Vulnerability Studies of E2E Voting Systems

Lauretha Rura,
Swinburne University of Technology, Malaysia

Biju Issac
Teesside University, UK

Manas Haldar
Swinburne University of Technology, Malaysia

CISSE 2012
7th – 9th December 2012

Introduction

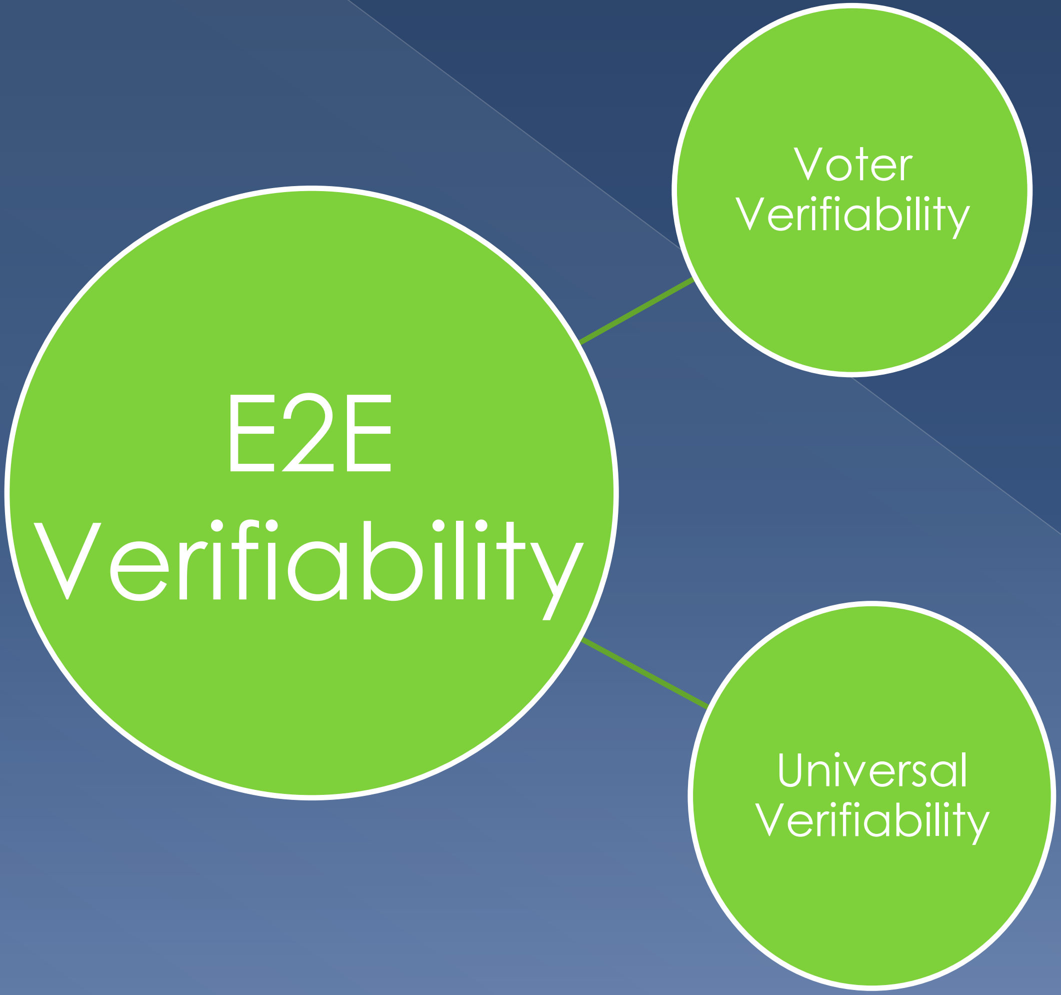
- Key concerns of elections
  - Trust
  - Transparency

