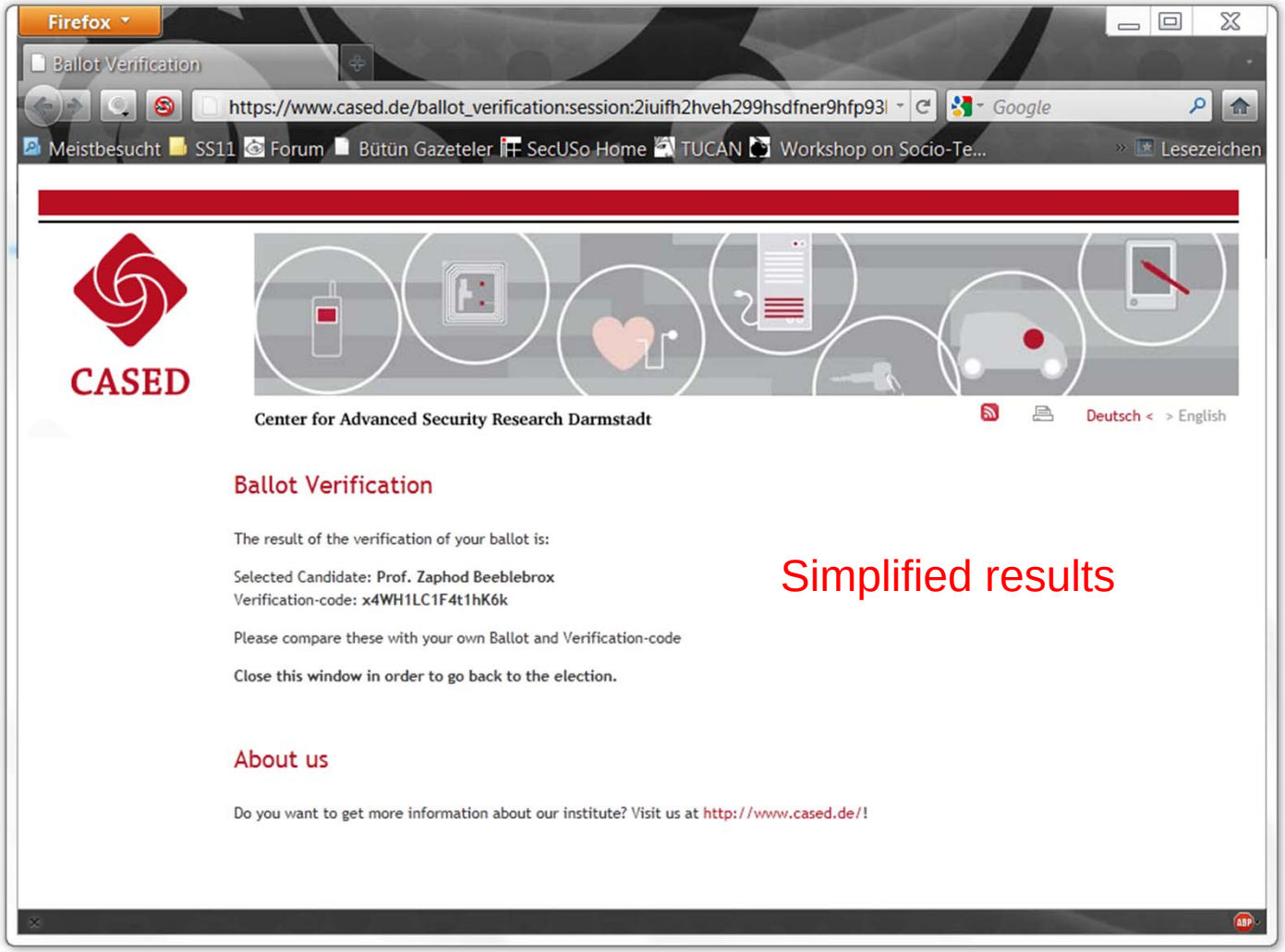


Improved Interfaces (5)



