Selene e-voting protocol: in your hand and in the booth

(E-Vote-ID 2017 - PhD Colloquium)

Marie-Laure Zollinger

Université du Luxembourg

October 24, 2017

Table of contents

Election set-up

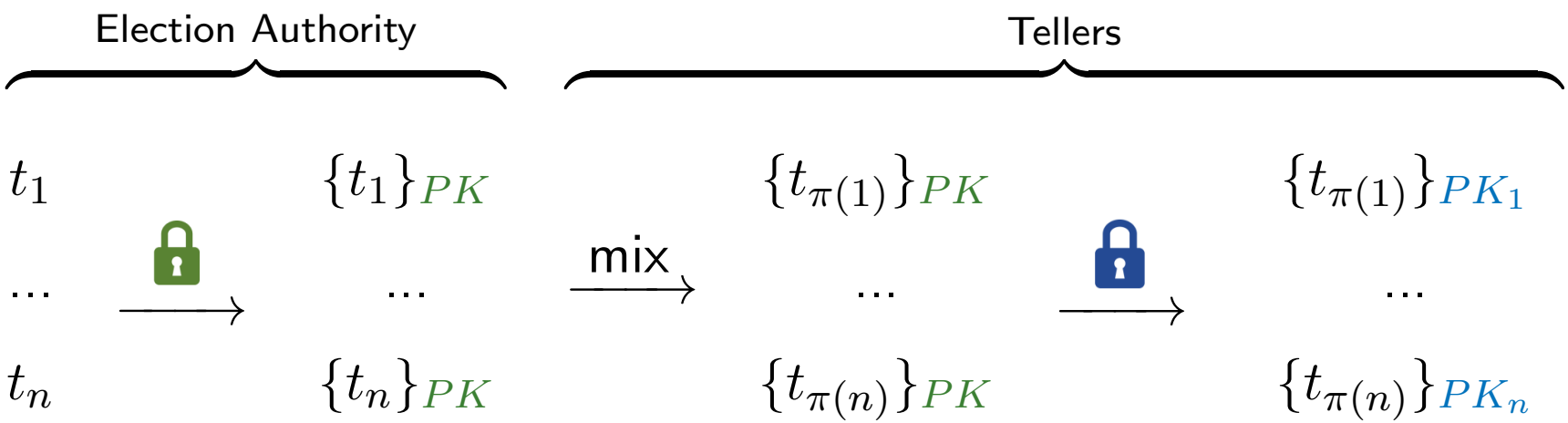
Selene is an e-voting protocol that notifies voters with a tracking number after the tally has been published.

Participants:

- Voters: public and secret keys,
- Election Authority: election public key,
- Bulletin Board: encrypted tracking numbers, voters public keys, commitments,
- Tellers: election secret keys, transcription of tracking numbers with voters keys

Trackers transcription

- Election authority key PK
- Voters key PK_i
- El-Gamal Encryption: $\{t_{\pi(i)}\}_{PK_i} = (\alpha, \beta)$ where β is the commitment