VS

Paper-ballot Voting

E-Voting System

End-to-End Verifiable System



E2E Verifiability

Voter Verifiability

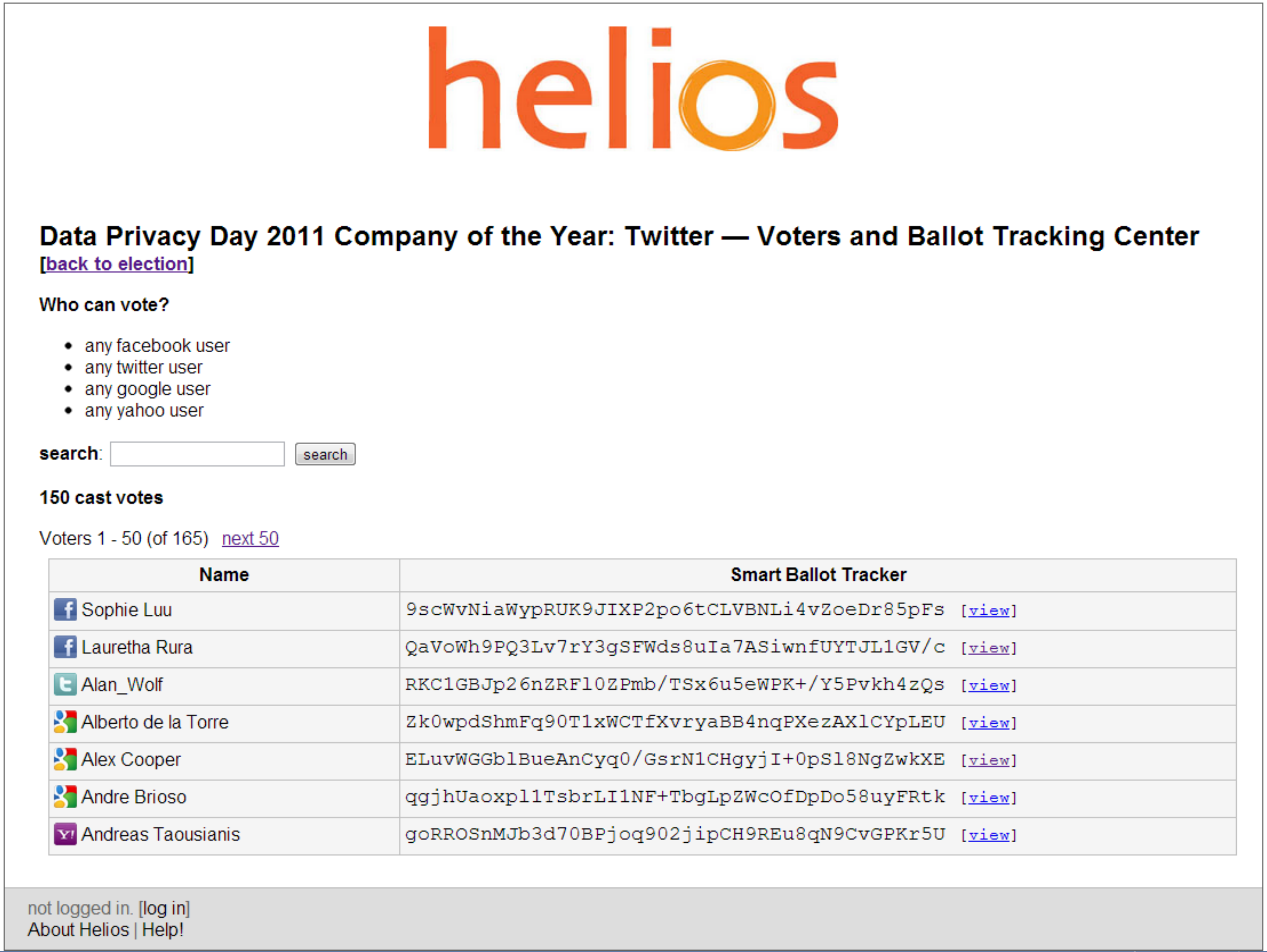
- Vote Receipt

Universal Verifiability

- Bulletin Board

Related E2E Voting Systems

- Helios
  - Open-source web-based open-audit voting system that offers verifiable online elections for anyone (B. Adida, 2008).
  - Ensures ballot secrecy and election integrity (low coercion)
  - Divided into two main categories:
    - Ballot Preparation
    - Ballot Casting
      - Smart Ballot Tracker and Ballot Tracking Center (Bulletin Board) for vote verification



helios

Data Privacy Day 2011 Company of the Year: Twitter — Voters and Ballot Tracking Center

[back to election]

Who can vote?

