Internet Voting Technology

Sven Heiberg, sven@ivotingcentre.ee

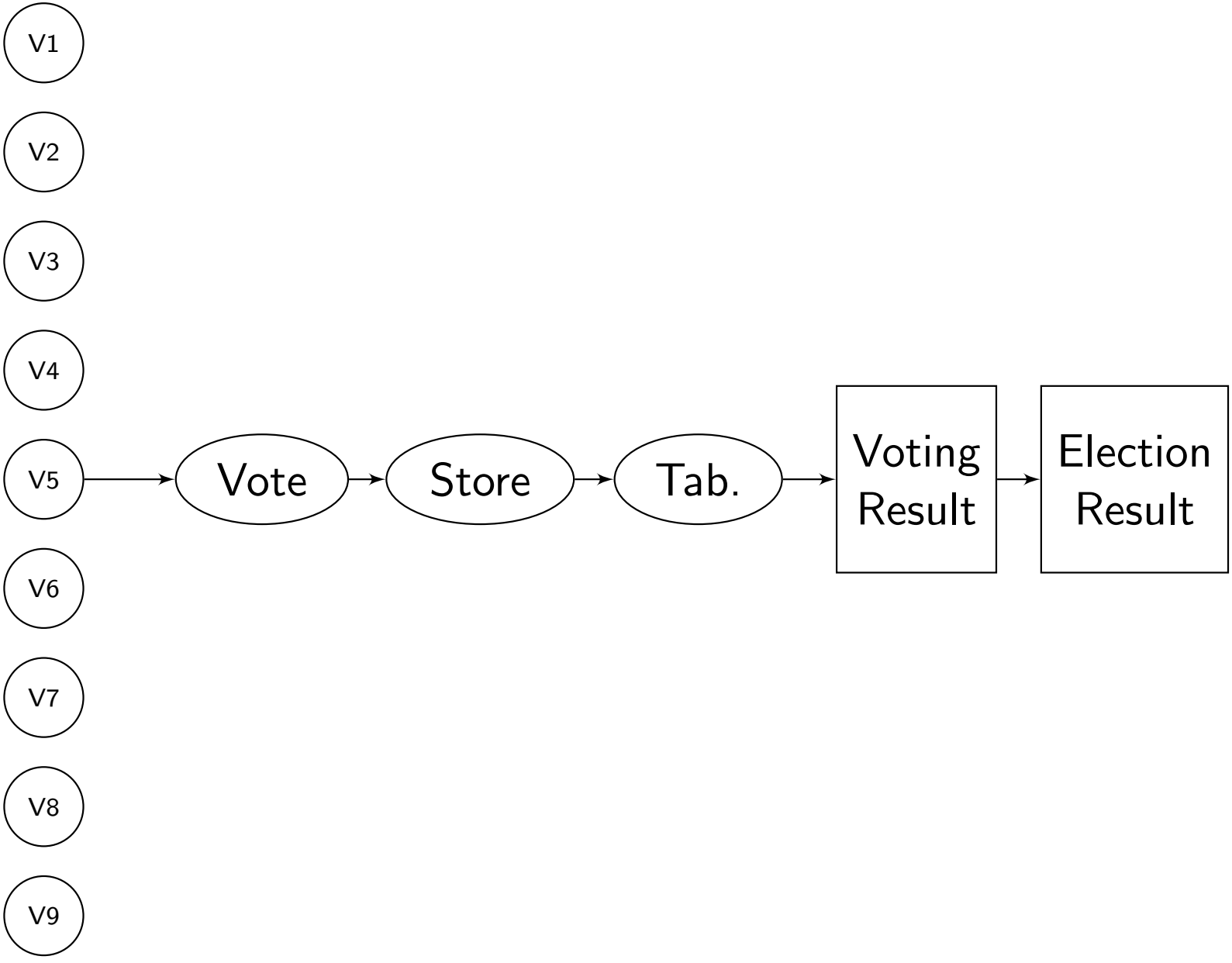
April 18th, 2017

Elections

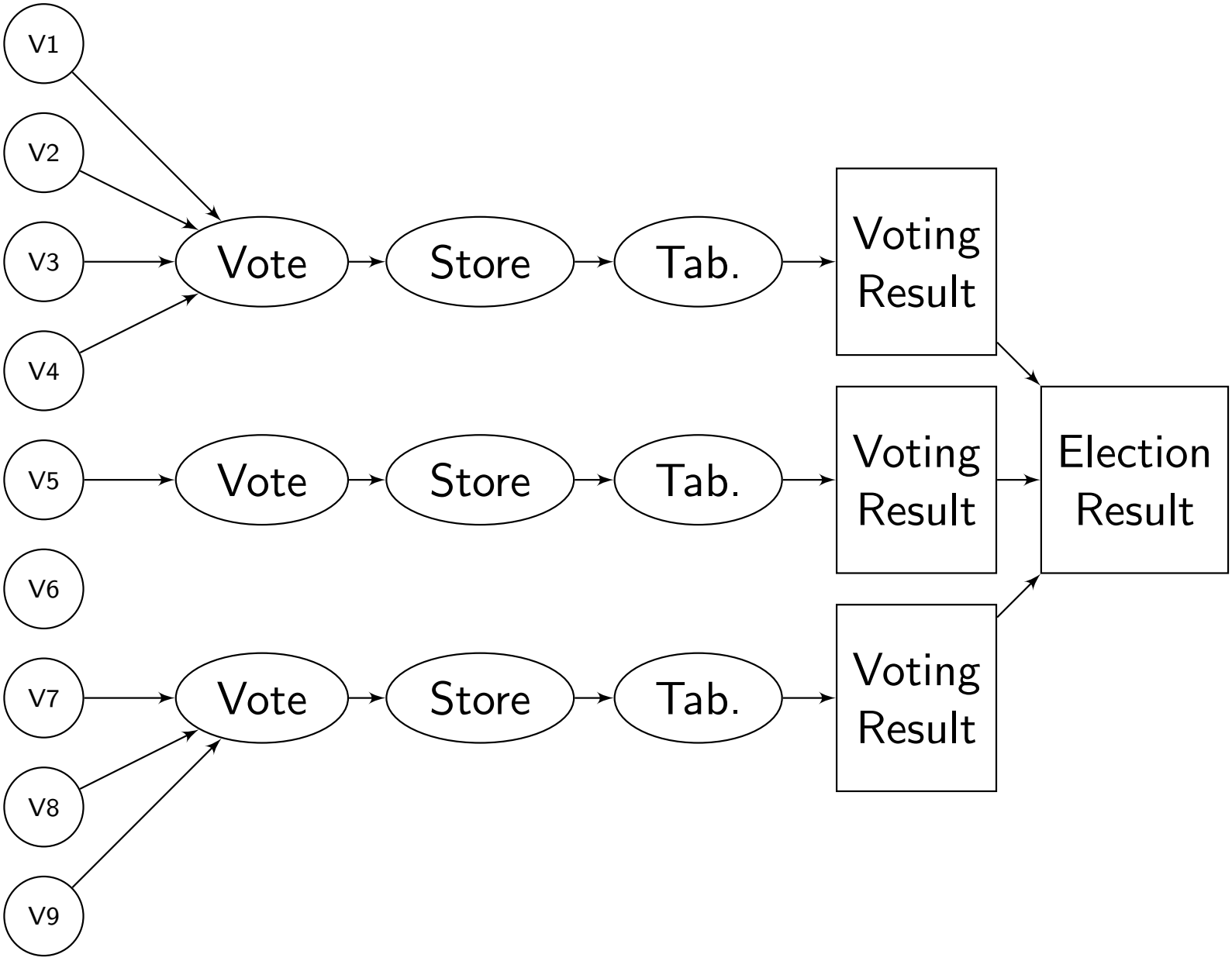
- §1 – Estonia is independent and sovereign democratic republic. The supreme power is vested in the people
- §56 – People exercise their power through citizens' right to vote
- Electoral systems determine the means by which the votes are translated into seats
- There is a pre-programmed conflict in every election
  - Transfer 900 000 opinions into 101 seats - this is lossy compression
- Voting methods determine the means by which votes are gathered from the elegible voters