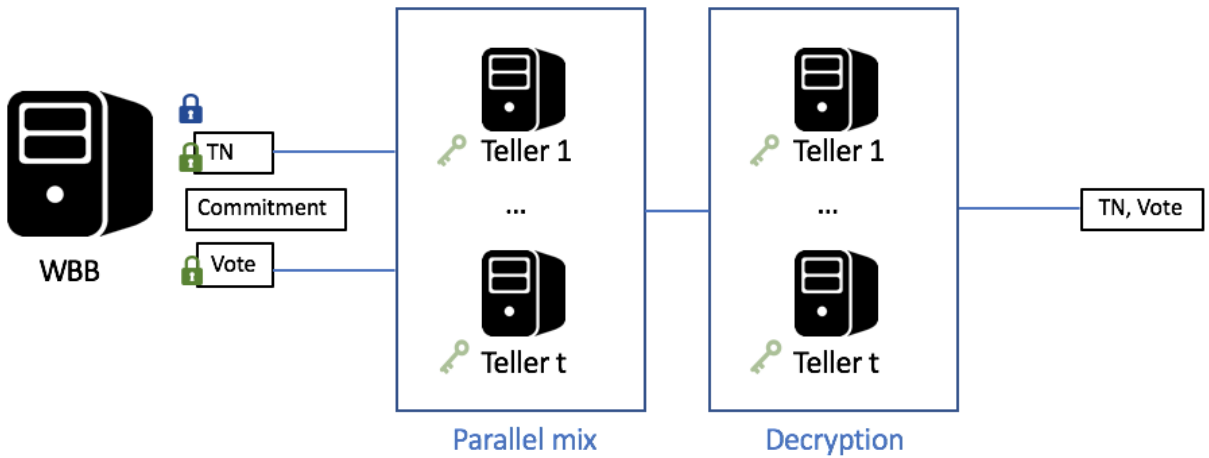


Protocol

1. A voter casts an encrypted vote.

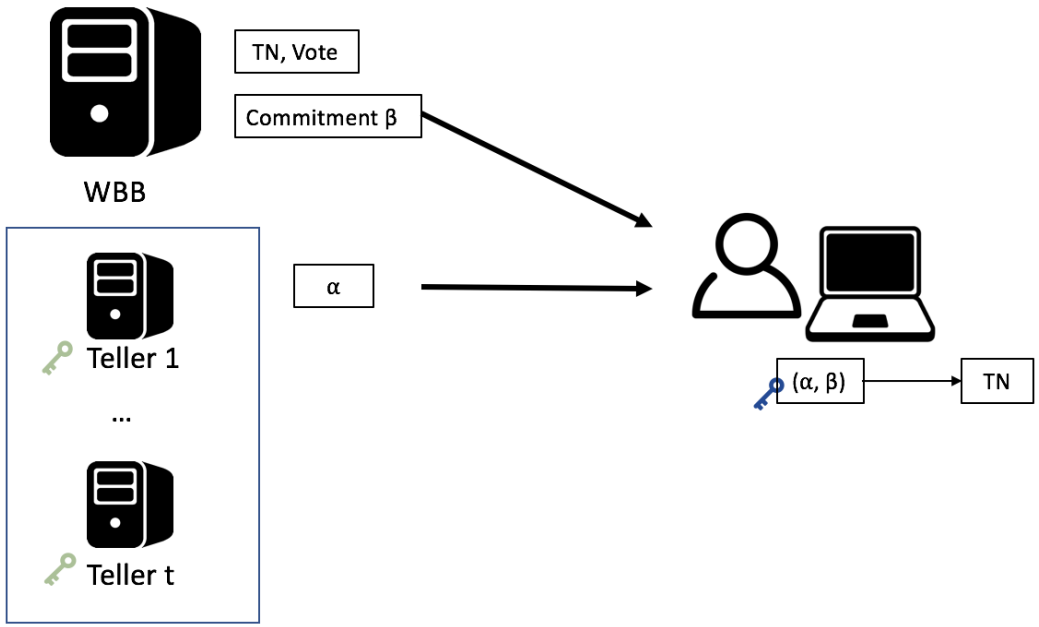
Protocol

1. A voter casts an encrypted vote.
2. The Tellers perform parallel mix and decryption of trackers and votes to extract the pairs (tracker,vote).



Protocol

1. A voter casts an encrypted vote.
2. The Tellers perform parallel mix and decryption of trackers and votes to extract the pairs (tracker,vote).
3. The Tellers notify the voters with the term α. The voter can calculate the decryption of their tracking number and verify her vote.