- any facebook user
- any twitter user
- any google user
- any yahoo user

search: search

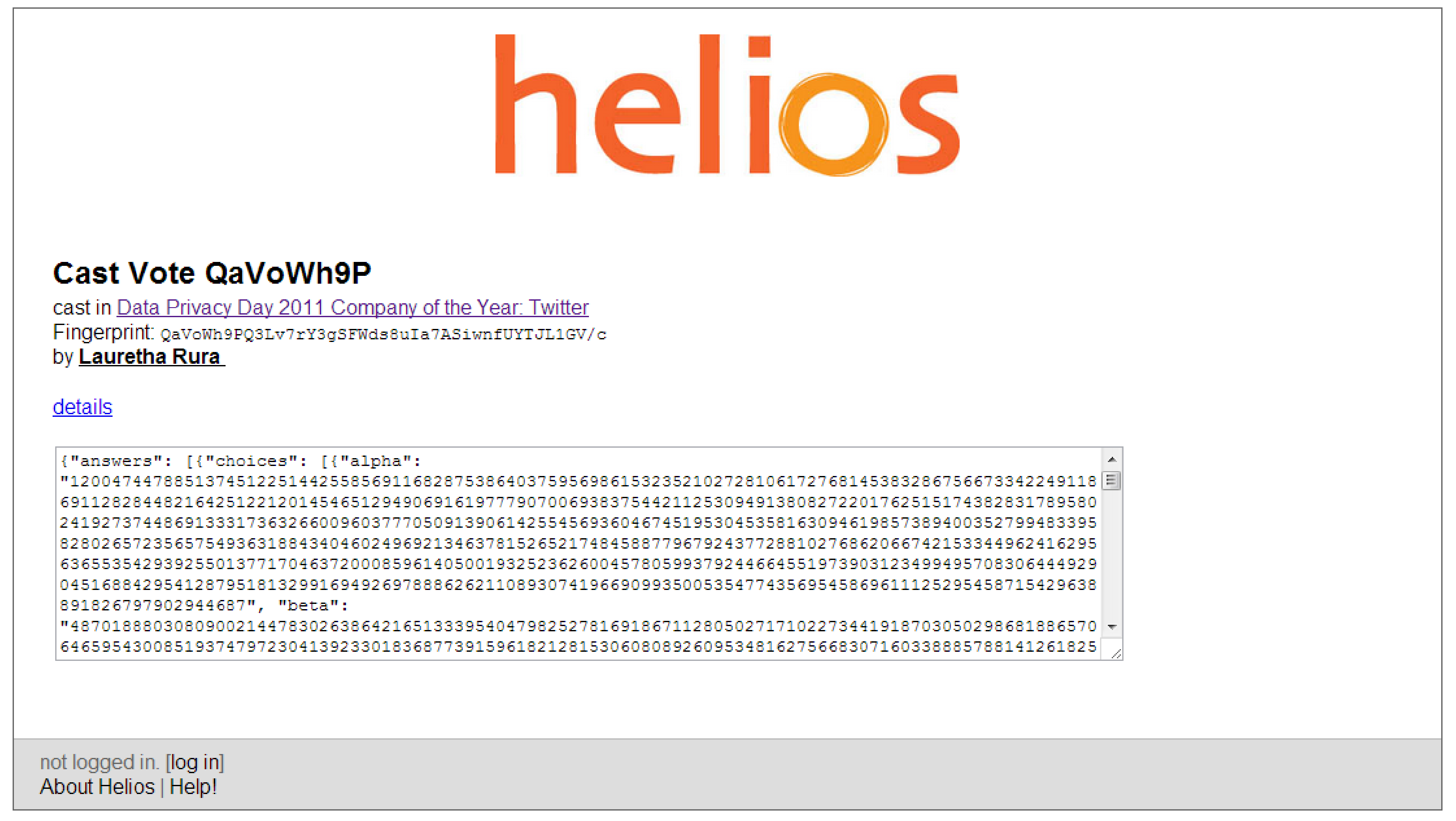
150 cast votes

Voters 1 - 50 (of 165) next 50

Name	Smart Ballot Tracker
Sophie Luu	9scWvNiaWypRUK9JIXP2po6tCLVBNLi4vZoeDr85pFs [view]
Lauretha Rura	QaVoWh9PQ3Lv7rY3gSFWds8uIa7ASiwnfUYTJL1GV/c [view]
Alan_Wolf	RKC1GBJp26nZRFl0ZPmb/TSx6u5eWPK+/Y5Pvkh4zQs [view]
Alberto de la Torre	Zk0wpdShmFq90T1xWCTfXvryaBB4nqPXezAXlCYpLEU [view]
Alex Cooper	ELuvWGGblBueAnCyq0/GsrN1CHgyjI+0pSl8NgZwkXE [view]
Andre Brioso	qgjhUaoxpl1TsbrLI1NF+TbgLpZWcOfDpDo58uyFRtk [view]
Andreas Taousianis	goRROSnMJb3d70BPjoq902jipCH9REu8qN9CvGPKr5U [view]

not logged in. [log in]
About Helios | Help!

