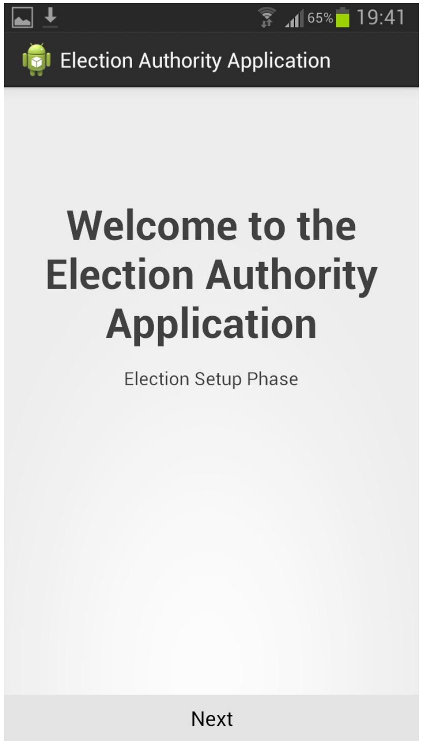
Election Authority Application

Oksana Kulyk, Stephan Neumann

TECHNISCHE UNIVERSITÄT DARMSTADT

SECUSO
SECURITY · USABILITY · SOCIETY

CASED
Usable Security Lab
Crypto Lab



Welcome to the Election Authority Application

Election Setup Phase

Motivation and Goals

Motivation

- Distribution of trust between the election authorities

- Appropriate cryptographic protocols exist

- Only suboptimal solutions implemented

Goals

- Implement trust distribution
  - Distributed election key generation
  - Verifiable distributed decryption
- Design usable interfaces
- Develop education materials to explain
  - functionality
  - security

Project Setting

Helios-like voting scheme

- El-Gamal cryptosystem
- Election stages

1. Distributed election key generation
2. Casting personalized votes
3. Vote anonymization
4. Verifiable distributed decryption

Helios-like voting scheme

- El-Gamal cryptosystem
- Election stages

1. **Distributed election key generation (authorities)**
2. Casting personalized votes
3. Vote anonymization
4. **Verifiable distributed decryption (authorities)**

Election Setting

- Electoral districts with 1000 voters
- 5 election authorities
- Threshold of 3 authorities
- One head of the election authorities
- Non-experts in information security
- No established PKI

Design Decisions

Hardware & Software

- Android smartphones as platform
    - Practical
    - Widespread
    - Mobile internet always available

- Java with third-party libraries
    - aSmack for communication between users
    - SpongeCastle for standard cryptographic operations

Public key exchange

Part of group data exchange protocol in SafeSlinger

- Usability
  - Short authentication strings of 24 bits
  - Displayed to participants as three words from PGP list
- Security
  - Out-of-band comparison against Man-in-the-Middle attacks
  - Commitments round against collision attacks

Distributed key generation

Scheme proposed by Pedersen (1991)

- Optimal trade-off between secrecy and robustness
- Verifiability via commitment round
- Decentralized
- Semantically secure with El-Gamal (Cortier et al., 2013)

Verifiable distributed decryption

Pedersen's protocol applied to e-voting (Cramer et. al.)

- Optimal trade-off between secrecy and robustness
- Verifiability via zero-knowledge proofs
- Decentralized

Communication

Extensible Messaging and Presence Protocol (XMPP)

- Open source
- No restriction on the participants' location
- No limit on message length
- Possibility of adding custom message types