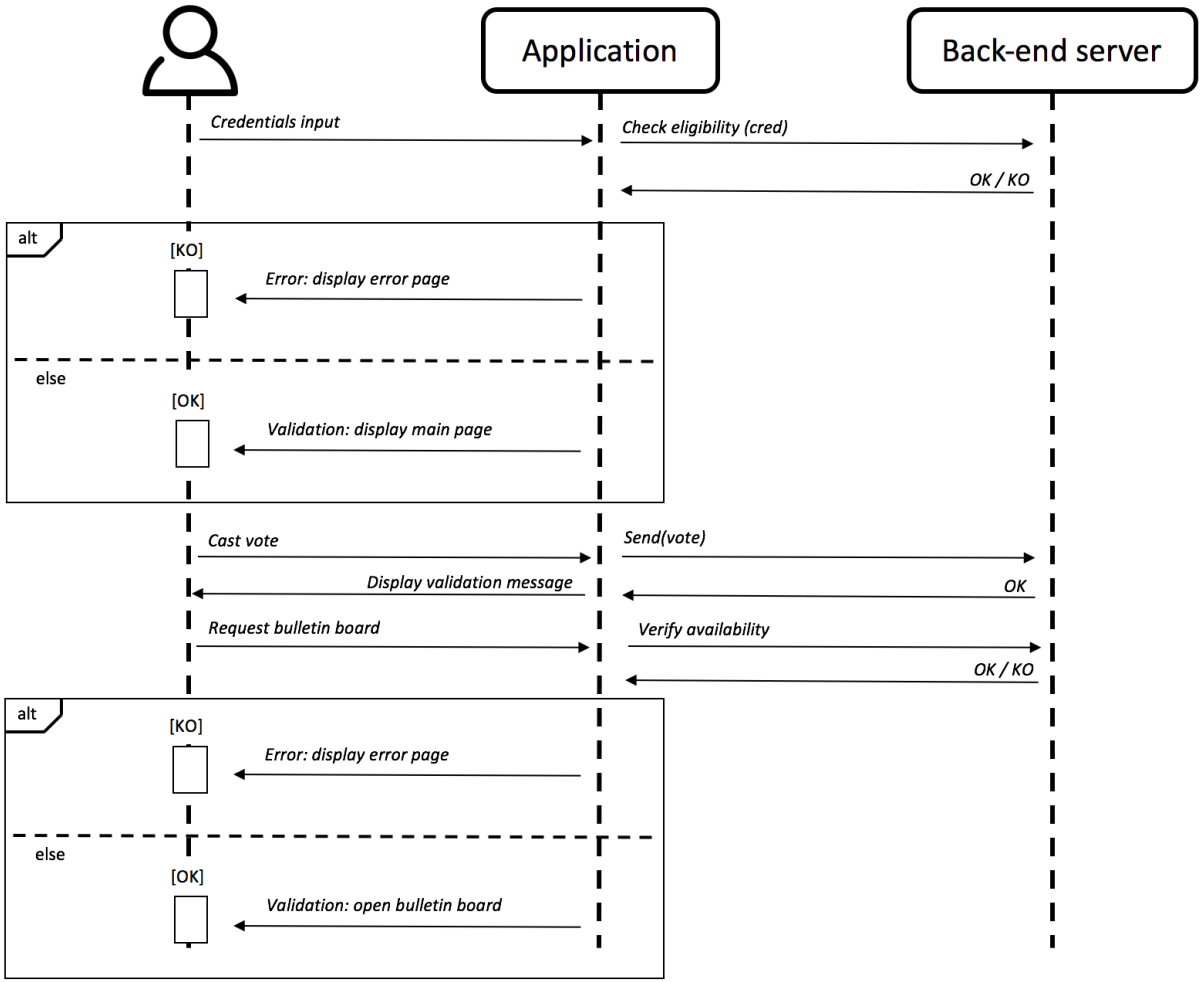
Goals

- Provide an adaptable mockup for Selene to test user experience
- Improve trust and confidence, by showing a good level of security
- Test usability of the app