Fig. 1 Ballot Tracking Center of Helios Voting System



helios

Cast Vote QaVoWh9P

cast in Data Privacy Day 2011 Company of the Year: Twitter
Fingerprint: `QaVoWh9PQ3Lv7rY3gSFWds8uIa7ASiwnfUYTJL1GV/c`
by **Lauretha Rura**

details

```
{"answers": [{"choices": [{"alpha":
"120047447885137451225144255856911682875386403759569861532352102728106172768145383286756673342249118
69112828448216425122120145465129490691619777907006938375442112530949138082722017625151743828317895 80
241927374486913331736326600960377705091390614255456936046745195304535816309461985738940035279948339 5
828026572356575493631884340460249692134637815265217484588779679243772881027686206674215334496241629 5
636553542939255013771704637200085961405001932523626004578059937924466455197390312349949570830644492 9
045168842954128795181329916949269788862621108930741966909935005354774356954586961112529545871542963 8
8918267979029446 87", "beta":
"487018880308090021447830263864216513339540479825278169186711280502717102273441918703050298681886570
646595430085193747972304139233018368773915961821281530608089260953481627566830716033888578814126182 5
```

Fig. 2 Helios Smart Ballot Tracker

- Scantegrity II
  - Practical enhancement for optical scan voting systems that achieves increased election integrity through a novel use of confirmation codes printed on ballots in invisible inks (Chaum et. all, 2008).
  - Improved version of two optical scan voting systems:
    - Punchscan
    - Scantegrity
  - Invisible Inks Technology

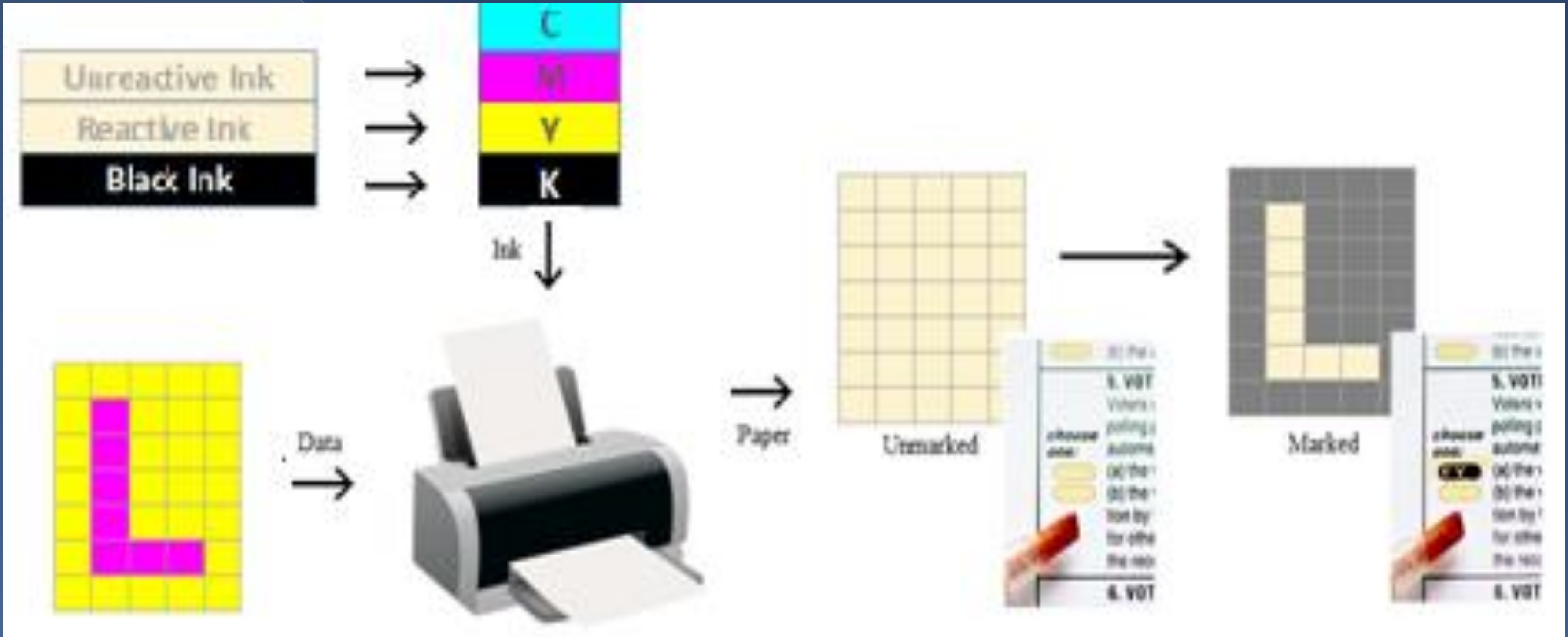
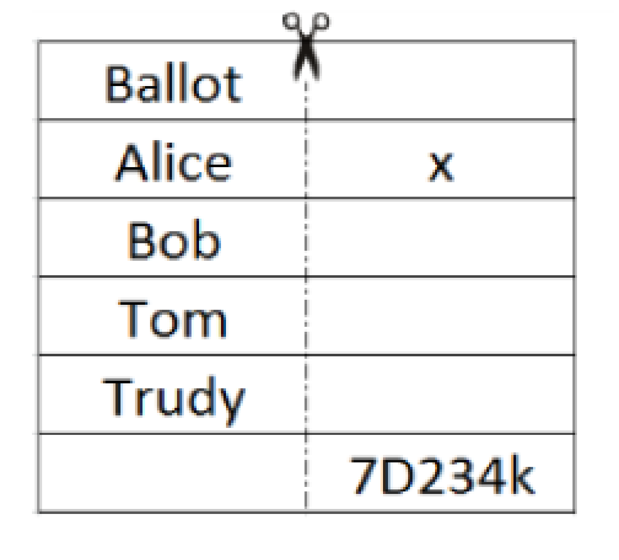