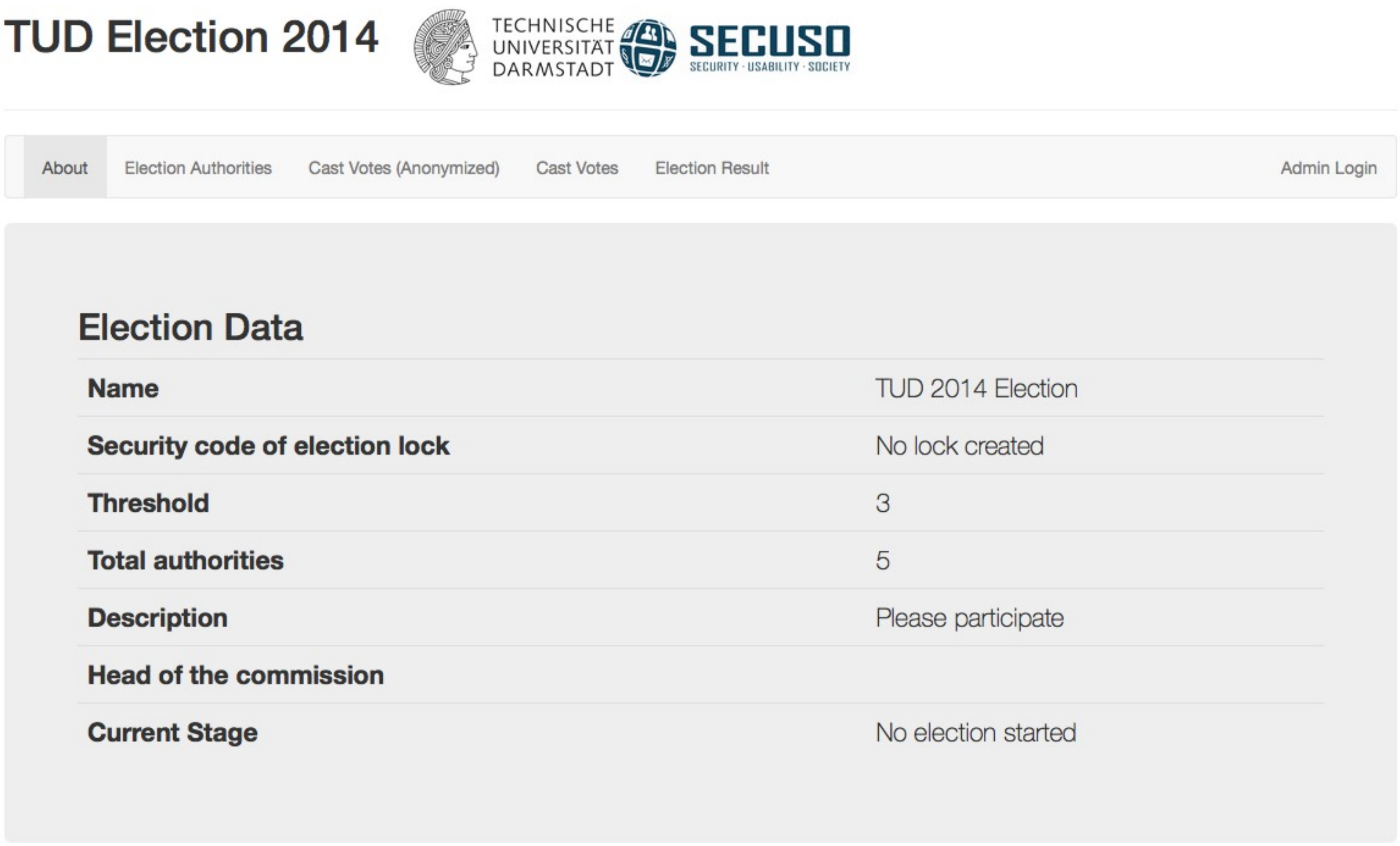
Public Information

Central web server (bulletin board)

- General information about the election
- A list of participating election authorities
- Public key for the election
- Cast votes
- Tallying results
- Zero-knowledge proofs of tallying results correctness