- Work on the acceptance of the scheme

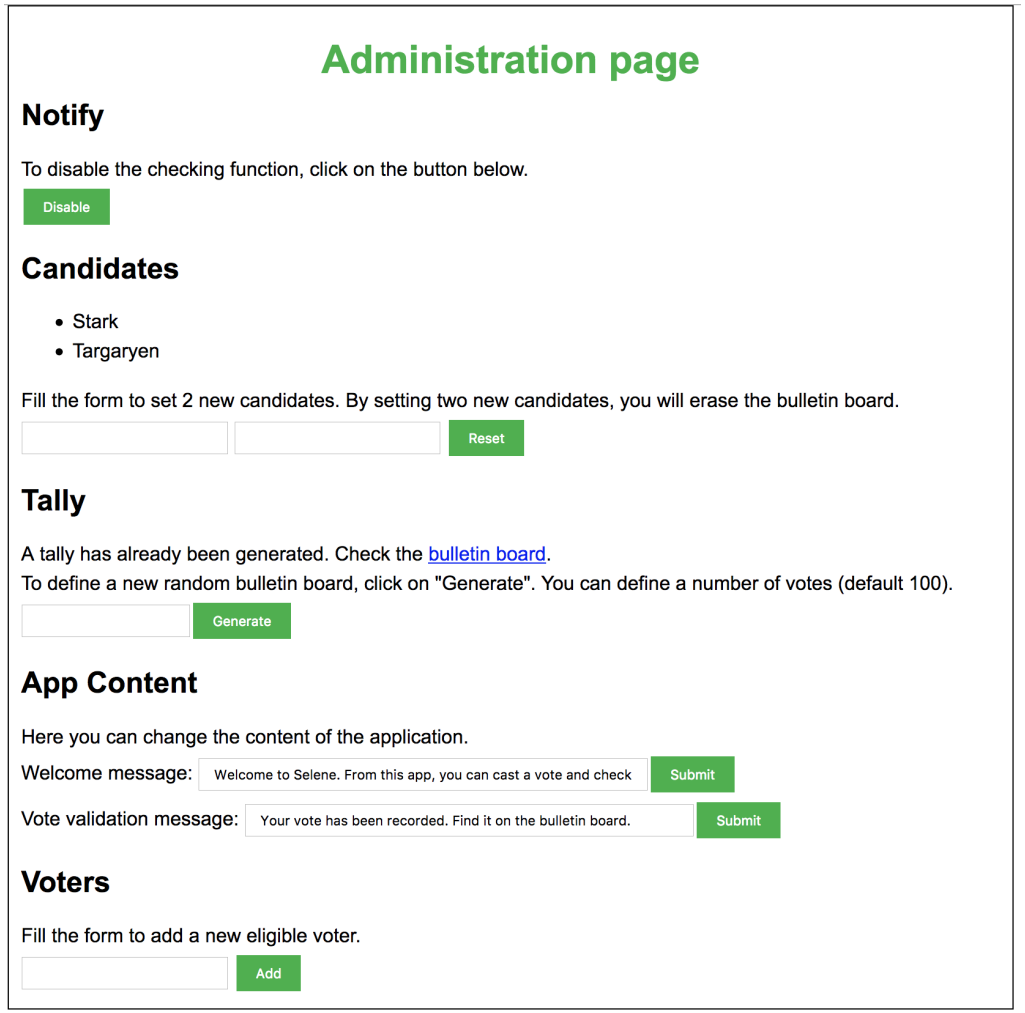
This project focuses on the verifiability aspect of Selene.
$\Rightarrow$ Cryptography aspects kept hidden