Voting method in the election process

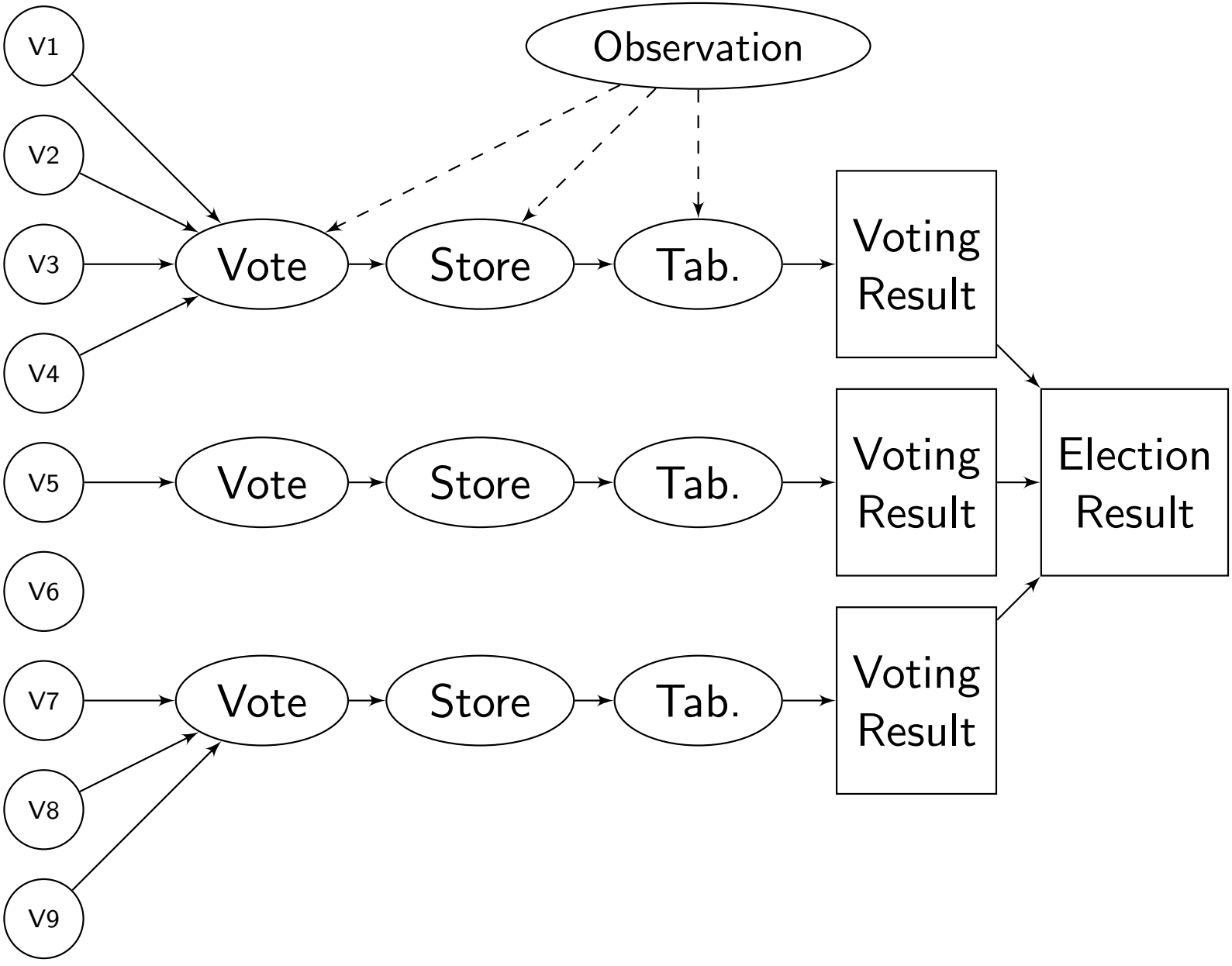
Voting method in the election process



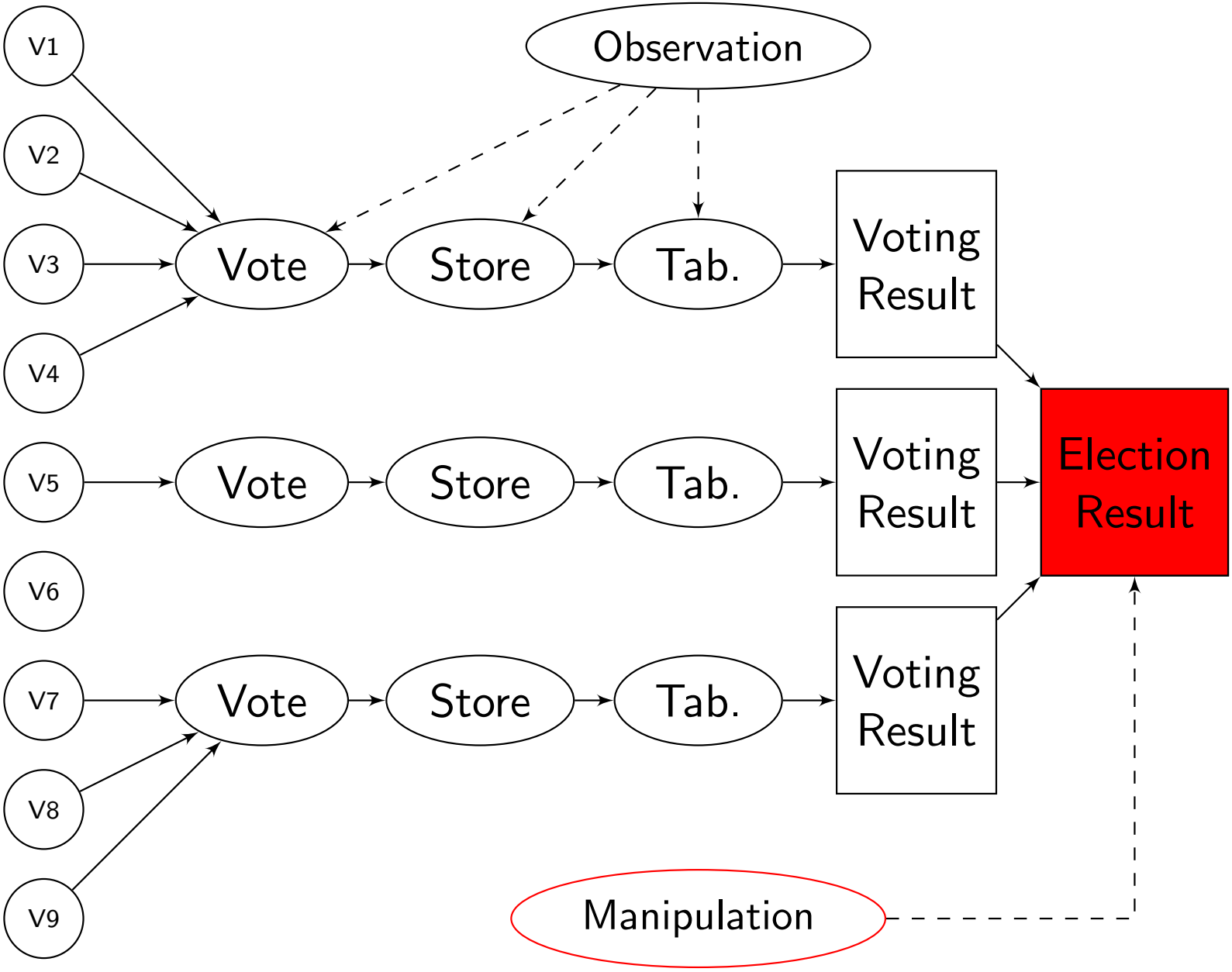
Voting method in the election process



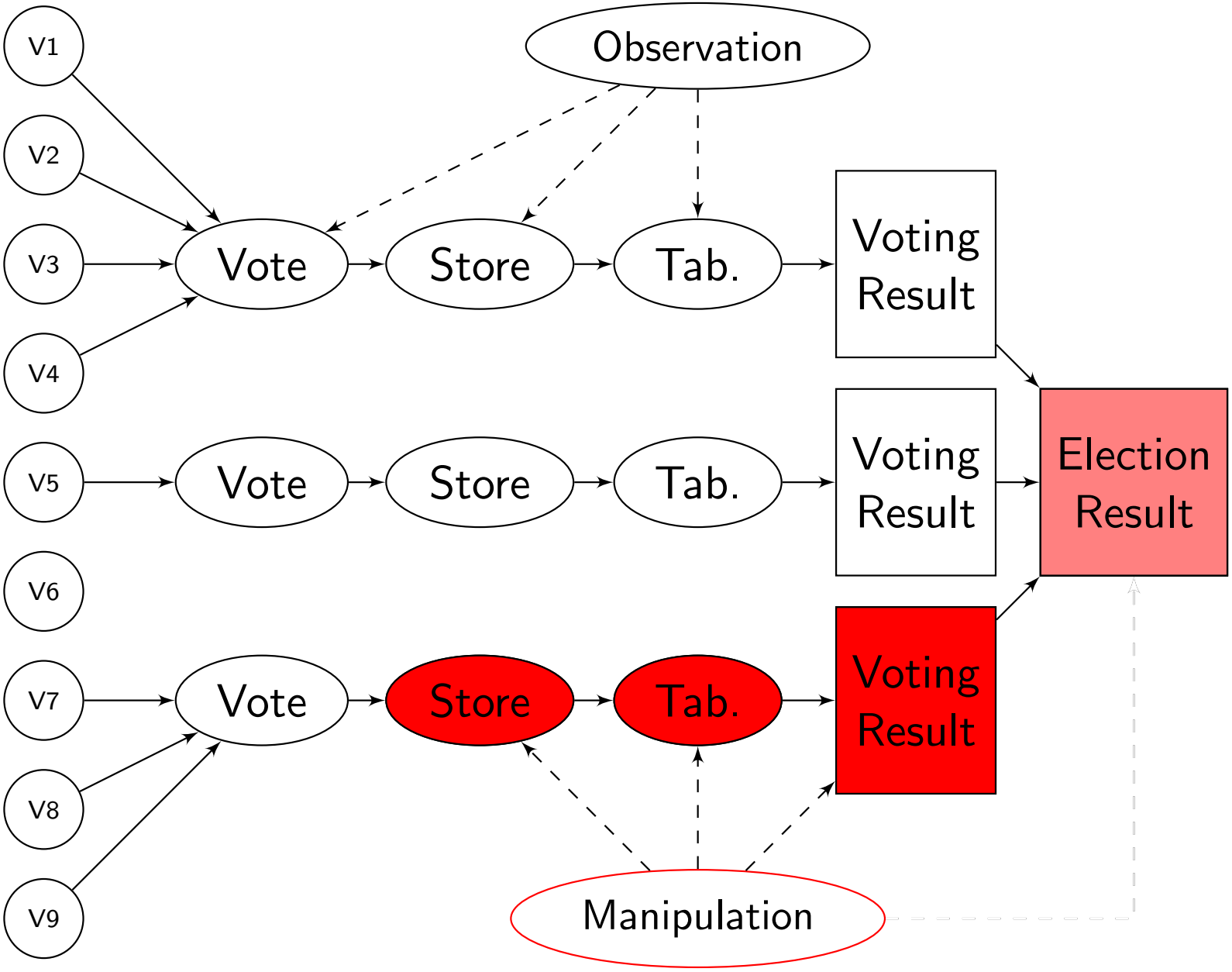
Voting method in the election process



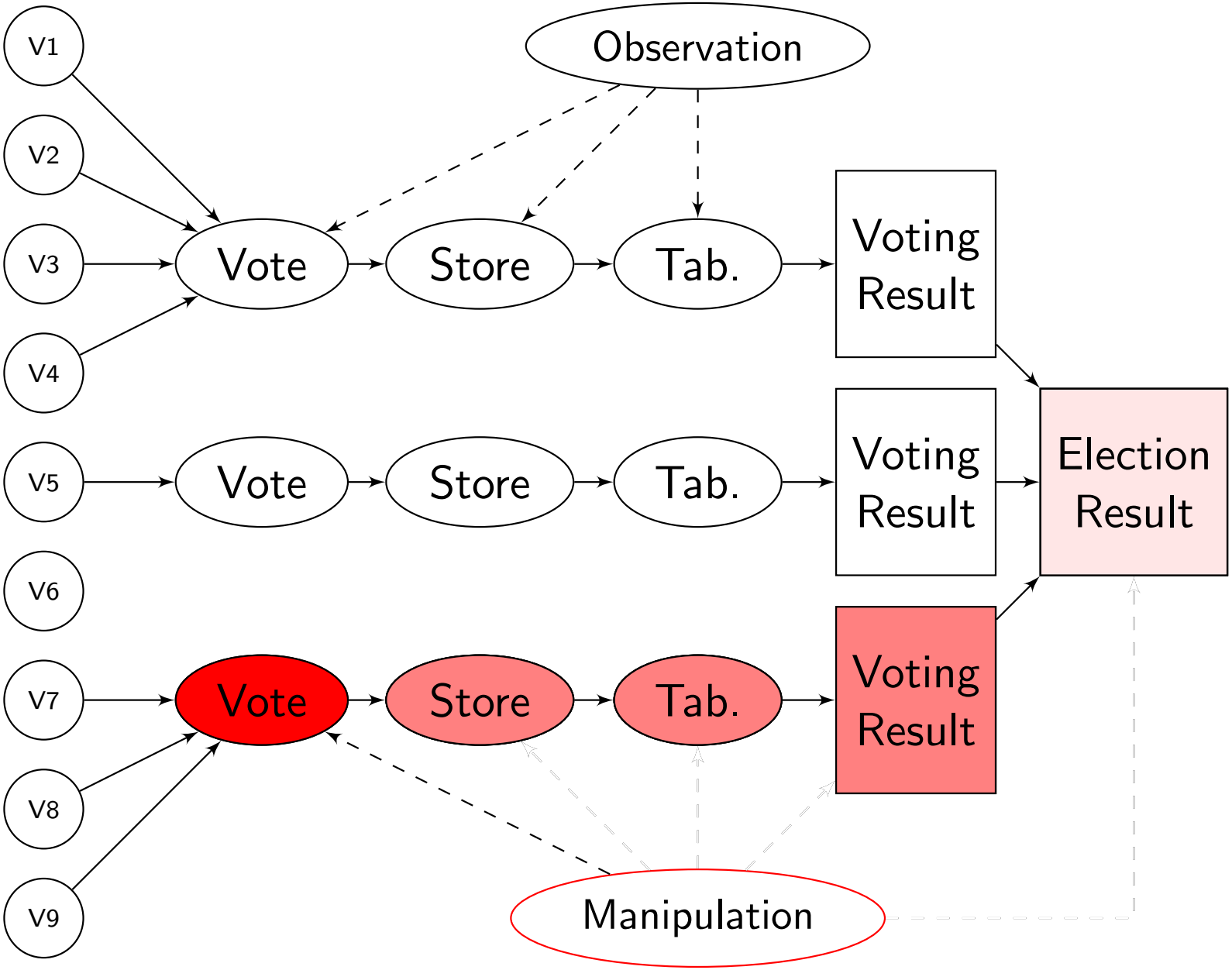
Voting method in the election process



Voting method in the election process



Voting method in the election process



General challenges with voting methods

- Integrity of the voting result
  - Eligibility assurance
  - Vote integrity throughout the process
  - Ballot-box integrity
  - Correct tabulation
- Confidentiality
  - Ballot secrecy
  - Voting result confidentiality
  - Coercion resistance
- The Challenge: How to find the right kind of balance between integrity, transparency and confidentiality?