Workflow

Setup - Screenshots

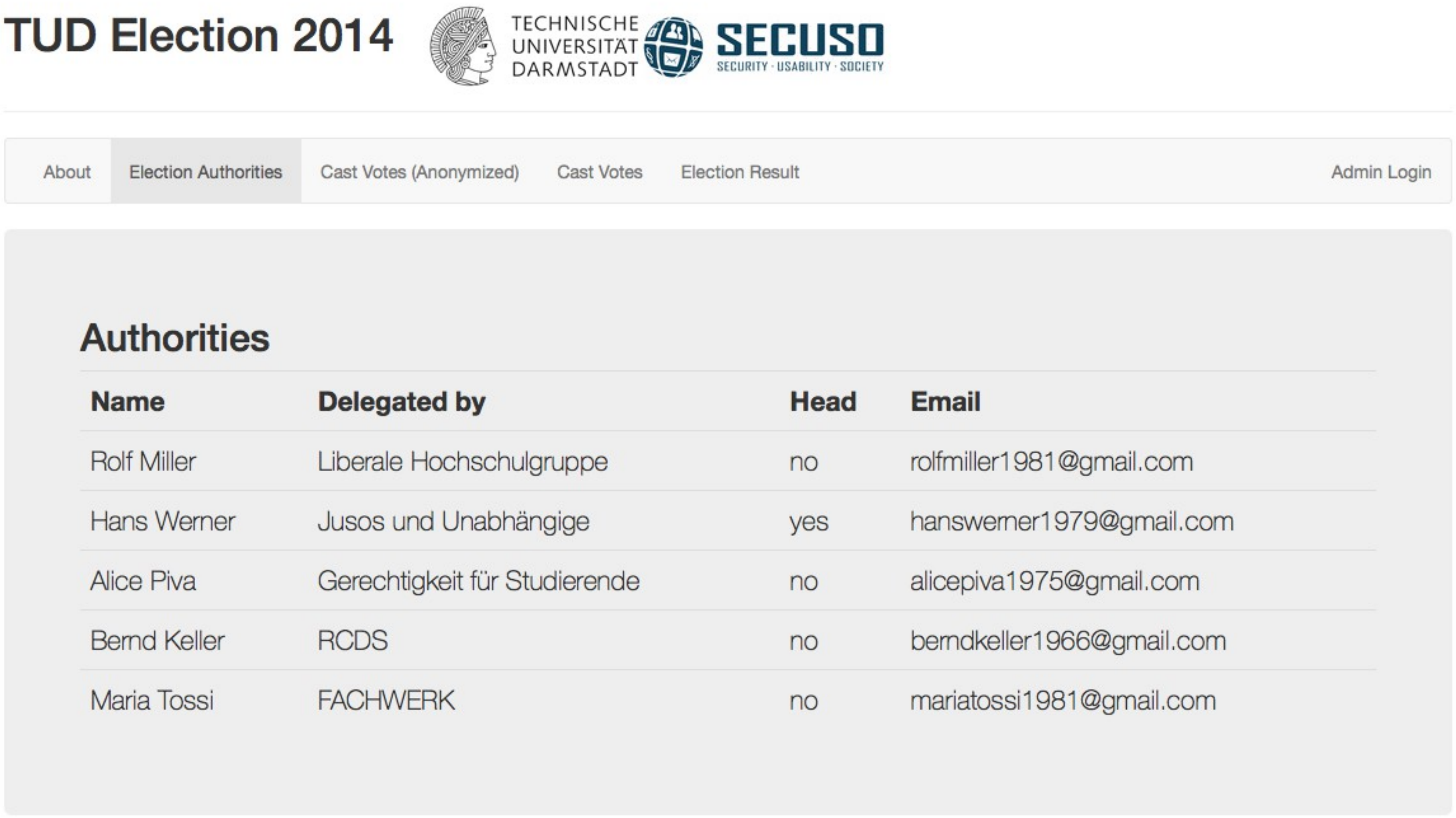


TUD Election 2014

Election Data

Name	TUD 2014 Election
Security code of election lock	No lock created
Threshold	3
Total authorities	5
Description	Please participate
Head of the commission	
Current Stage	No election started

Setup - Screenshots

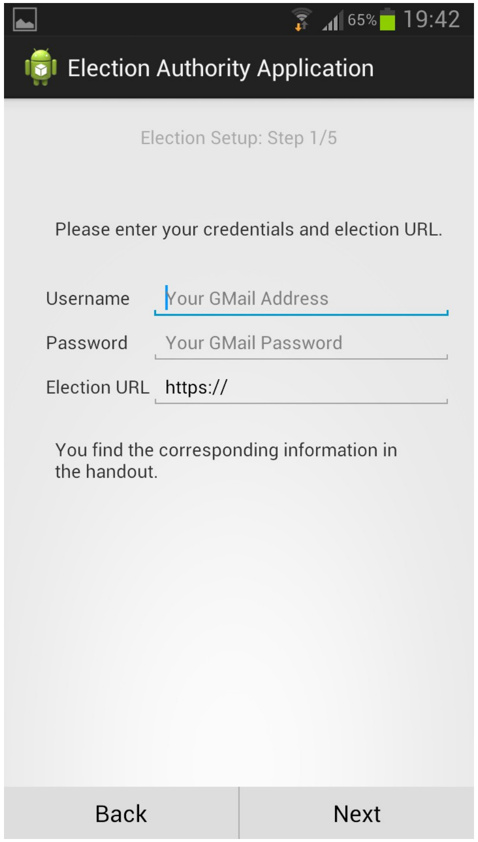


Authorities

Name	Delegated by	Head	Email
Rolf Miller	Liberale Hochschulgruppe	no	rolfmiller1981@gmail.com
Hans Werner	Jusos und Unabhängige	yes	hanswerner1979@gmail.com
Alice Piva	Gerechtigkeit für Studierende	no	alicepiva1975@gmail.com
Bernd Keller	RCDS	no	berndkeller1966@gmail.com
Maria Tossi	FACHWERK	no	mariatossi1981@gmail.com

Setup - Screenshots

Login



65% 19:42

Election Authority Application

Election Setup: Step 1/5

Please enter your credentials and election URL.