An implementation of Selene's security mechanisms has been done by Vincenzo Iovino in C language, and can be used as a library.

Design - Sequence diagram



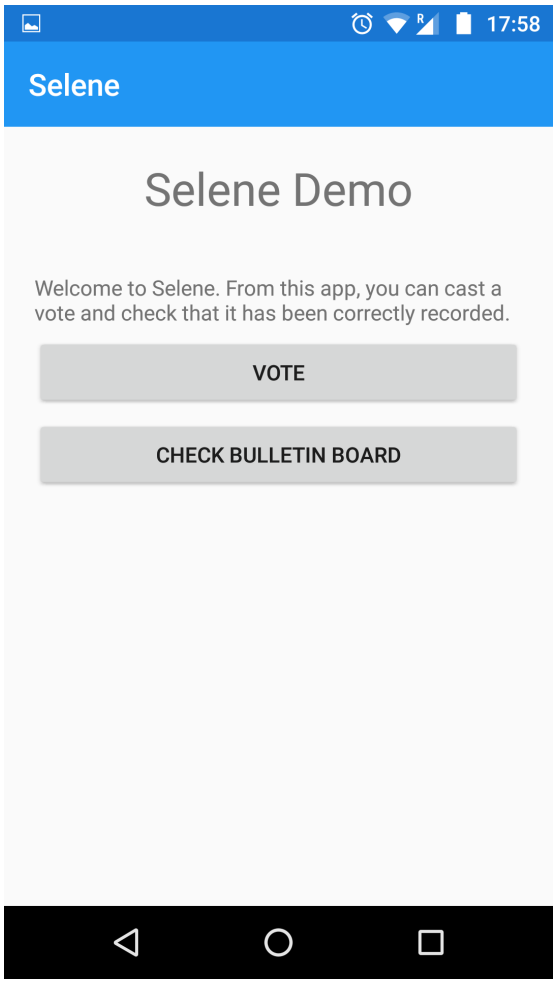
Administration



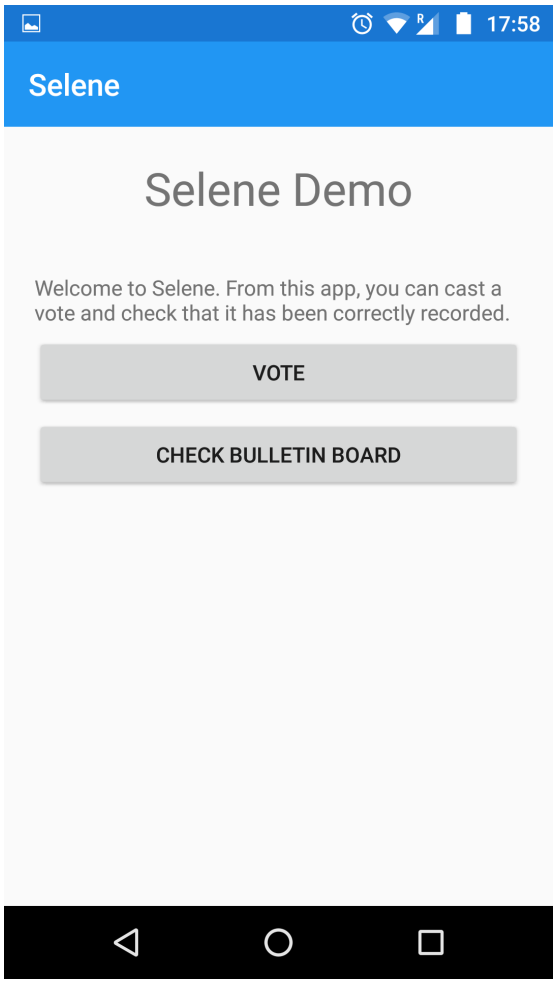
Application

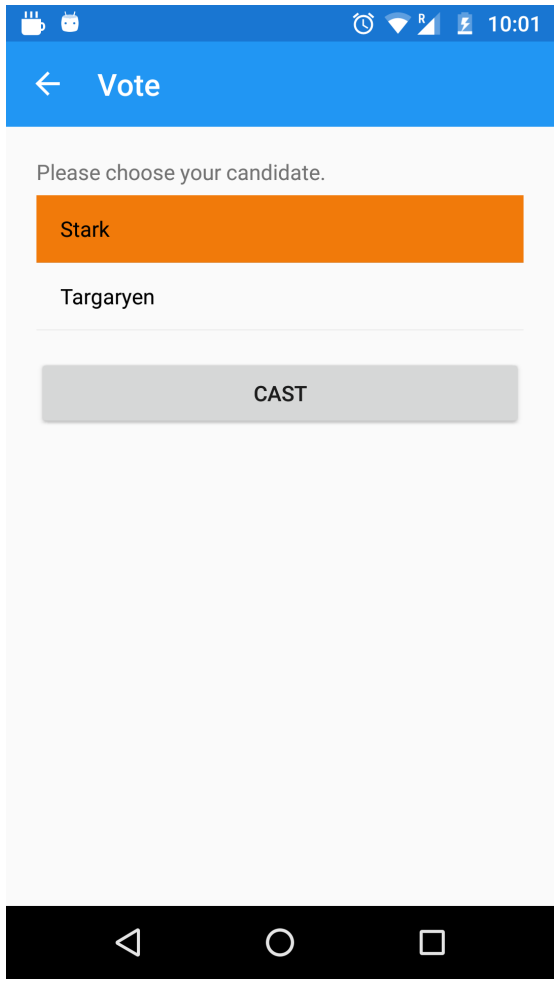
Application

Application



Application





Web bulletin board

Web Bulletin Board

We display here a set of votes. From your Selene app, you can know which one is yours.
The election result is: Targaryen with 2 votes, Stark with 7 votes
The winner is: Stark