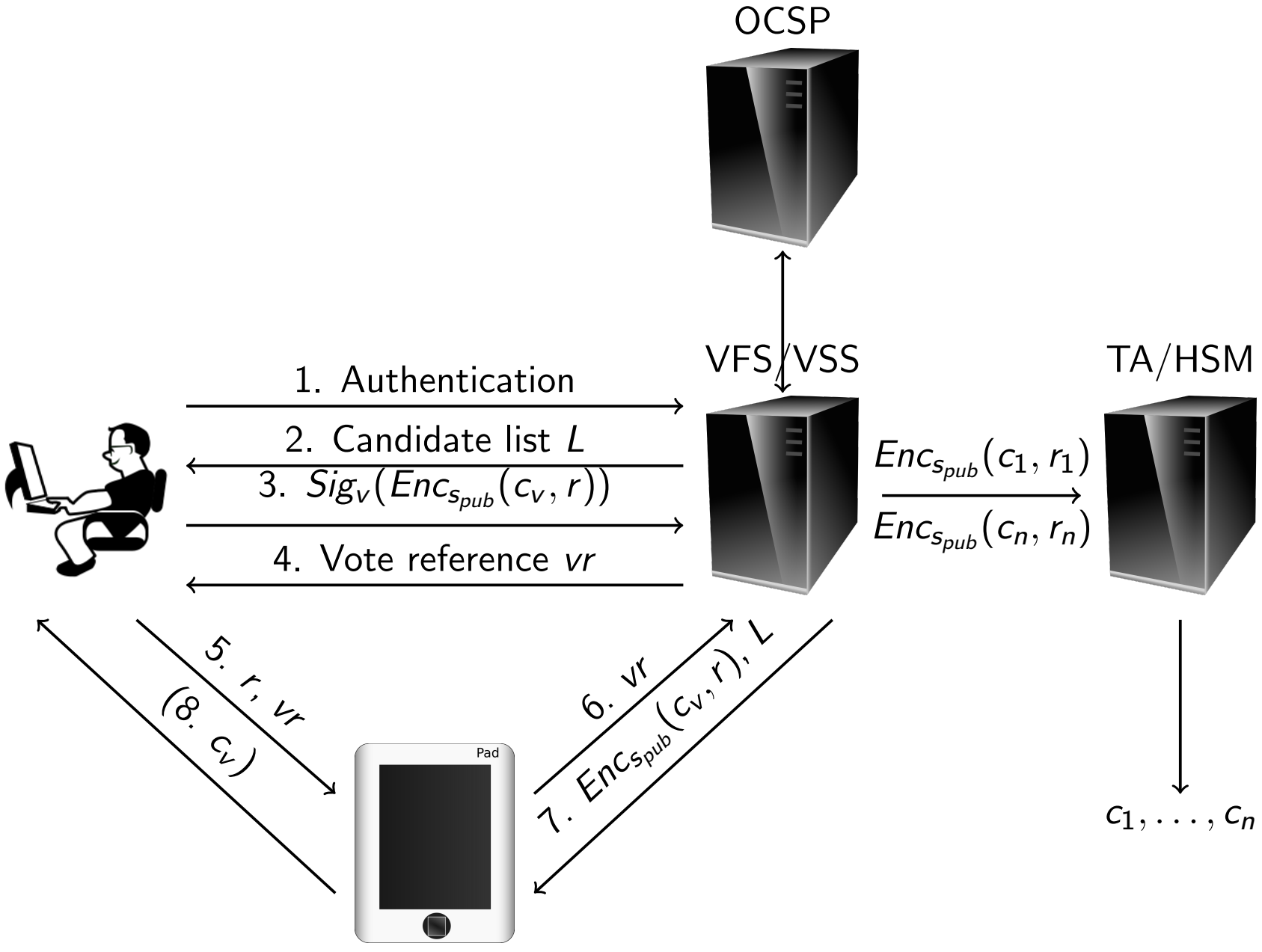
Internet voting

- Electronic voting: a voting method that relies on the help of electronic device(s) in performing any of its core functions
  - eligibility verification;
  - voting;
  - recording of the votes;
  - storing votes for tally;
  - tabulation of the voting result.
- Internet voting: a remote electronic voting relying on the Internet as a communication channel between the voter and the electronic ballot-box.
  - nonsupervised environment
  - voter's device - PC, tablet, smartphone
- The Challenge: Human inability to observe electronic processes

Estonian Internet voting: the beginning

- In 2001, two studies on the feasibility of i-voting in 2002
  - Ministry of Justice: it is unrealistic to implement statewide i-voting in 2002 (Lipmaa et al., 2001)
  - Ministry of Transport and Communications: it is possible to implement statewide i-voting in 2002 (Tammet et al., 2001)
- In 2002, i-voting was regulated in the Election Law with the condition that the method shall not be applied before 2005
- In 2003, i-voting conception developed by inclusive process (private sector, academia, NEC)
  - i-voting is allowed during the Advance Voting Period
  - e-ID is used for authentication and digital signatures
  - Repeated i-voting is allowed to counter coercion
  - Paper-vote takes precedence over an i-vote
- In 2004, public tender for development won by Cybernetica AS

Estonian system so far



e-ID

- Estonian citizens have access to secure and reliable digital signature system since 2000
- Today compulsory for all residents (Certificates can be revoked)
  - e-mail address Forename.Surname@eesti.ee
  - Key and certificate for authentication
  - Key and certificate for digital signature (legally binding!)
  - RSA2048 since 2011, RSA1024 on earlier cards
  - Pinpad readers promoted to tackle the biggest vulnerability
- Alternative eID - MobileID, since May 2007
  - PKI-capable SIM cards
  - Equal legal power with ID-card
  - ECC starting from 2015

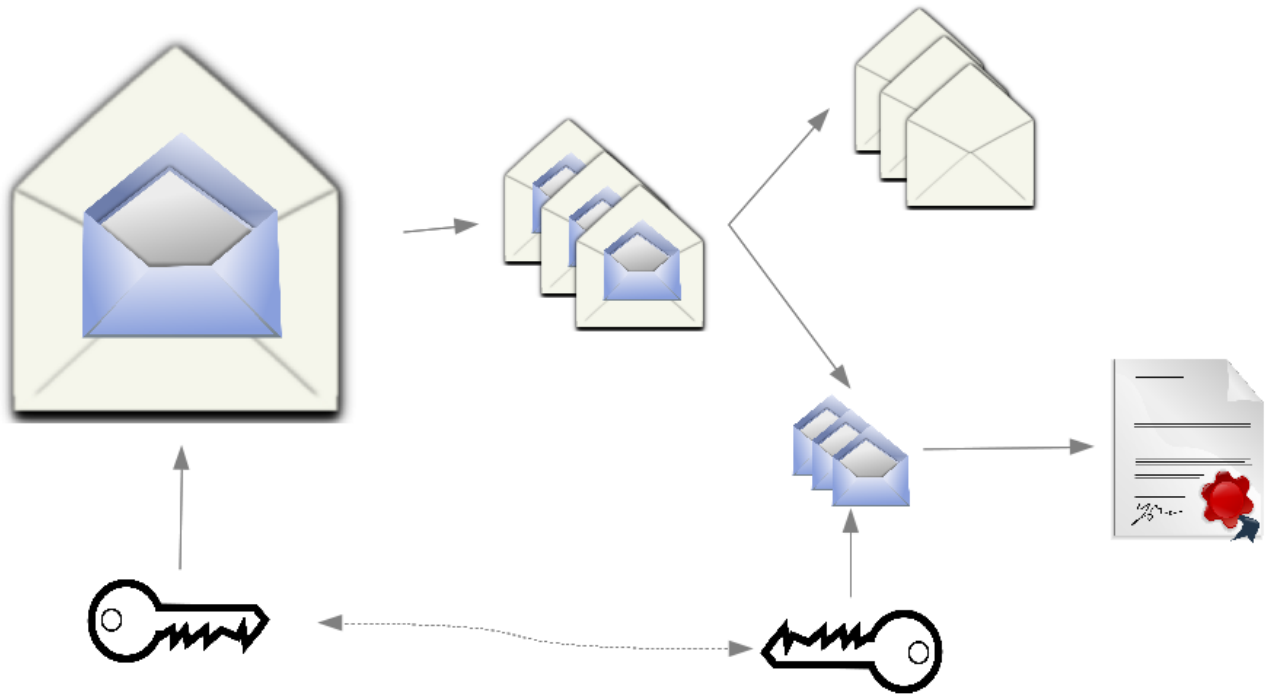
Encryption

- Alice and Bob want to exchange confidential information in the presence of an eavesdropper Eve
- Option 1: Alice and Bob use symmetric cryptosystem (E, D) to encode the message M
  - Alice and Bob share a key K
  - Alice encrypts the message: $C = E(M, K)$
  - Bob decrypts the message: $M = D(C, K)$
  - Given that cryptosystem is secure and Eve does not have the key K, the confidentiality of the message M is not violated
  - Problem: The key sharing is difficult task