Fig. 3 Process of Invisible Ink Printing

Prêt à Voter

- Paper-based ballot E2E voting system that ensures ballot secrecy and anonymity through the implementation of mix-net scheme.

- System’s stages:
  - Ballot Generation
  - Vote Capture
  - Vote Processing
  - Auditing



Ballot	
Alice	x
Bob	
Tom	
Trudy	
	7D234k

Fig. 4 Prêt à Voter’s sample ballot

- Rijnland Internet Election System (RIES)
  - Combination of paper-based and non paper-based ballot voting systems with the assistance of its administrator called TTPI (Trusted Third Party Internetstemmen).
  - Applied for the first time in 2004 Water Boards Election at Rijnland and De Dommel.
  - Vote Casting:
    - by Registered Mail
    - Electronically
  - System's stages:
    - Initial Stage
    - Election Stage
    - Tally Stage

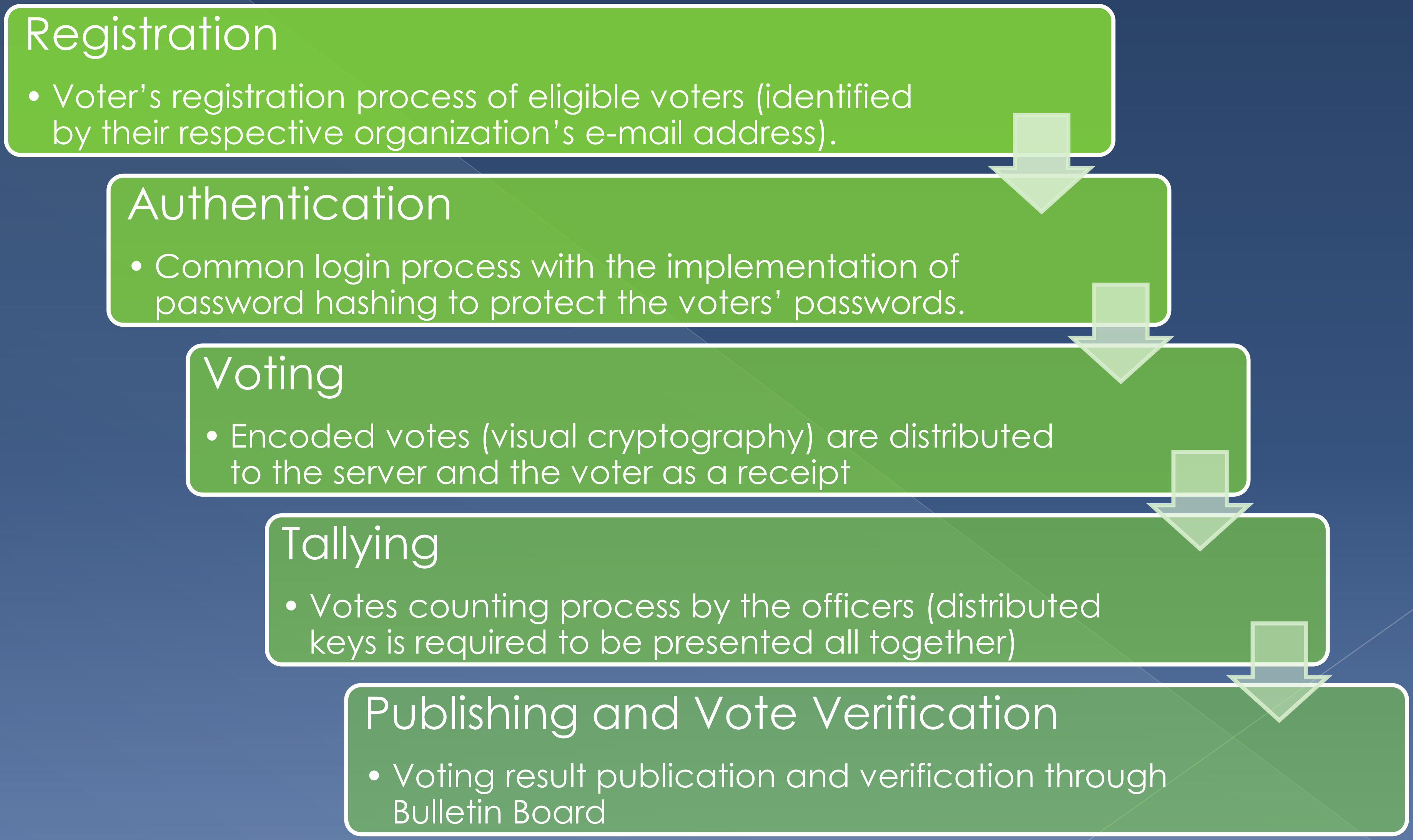
Proposed System: eVote

- The implementation of cryptography and steganography in E2E voter verifiable remote electronic voting

- Cryptography is the art and science of keeping messages secure (B. Schneier, 1996), while Steganography is the art and science of hiding communication (Provos and Honeyman, 2003).

- Three Types of Users:
  - Administrators
  - Election Officers
  - Voters

System Design



Registration

- Voter’s registration process of eligible voters (identified by their respective organization’s e-mail address).

Authentication

- Common login process with the implementation of password hashing to protect the voters’ passwords.