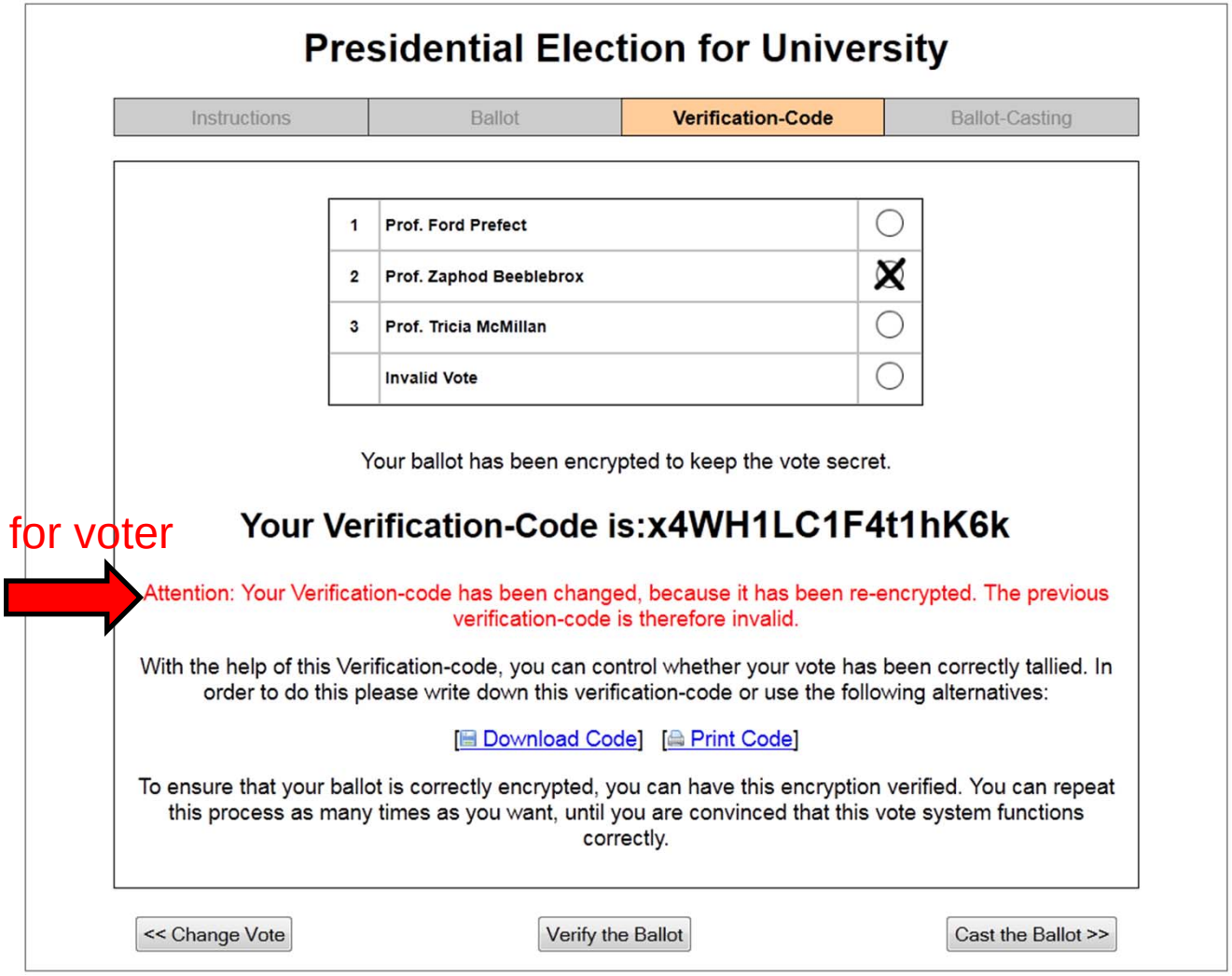
Trusted institutions for verification

Improved Interfaces (6)



Simplified results

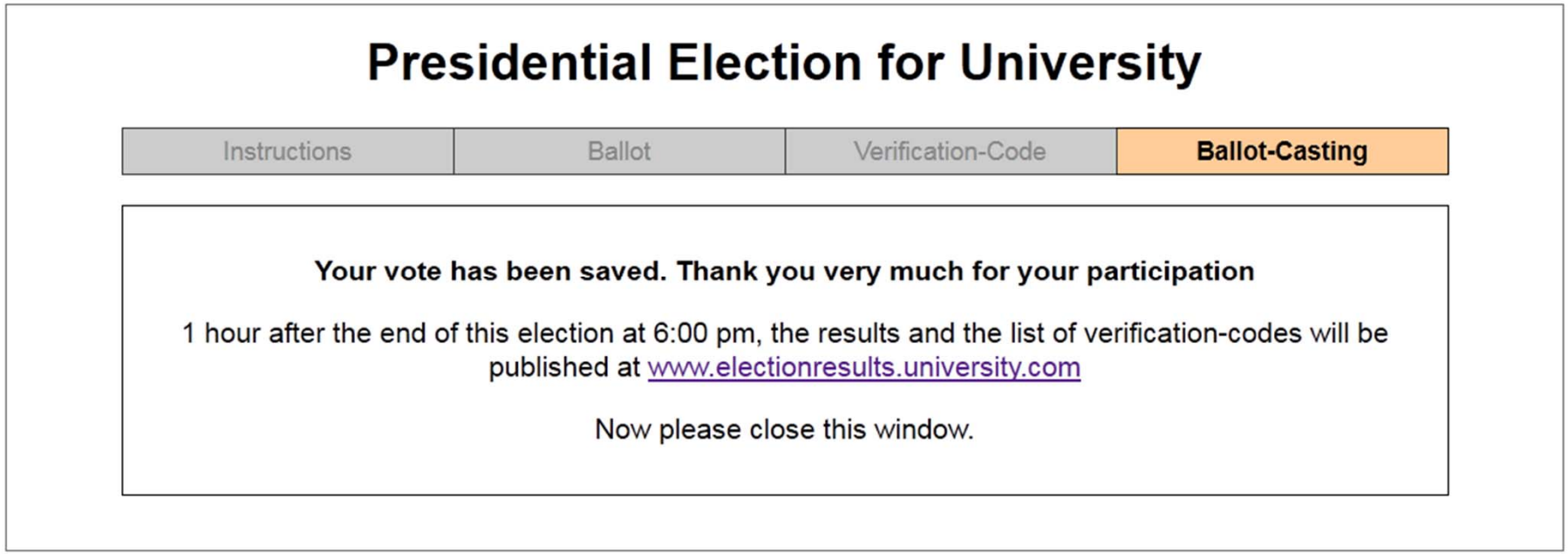
Improved Interfaces (7)



Explanation for voter

Improved Interfaces (8)

Improved Interfaces (9)



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

CASED

- 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?