Username: Your GMail Address

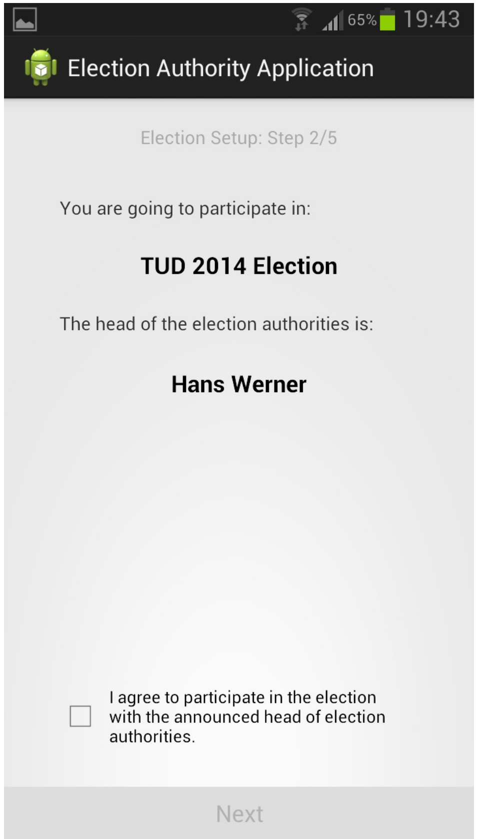
Password: Your GMail Password

Election URL: https://

You find the corresponding information in the handout.

Setup - Screenshots

Election Information



65% 19:43

Election Authority Application

Election Setup: Step 2/5

You are going to participate in:

TUD 2014 Election

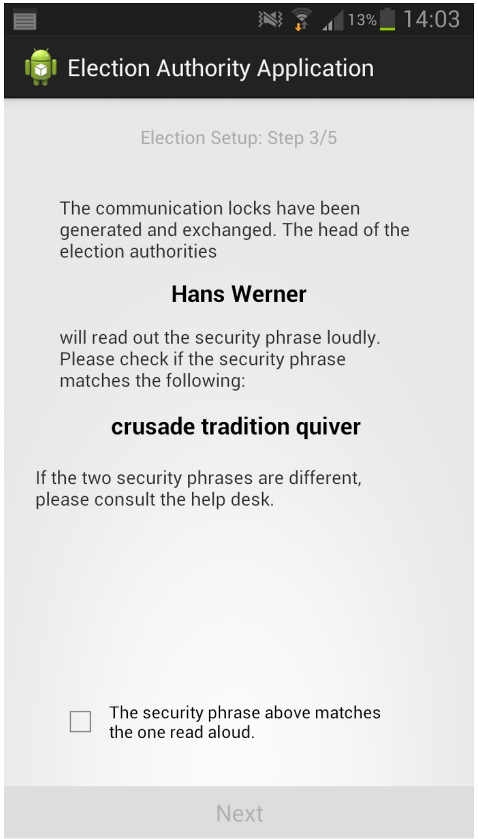
The head of the election authorities is:

Hans Werner

☐ I agree to participate in the election with the announced head of election authorities.

Setup - Screenshots

Public key exchange



Election Authority Application

Election Setup: Step 3/5

The communication locks have been generated and exchanged. The head of the election authorities

Hans Werner

will read out the security phrase loudly. Please check if the security phrase matches the following:

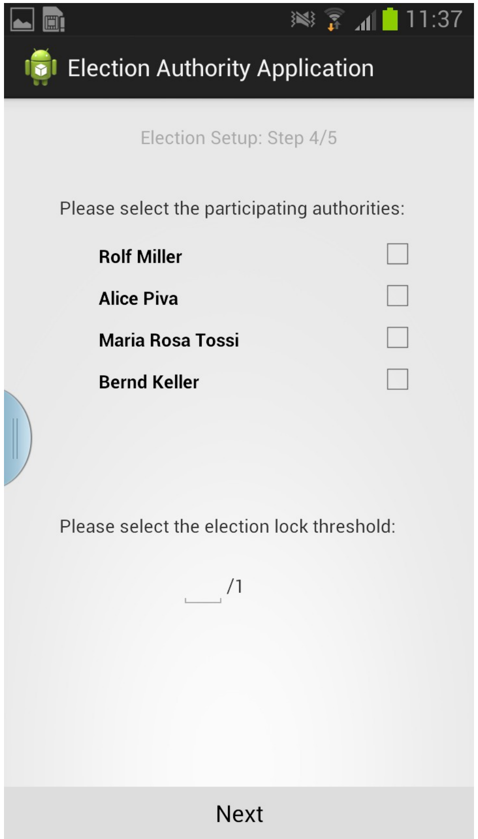
crusade tradition quiver

If the two security phrases are different, please consult the help desk.

□ The security phrase above matches the one read aloud.