Tracking number	Vote
1	Stark
2	Stark
3	Stark
4	Stark
5	Targaryen
6	Stark
7	Stark
8	Stark
9	Targaryen

Ideas

Short term

- Preparation phase: focus groups
- Improve the administration part
  → store data for a better data analysis
  → Bring more adaptable elements to configure the app

Long term

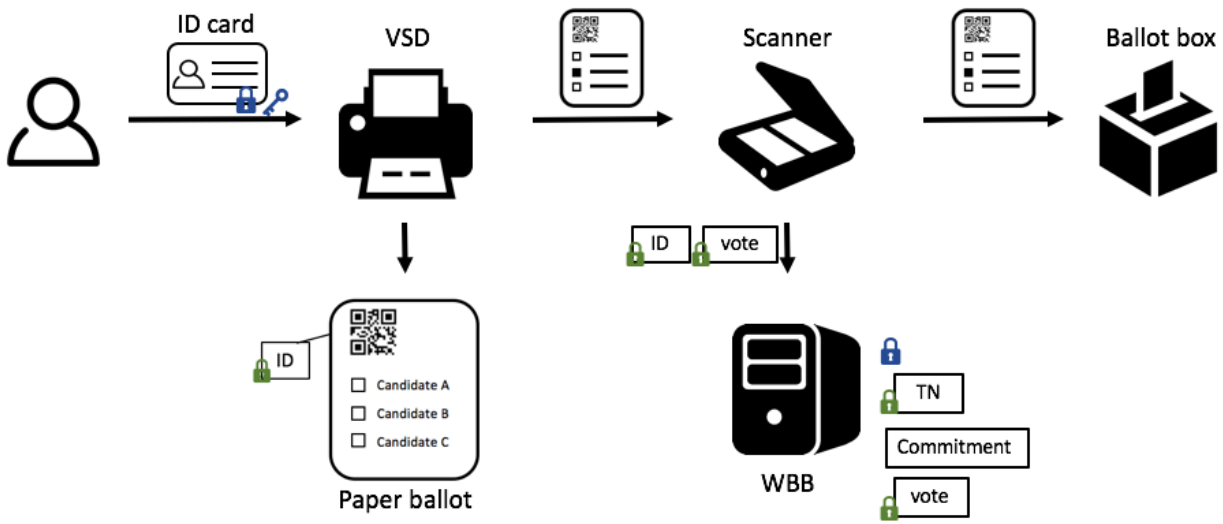
- Use Vincenzo's library that implements Selene's mechanisms
  → keys distribution, encryptions, decryptions, commitments
- Design a secure architecture for the bulletin board
  → accessibility
  → data storage
  → communication protocol