Voting

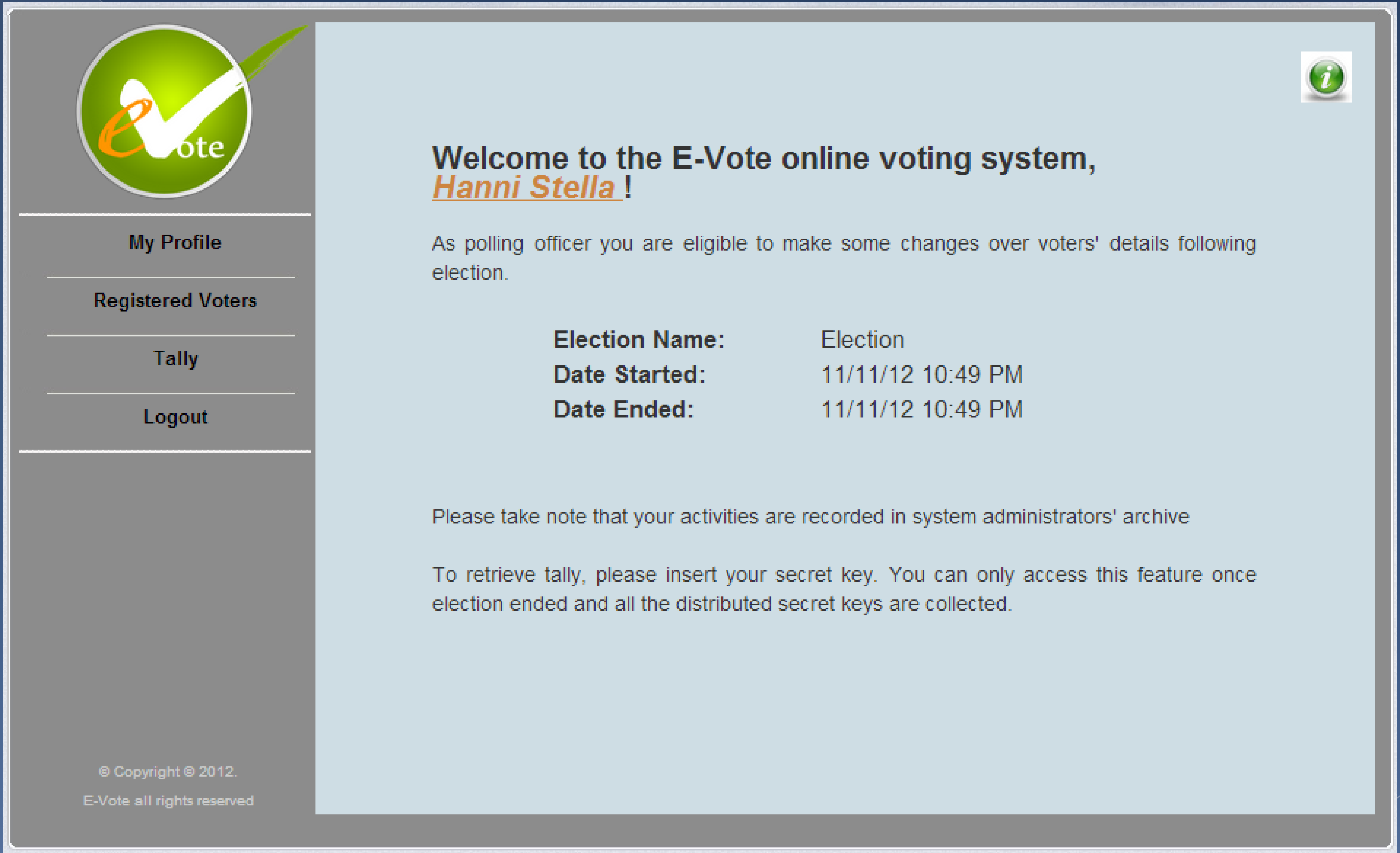
- Encoded votes (visual cryptography) are distributed to the server and the voter as a receipt

Tallying

- Votes counting process by the officers (distributed keys is required to be presented all together)

Publishing and Vote Verification

- Voting result publication and verification through Bulletin Board



Welcome to the E-Vote online voting system, Hanni Stella !