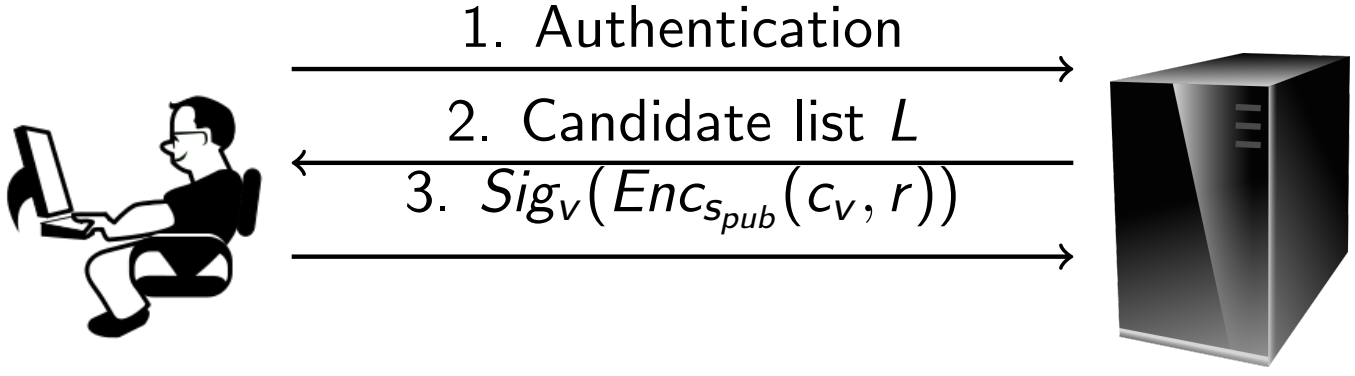
Public Key Encryption

- Alice and Bob want to exchange confidential information in the presence of an eavesdropper Eve
- Option 2: Alice and Bob use asymmetric cryptosystem (E, D) to encode the message M
  - Alice generates a private and public keypair $(Priv_A, Pub_A)$
  - Bob generates a private and public keypair $(Priv_B, Pub_B)$
  - Alice and Bob publish their public keys: Pub_A, Pub_B
  - Alice encrypts using Bob's public key: $C = E(M, Pub_B)$
  - Bob decrypts using his private key: $M = D(C, Priv_B)$
  - Given that cryptosystem is secure and Eve does not have access to the key $Priv_B$, the confidentiality of the message M is not violated
  - It is possible to secure the private key
- Public Key Encryption is also basis of digital signatures - if something is encrypted with Bob's private key, then Bob must have done it

Double Envelope Scheme



Estonian Internet voting protocol: 2005 - 2011



Verifiability

- How can you trust a voting machine or electronic tabulation?

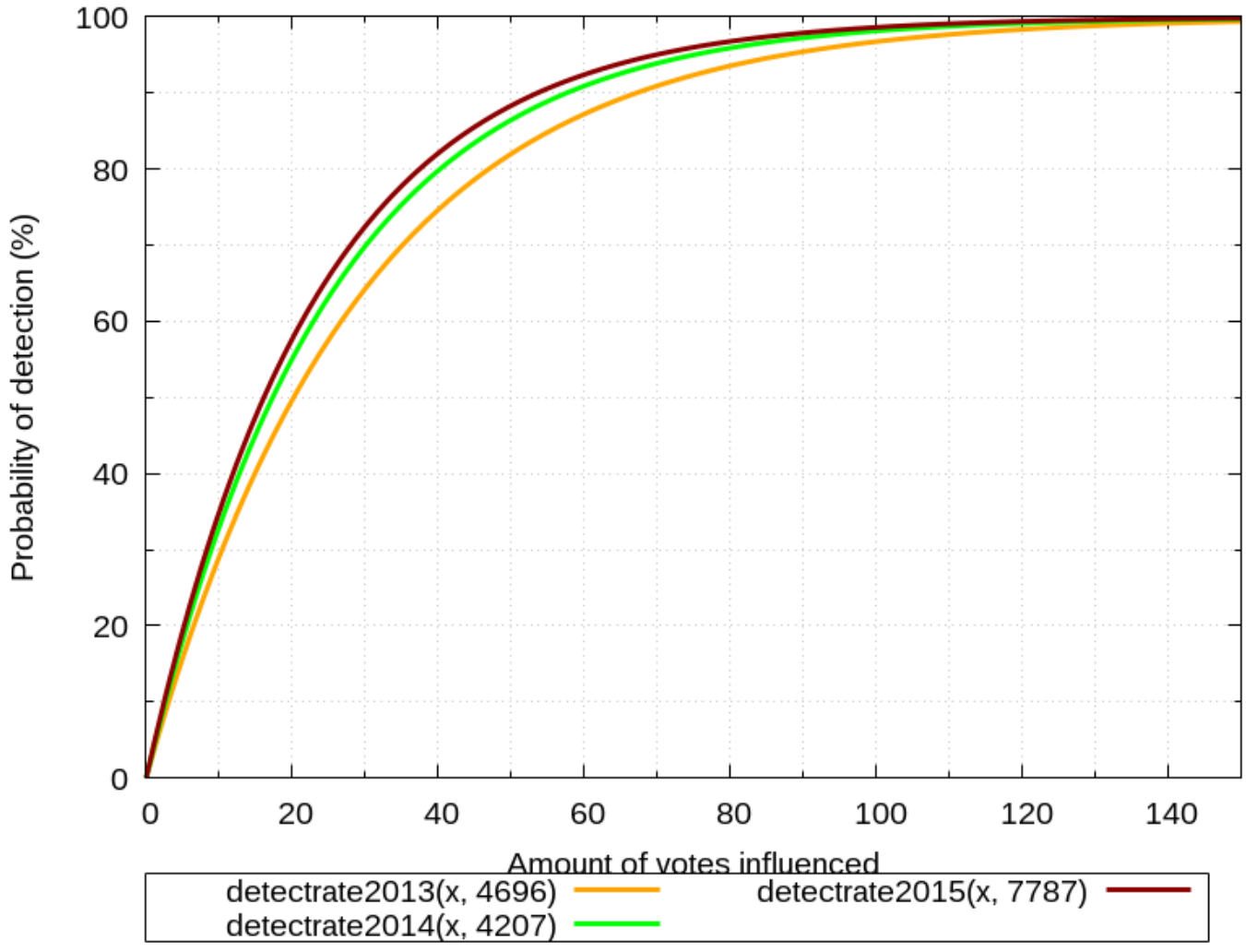
Individual verifiability

- Voter has means to verify some of following claims
  - Voting tool correctly encoded my will as a vote (cast as intended)
  - My vote was accepted into ballot-box (recorded as cast)
  - My vote was tabulated correctly (tabulated as recorded)