Setup - Screenshots

Initiating distributed election key generation



11:37

Election Authority Application

Election Setup: Step 4/5

Please select the participating authorities:

Rolf Miller □

Alice Piva □

Maria Rosa Tossi □

Bernd Keller □

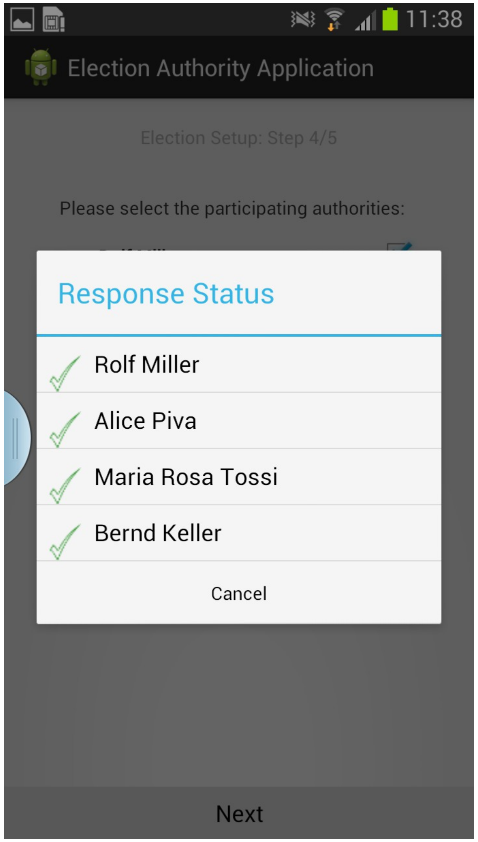
Please select the election lock threshold:

____ /1

Next

Setup - Screenshots

Initiating distributed election key generation



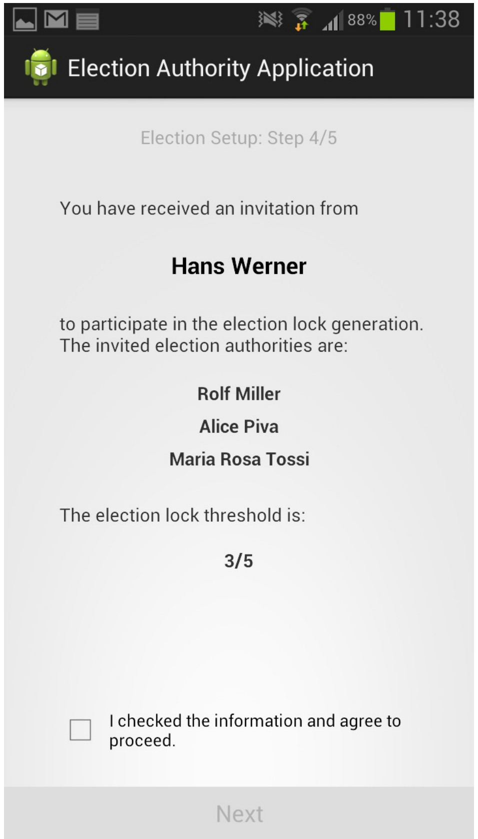
Election Authority Application

Election Setup: Step 4/5

Please select the participating authorities:

Response Status

- ✓ Rolf Miller
- ✓ Alice Piva
- ✓ Maria Rosa Tossi
- ✓ Bernd Keller



Election Authority Application

Election Setup: Step 4/5

You have received an invitation from

Hans Werner

to participate in the election lock generation.
The invited election authorities are:

Rolf Miller
Alice Piva
Maria Rosa Tossi

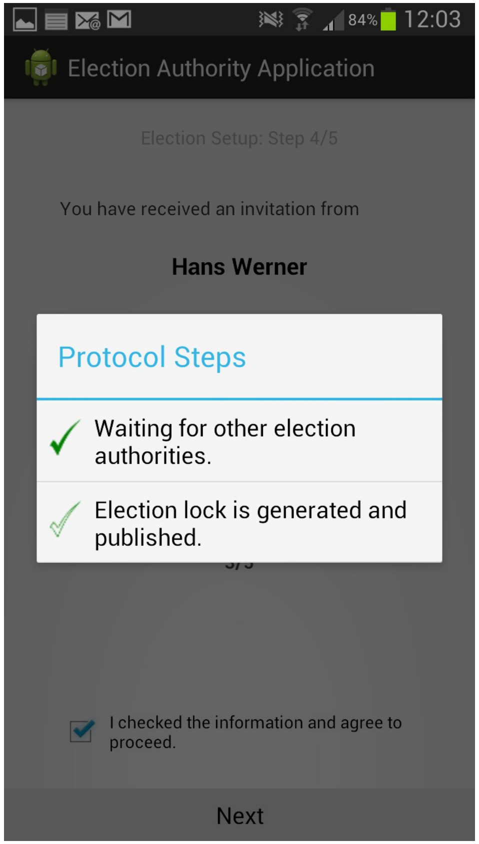
The election lock threshold is:

3/5

☐ I checked the information and agree to proceed.