Selene in the booth

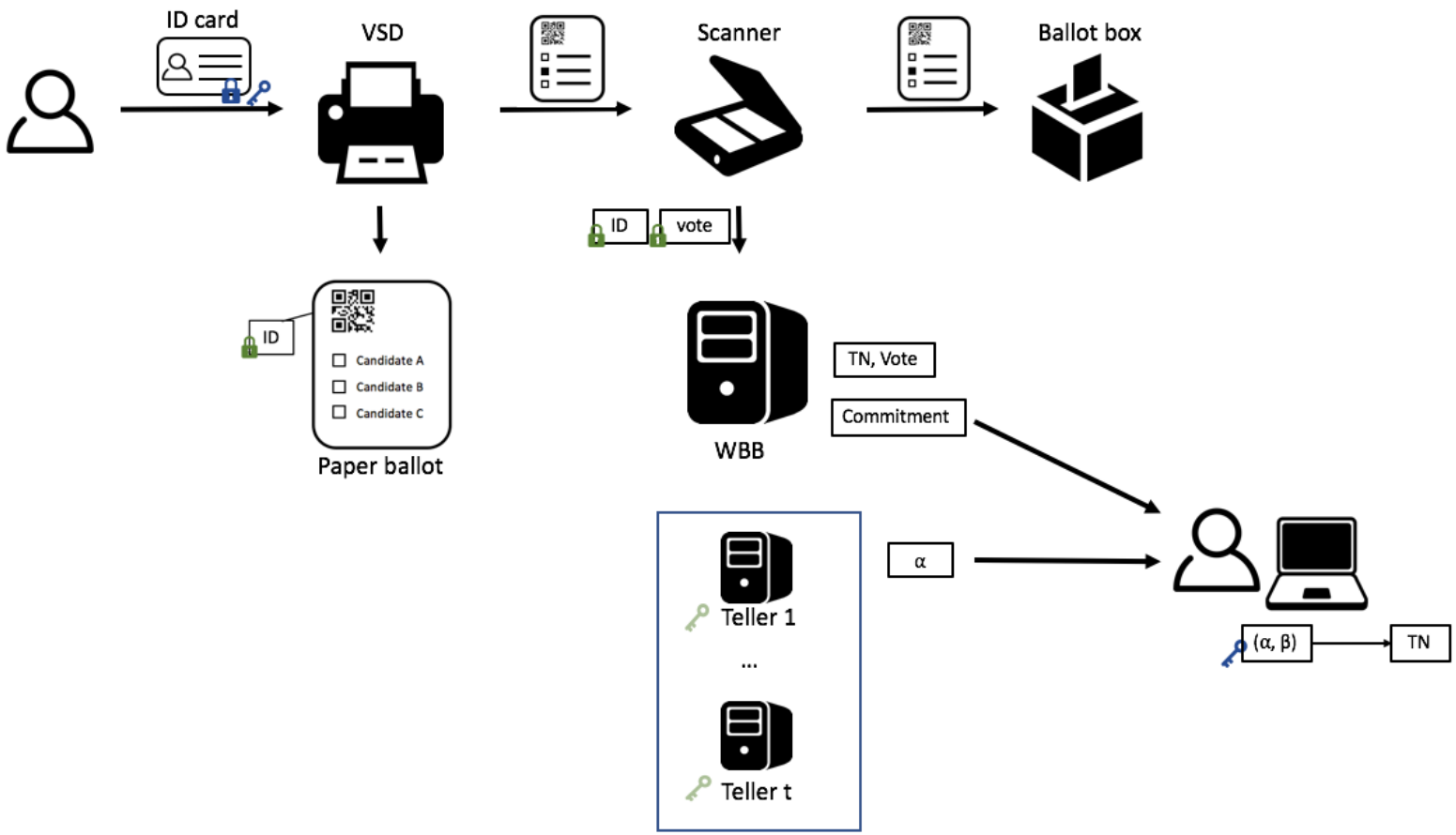
Goal

- Adapt Selene to in-booth voting scheme: from an individual voting process to a shared and public site
- Advantage: better coercion resistance
- Inconvenient: introduction of new issues
  $\Rightarrow$ How do we authenticate a voter to use her keys?
  $\Rightarrow$ How to notify the tracking number?
  $\Rightarrow$ How do we design the ballot?

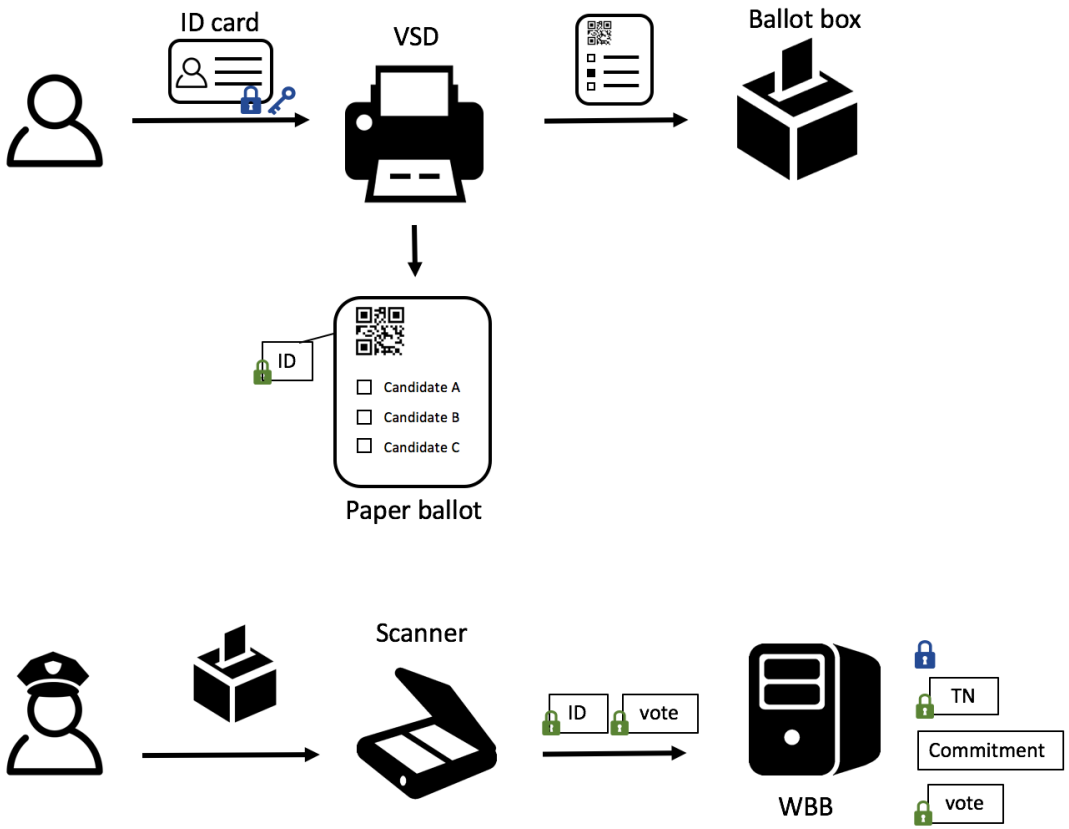
Workflow


ID card
VSD
Scanner
Ballot box
ID
vote
ID
Candidate A
Candidate B
Candidate C
Paper ballot
TN
Commitment
vote
WBB