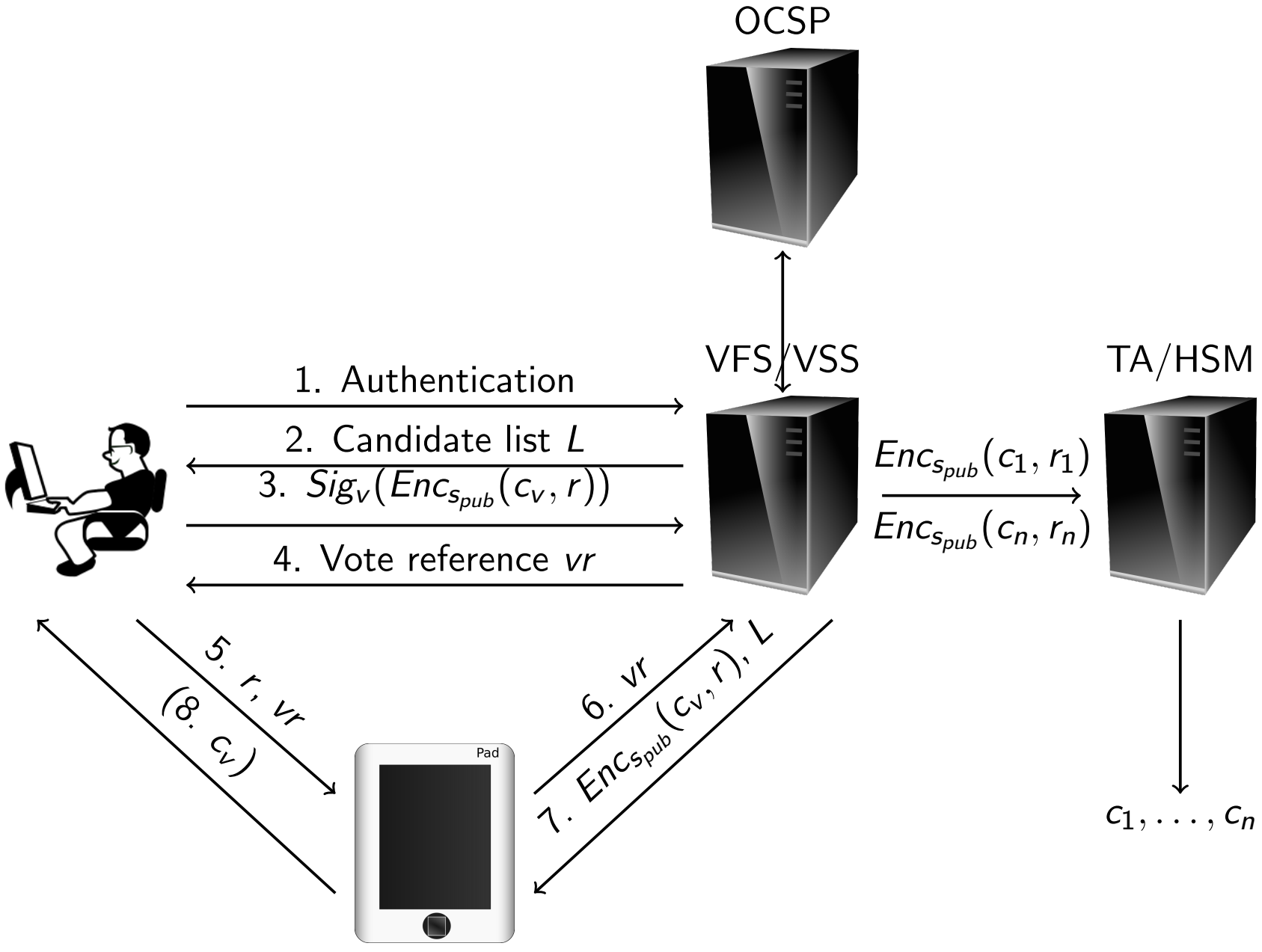
Universal verifiability

- Observer has means to directly verify following claims
  - Only votes by elegible voters are in ballot-box
  - At most one vote per voter is in ballot-box
  - No un-authorized modifications to ballot-box have occured
  - The result is calculated correctly

Verification in 2013 - 2015



Estonian system so far



The trustworthiness of the system and its operations?

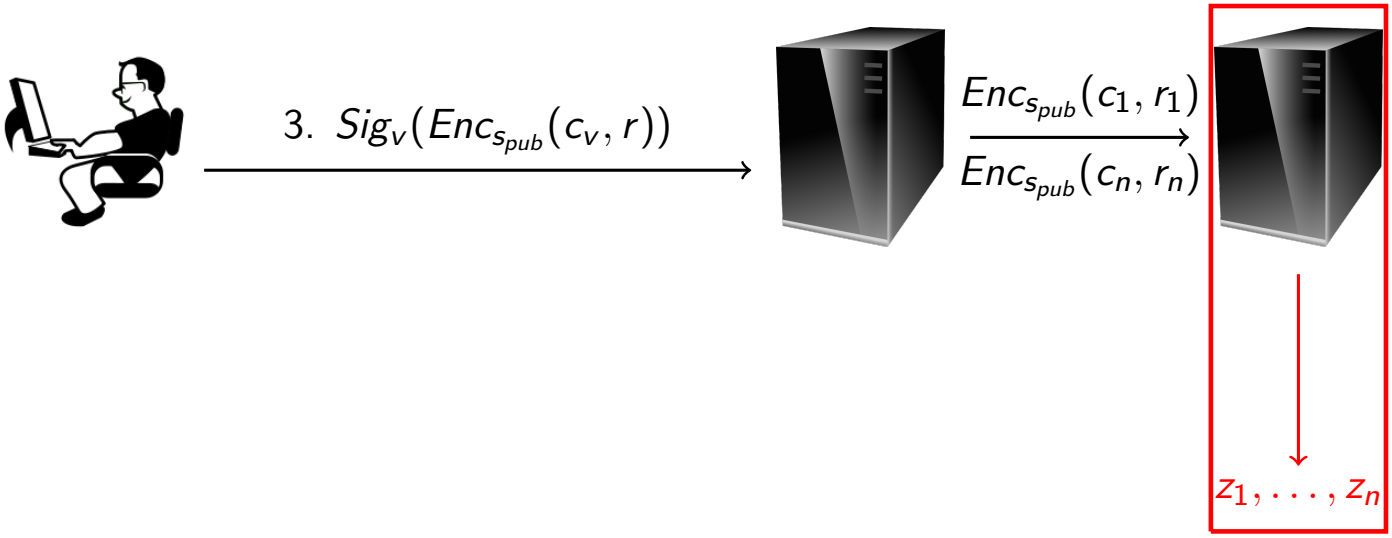
- 2003: "The other side of the compromise or, in principle, the weak point of the scheme, is the need to trust central servers and computers of the voters. Is such a compromise reasonable? In our opinion – yes."

The trustworthiness of the system and its operations?

- 2013: "The other side of the compromise or, in principle, the weak point of the scheme, is the **need** to trust central servers ~~and computers of the voters~~. Is such a compromise reasonable? ~~In our opinion – yes.~~"
- Number of physical and organizational measures to ensure the trustworthiness...
  - ...that can always be cast under the shadow of a doubt.
  - The application of these measures requires high technical level of involvment of the NEC.
- How can we really *prove* to a third party that the voting result is correct according to the rules?

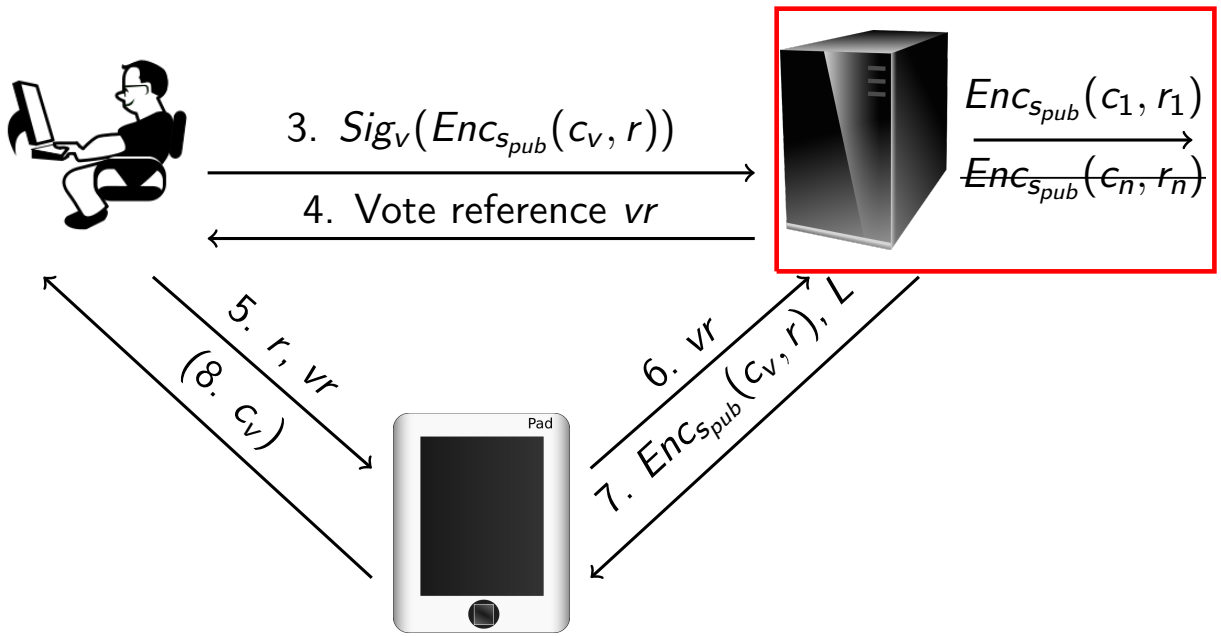
Shortcomings: tabulation integrity

- It is not possible to verify the correctness of the decryption.
- Compromised tabulation tool could change the result without anyone noticing.



