

# Desirable Properties and Definitions



Johannes Buchmann and Melanie Volkamer



October 2009 | NIST-E2E-voting workshop | 1



## Verifiability Classes



- Plaintext receipt (on paper) → eg VVPAT
  - can be checked by the voter
  - must be put into the ballot box
  - can be used for manual recounts
- Encrypted receipt (probably also on paper) → E2E
  - can be taken home by the voter
  - can be used by the voter to verify on the bulletin board (BB) whether his vote has been altered or deleted
  - enables everyone to recount the result based on the BB

October 2009 | NIST-E2E-voting workshop | 2



## Verifiability Classes



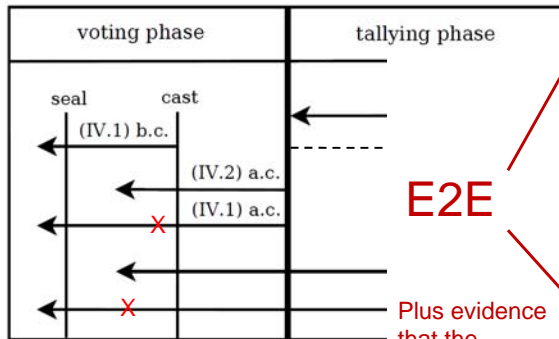
- Plaintext receipt (on paper ) → eg VVPAT
  - can be checked by the voter
  - must be put into the ballot box
  - can be used for manual recounts
- **Encrypted receipt (probably also on paper)→E2E**
  - can be taken home by the voter
  - can be used by the voter to verify on the bulletin board (BB) whether his vote has been altered or deleted
  - enables everyone to recount the result based on the BB

## Outline



- Definitions for verifiability requirements
- Additional requirements/open issues

## Definitions



UV.1: Continuous universal verifiability:  
Anyone can verify all parts of the correct processing of the ballots in tallying phase.

UV.1: Discrete universal verifiability:  
Anyone can verify certain (but not all) parts of the correct processing of the ballots in tallying phase.

IV.1: Inner individual verifiability: The voter can verify that his ballot contains the vote which the voter intended to cast.

IV.2 Outer individual verifiability: The voter can verify that his ballot has been published on the bulletin board, but he cannot verify that his ballot contains the vote which the voter intended to cast.

**E2E**  
Plus evidence that the sealed ballot contains the intended vote

b.c. – before casting  
a.c. – after casting  
a.t. – after tallying

## Not to forget ...



- Ensure election secrecy
  - without verifiability techniques? Hard to explain
  - plus receipt freeness, coercion resistance, long-term secrecy
- Handle complaints like
  - who has to provide the proof? (voter/authority)
  - which information is required? (plaintext votes)
  - what happens if voters wrongly claim that sth. went wrong?
  - how to prevent people to wrongly claim that results are wrong?

## Not to forget ... (2)



- Usability aspects
  - possible for people without specialist knowledge
  - not too many actions for the voter
  - not to compare too long (hash) strings
- Didactic aspects, how to communicate that
  - system is evaluated but additional mechanisms are required
  - additional steps are required after ballot casting
  - verifiability of pre-ballots ensures accuracy

## Not to forget ... (3)



- Impact on the Evaluation
  - Can some requirements be removed?
  - How to integrate verifiability requirements?
- Flexibility of Election Law
  - Are randomized candidate order possible?
  - Is vote-updating possible?

---

Thank you for your attention!  
Questions?

Contact  
[volkamer@cased.de](mailto:volkamer@cased.de)