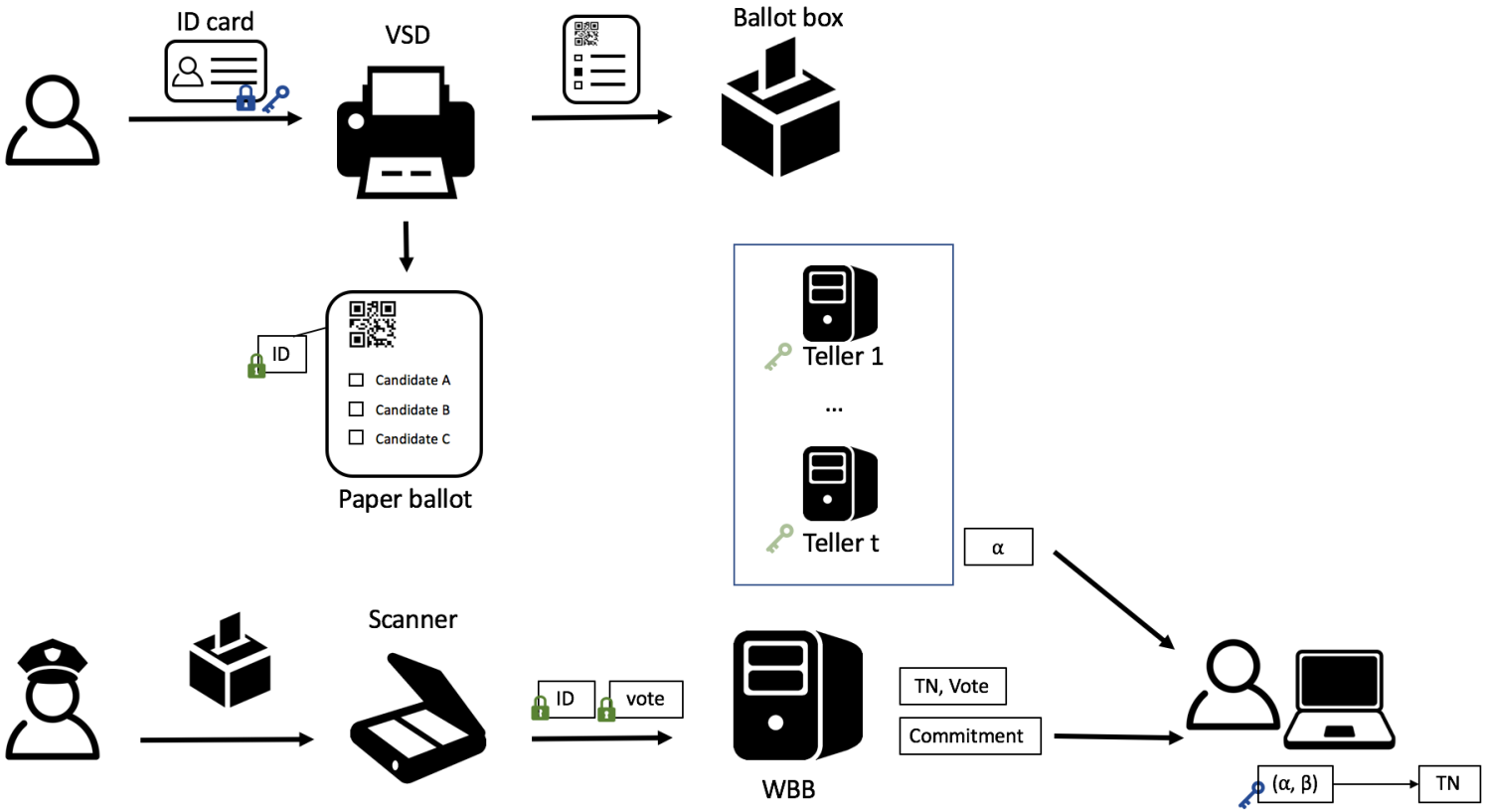
Workflow


ID card
VSD
Scanner
Ballot box
ID
vote
ID
Candidate A
Candidate B
Candidate C
Paper ballot
WBB
TN, Vote
Commitment
Teller 1
...
Teller t
α
(α, β)
TN

Workflow


ID card
VSD
Ballot box
ID
Candidate A
Candidate B
Candidate C
Paper ballot
Scanner
ID
vote
TN
Commitment
vote
WBB

Workflow


ID card
VSD
Ballot box
ID
Candidate A
Candidate B
Candidate C
Paper ballot
Teller 1
...
Teller t
α
Scanner
ID
vote
WBB
TN, Vote
Commitment
(α, β)
TN

Work in progress...

- ID card
  ⇒ Content definition: certificates, PIN codes, etc.
- Notification of the tracking number
  ⇒ Verification application for mobile?
  ⇒ Email/text message with tracker?
- Dispute resolution
  ⇒ Ballot proof: receipt to prove that a voter cast a ballot but cannot be used for verifiability purpose
  ⇒ Paper audit trail: RLA with comparison algorithm