Shortcomings: i-ballot box integrity

- Assuming the outer envelope (a.k.a. *signature*) can not be forged, ballot box stuffing and vote manipulation are practically unachievable.
- However, a malicious ballot box may choose to drop votes.

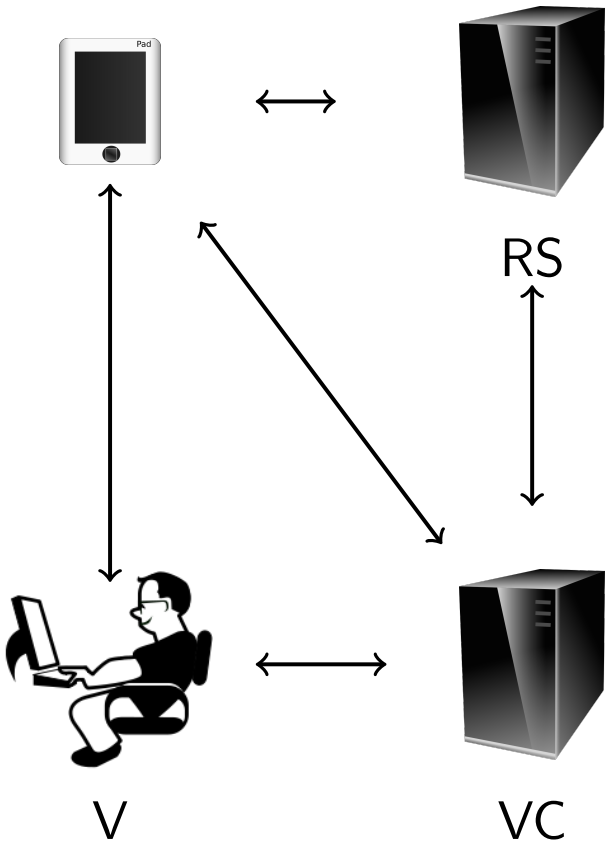


Third party auditability

- We want to allow a third party auditor[1] to verify i-ballot box properties in a privacy preserving manner.
  - The auditor should be able to check the eligibility, well-formedness and tallied-as-recorded properties.
  - We need assurance that there is no invisible way to drop votes.
- If the integrity of the vote collection can be audited, it becomes possible to outsource this procedure.
- The verifiability of the correct tabulation would increase the trustworthiness of the voting result.

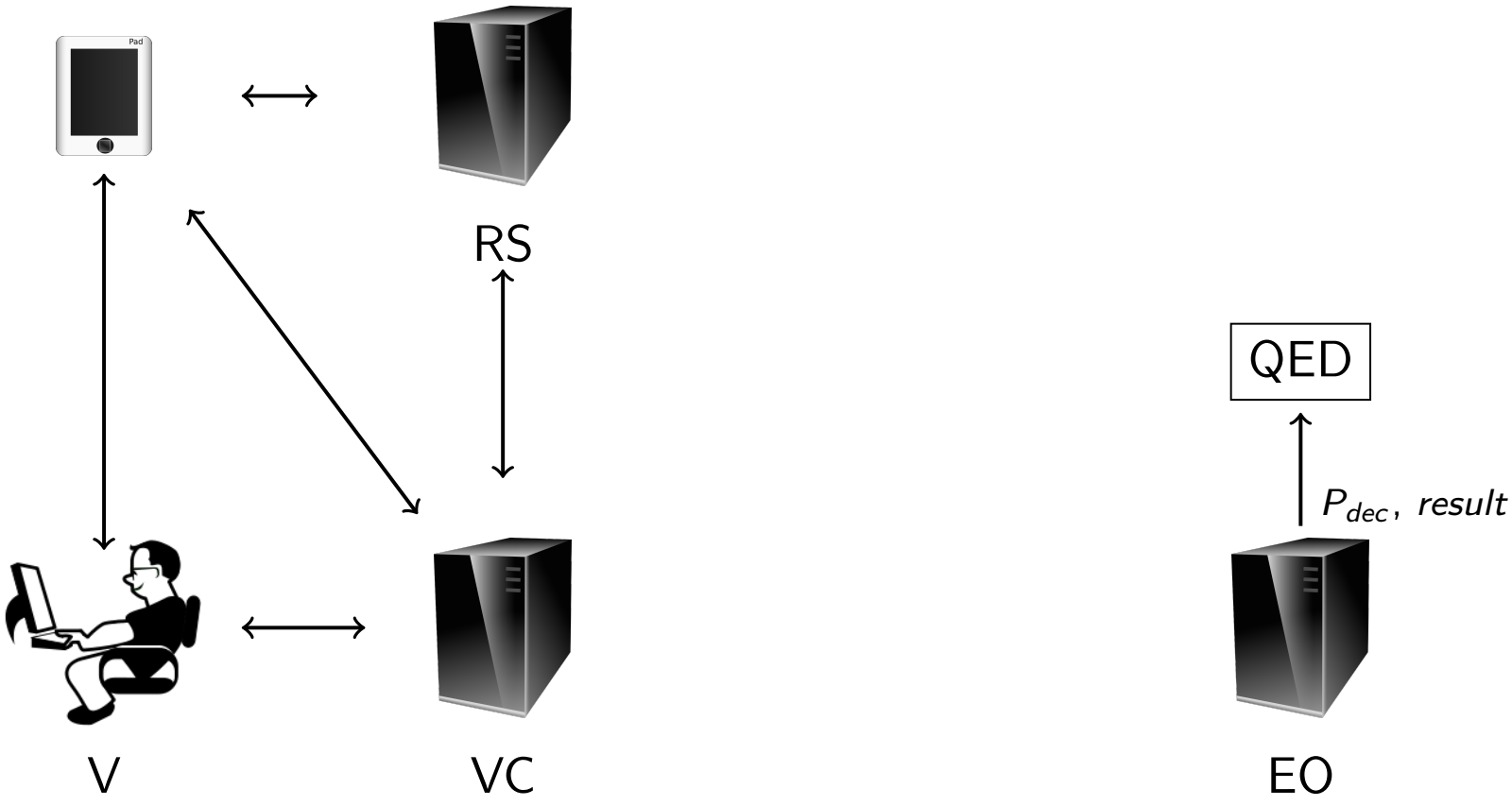
[1] In principle, Anyone. In practice, limitations may apply.