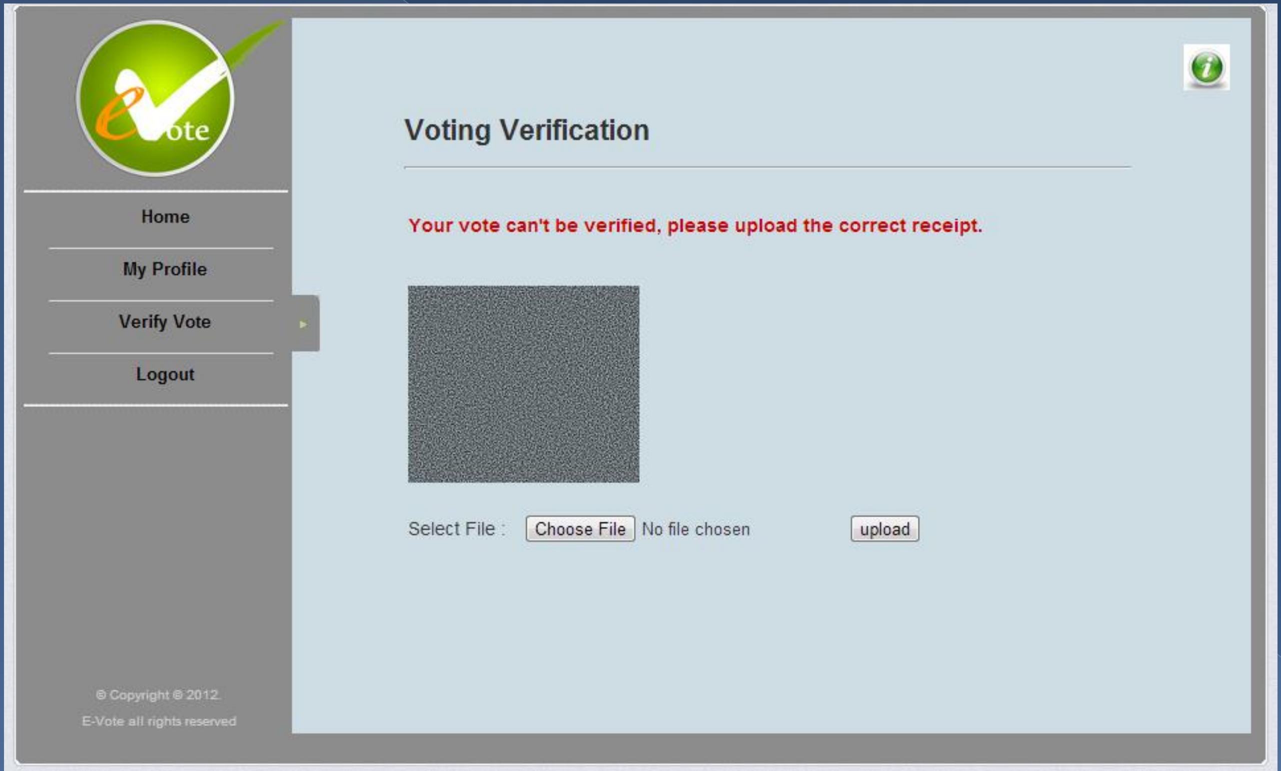
As polling officer you are eligible to make some changes over voters' details following election.

Election Name:	Election
Date Started:	11/11/12 10:49 PM
Date Ended:	11/11/12 10:49 PM

Please take note that your activities are recorded in system administrators' archive

To retrieve tally, please insert your secret key. You can only access this feature once election ended and all the distributed secret keys are collected.

Fig. 5 Homepage of eVote voting system (officer's level)



Voting Verification

Your vote can't be verified, please upload the correct receipt.

Select File : Choose File No file chosen

Fig. 6 eVote system voting verification feature.

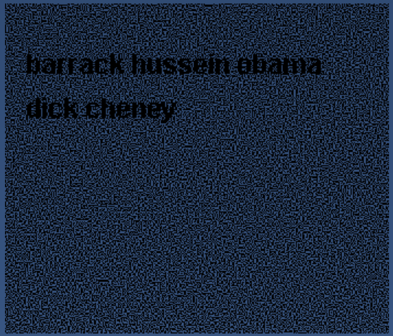


Fig. 7 eVote's sample ballot receipt

E2E System Requirements and Threats

- Requirements:
  - Functional Requirements
  - Usability Requirements
  - Security Requirements

- Threats:
  - Internal Threats Sources
  - External Threats Sources
    - Randomization Attack
    - Simulation Attack
    - Forced-abstention Attack
    - DoS Attack

Comparison and Results

- Comparison of E2E Voting Systems based-on E2E System Requirements

Measurement		Helios	Scantegrity II	PV	RIES	eVote
System Requirements	Functionality Requirements	High	High	Med	Med	High
	Usability Requirements	Low	Med	Med	Med	Med
	Security Requirements	High	Med	Low	Med	High

Comparison and Results

- Comparison of E2E Voting Systems based-on its Defense Mechanism against External Threats Sources

Threats		Helios	Scantegrity II	PV	RIES	eVote
External Threat Sources	Randomization Attack	No	Yes	Yes	Yes	No
	Simulation Attack	Yes	No	Yes	No	Yes
	Forced-absention Attack	Yes	Yes	Yes	Yes	No
	DoS Attack	Yes	Yes	Yes	Yes	Yes

Conclusion

- We believe the implementation of cryptography and steganography schemes in eVote system are sufficient to provide a secure, reliable and convenient voting system for medium range election.
- However, based on our comparison we found out that E2E voting systems are not fully resistant over attacks from the adversary. They can only fulfil a certain level of security.
- Ergo, flexible system would be the best option at this moment. The users could adjust the system easily according to their skills and requirements.

Q & A