Setup - Screenshots

Running distributed election key generation



84% 12:03

Election Authority Application

Election Setup: Step 4/5

You have received an invitation from

Hans Werner

Protocol Steps

✓ Waiting for other election authorities.

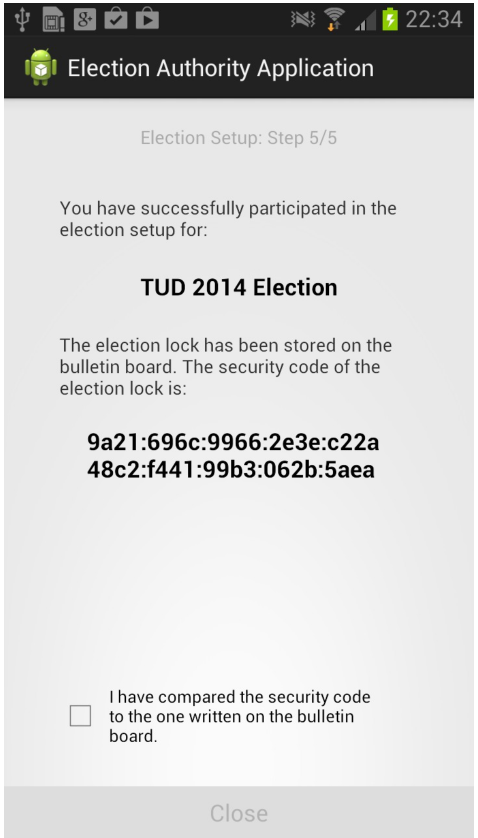
✓ Election lock is generated and published.

☑ I checked the information and agree to proceed.

Next

Setup - Screenshots

Distributed election key generation results



Election Setup: Step 5/5

You have successfully participated in the election setup for:

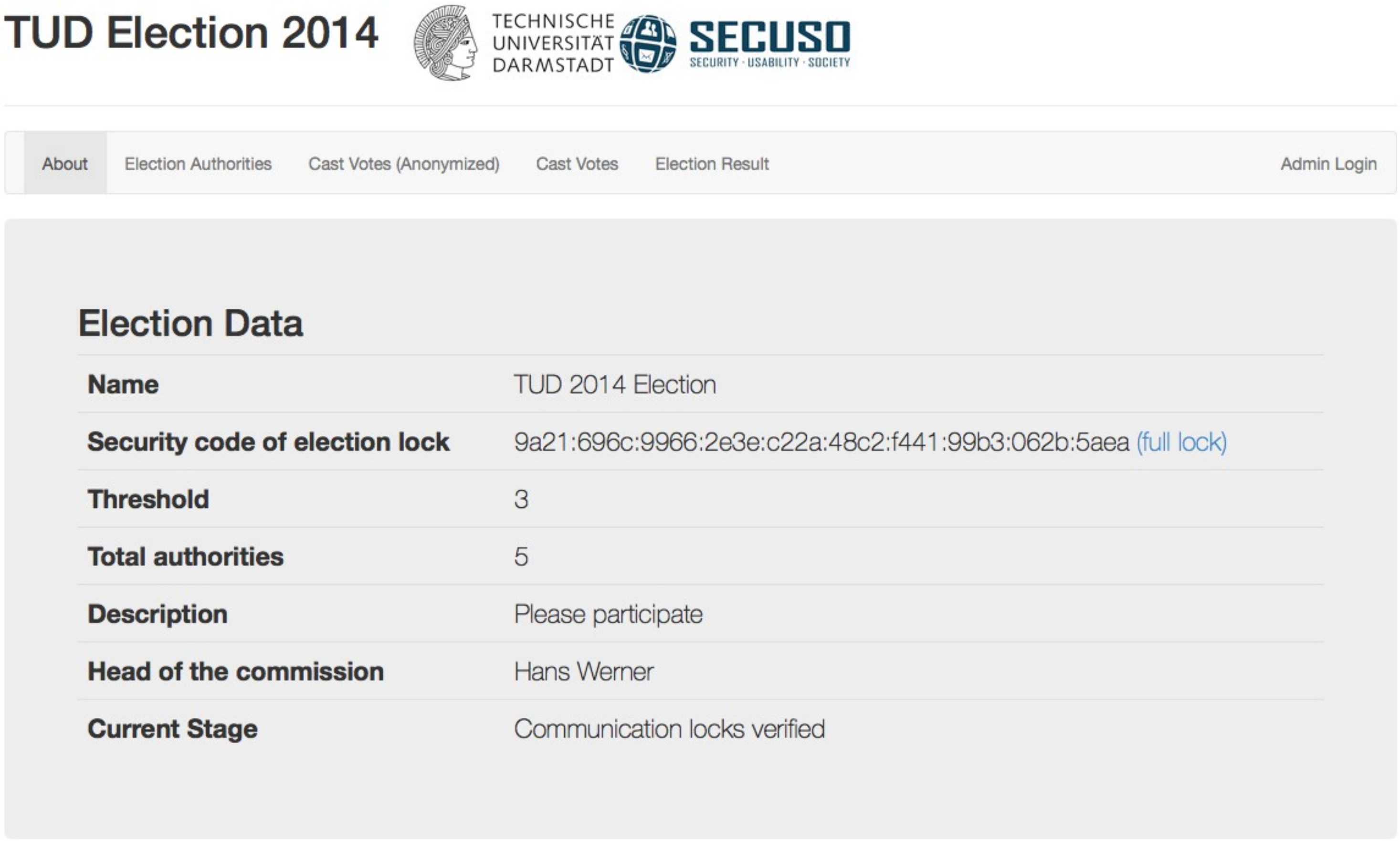
TUD 2014 Election

The election lock has been stored on the bulletin board. The security code of the election lock is:

9a21:696c:9966:2e3e:c22a
48c2:f441:99b3:062b:5aea

□ I have compared the security code to the one written on the bulletin board.

Setup - Screenshots

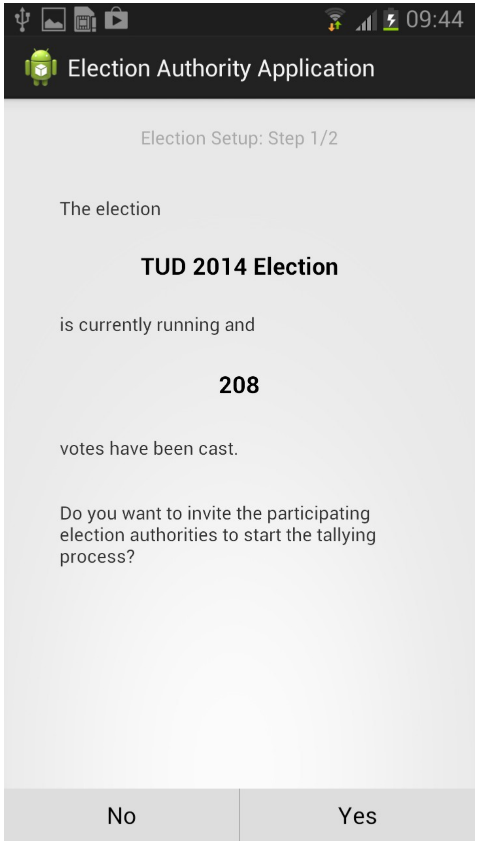


Election Data

Name	TUD 2014 Election
Security code of election lock	9a21:696c:9966:2e3e:c22a:48c2:f441:99b3:062b:5aea (full lock)
Threshold	3
Total authorities	5
Description	Please participate
Head of the commission	Hans Werner
Current Stage	Communication locks verified

Tallying - Screenshots

Initiating distributed decryption



Election Setup: Step 1/2

The election

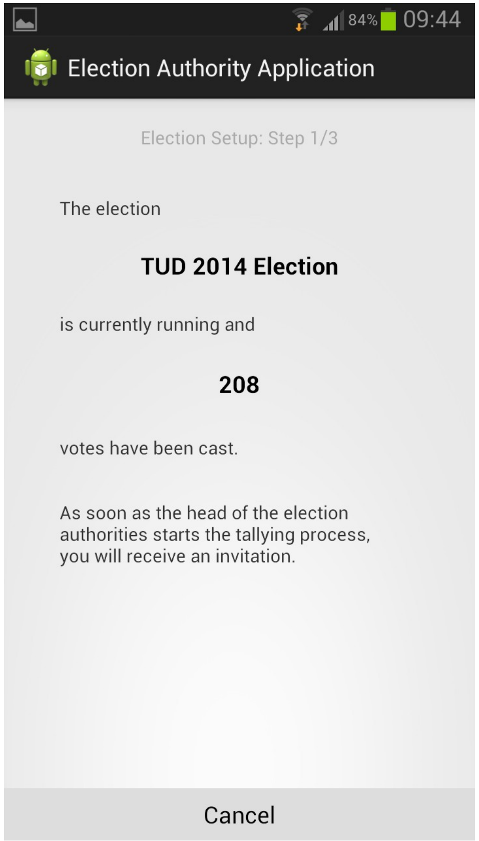
TUD 2014 Election

is currently running and

208

votes have been cast.