IVXV: The Big Picture



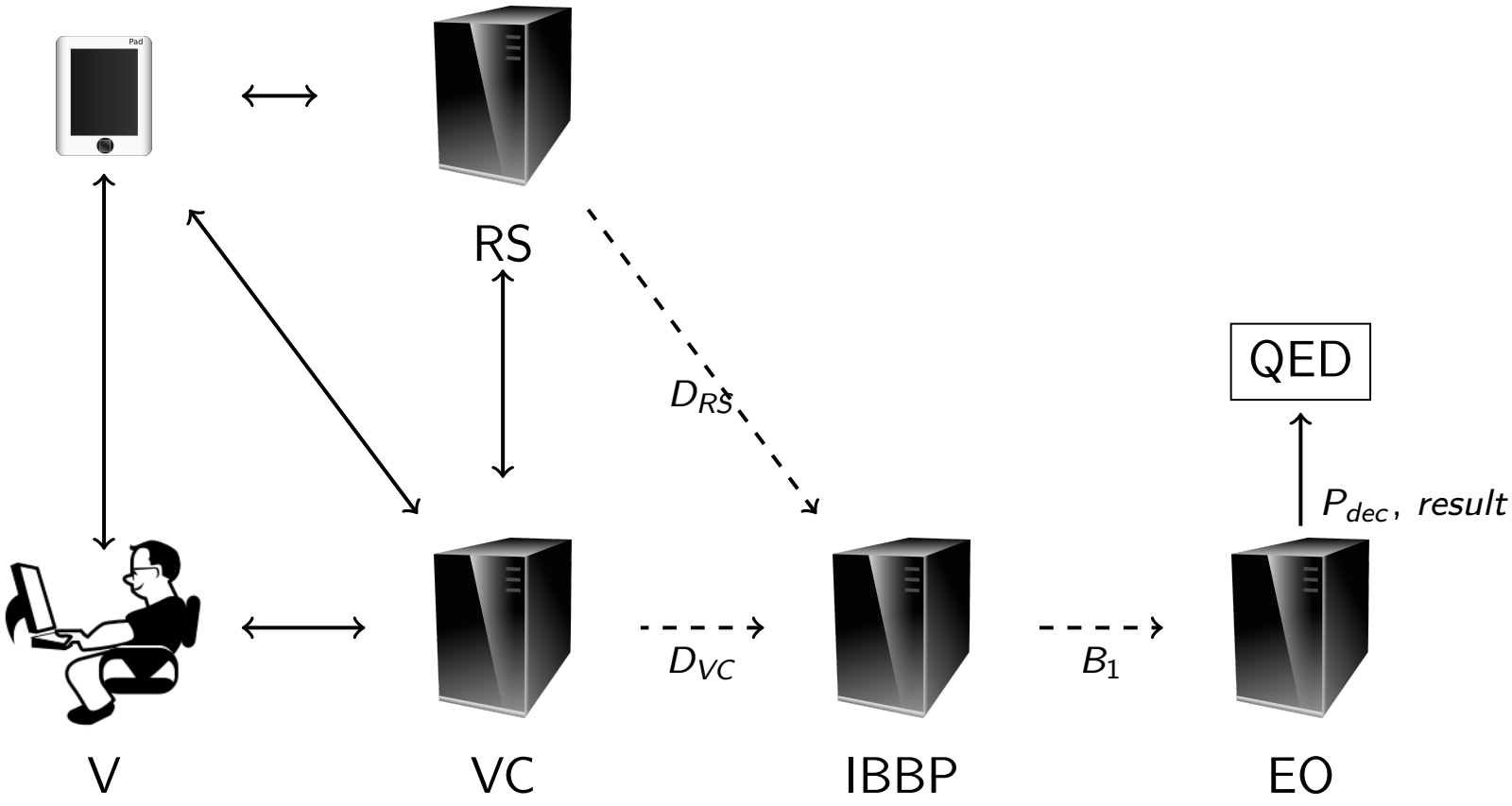
- Vote Collector shall register each vote to an independently hosted Registration Service.
- The consistency shall be audited both by voters and auditors.

IVXV: The Big Picture



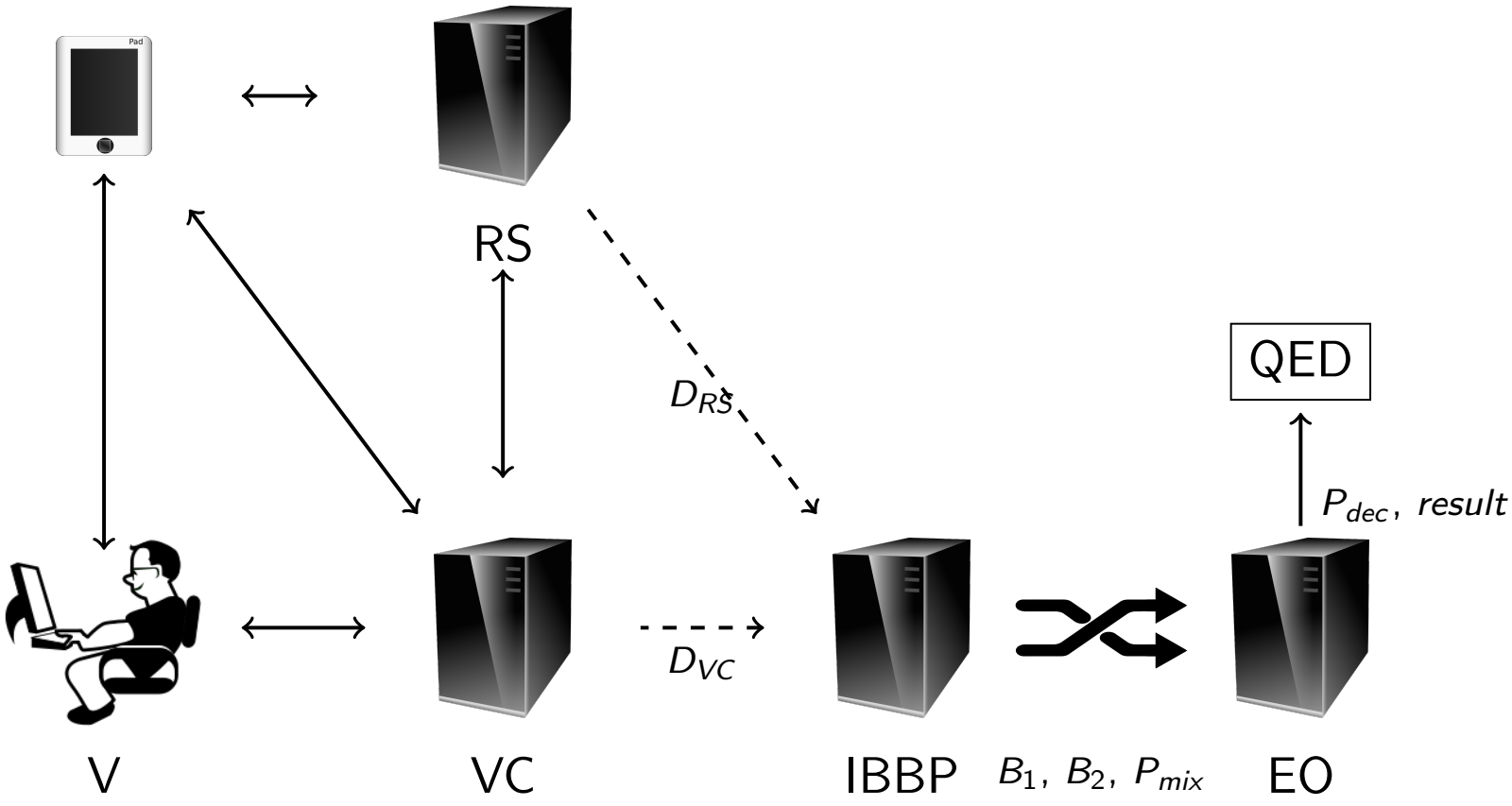
- The tabulation application shall provide a proof of correct decryption for each ballot.

IVXV: The Big Picture



- The i-ballot box processor audits the vote collection and anonymizes votes for the tabulation.

IVXV: The Big Picture



- In order to provide an external auditor with access to both digitally signed votes and decryption proofs, a verifiable re-encryption mix-net must be applied.

IVXV: Complete audit of an election

- Data Auditor would have to audit
  - All votes in D_{VC} belong to eligible voters and verify successfully,
  - All votes are consistent with the rules of well-formedness,
  - All confirmations in D_{RS} verify successfully,
  - The views D_{VC} and D_{RS} are consistent,
  - The set of encrypted votes B_1 is calculated correctly,
  - P_{mix} is correct,
  - P_{dec} is correct,
  - *result* is correct.

Conclusions and further work

- The Estonian Internet voting scheme will be getting two major updates:
  - Vote Collector needs to commit the vote operations to a registration service, hence making all of its actions independently auditable;
  - The tabulation application will issue proofs of correct decryption.
    - To allow full independent auditability, a mix-net needs to be applied.
- The first update is scheduled to be implemented by fall 2017 local elections; we sincerely hope that it is possible to implement the second update by that time, too.

Thank you!