Do you want to invite the participating election authorities to start the tallying process?



Election Setup: Step 1/3

The election

TUD 2014 Election

is currently running and

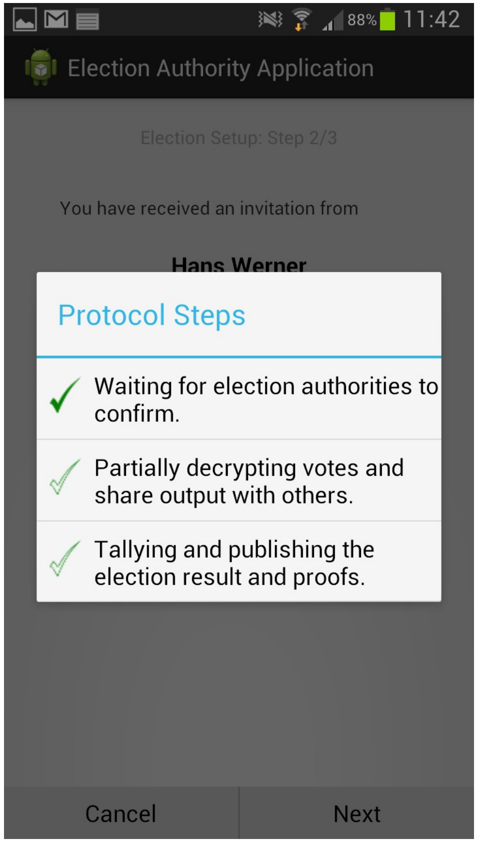
208

votes have been cast.

As soon as the head of the election authorities starts the tallying process, you will receive an invitation.

Tallying - Screenshots

Running distributed decryption



Election Authority Application

Election Setup: Step 2/3

You have received an invitation from

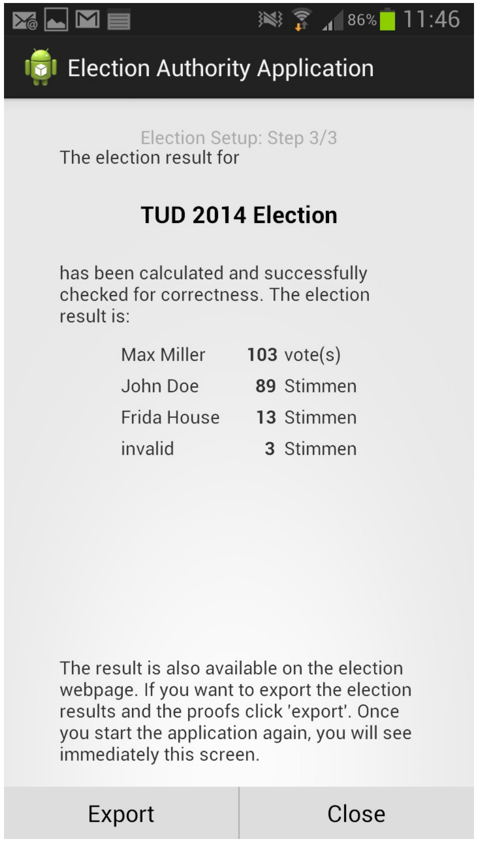
Hans Werner

Protocol Steps

- ✓ Waiting for election authorities to confirm.
- ✓ Partially decrypting votes and share output with others.
- ✓ Tallying and publishing the election result and proofs.

Tallying - Screenshots

Distributed decryption results



Election Setup: Step 3/3

The election result for

TUD 2014 Election

has been calculated and successfully checked for correctness. The election result is:

Max Miller	**103** vote(s)
John Doe	**89** Stimmen
Frida House	**13** Stimmen
invalid	**3** Stimmen

The result is also available on the election webpage. If you want to export the election results and the proofs click 'export'. Once you start the application again, you will see immediately this screen.

Security Model

Secrecy

- Definition: Inability to decrypt the personalized encrypted votes
- Assumptions
  - Threshold of election authorities honest
  - Trustworthy bulletin board
  - At least one mix node honest
  - Reliable cryptographic primitives

Integrity

- Definition: Detection if the decrypted and anonymized votes do not match
- Assumptions
  - Threshold of election authorities honest
  - Trustworthy bulletin board
  - Reliable cryptographic primitives

Robustness

- Definition: Possibility to decrypt the anonymized votes from the bulletin board
- Assumptions
  - Threshold of election authorities honest
  - Communication network between honest authorities and bulletin board available

Discussion

Discussion

- The application is work in progress
- Better solutions available?
  - More efficient protocols?
  - Ways to improve security model?
  - etc.
- Suggestions welcome!