Secure and verifiable Online Voting

Post E-Voting

THE STEPS

Credentials Phase

1 **Voting Credentials**

Voting Phase

2 **Voting**

3 **Ballot Box Recording**

Tally Phase

4 **Ballot Box Verification**

5 **Mixing**

6 **Decryption**

7 **Tallying**

SECURITY AND VERIFIABILITY IN CONTEXT

PRIVACY

- End-to-End Encryption

Votes are encrypted on the voter's device, ensuring they remains secret throughout the process.

Votes are decrypted using a verifiable Mix-net and a secret sharing scheme. This ensures that the anonymity of voters is maintained.

ELIGIBILITY

- Eligibility Verification

Encrypted votes are also digitally signed on the voter's device using a key roaming mechanism, protecting the integrity of votes and ensuring voter eligibility

VOTE CORRECTNESS

- Vote Correctness

Voting servers can check if the contents of the encrypted votes are valid without need to decrypt them, allowing to double check that invalid votes are not cast by voters, all this without breaking vote secrecy. Vote correctness is guarantee during the whole process at each step.

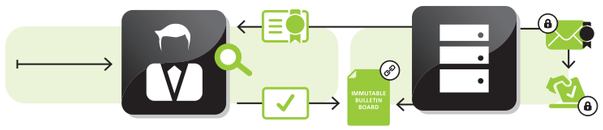
INDIVIDUAL VERIFICATION

- Cast-as-Intended

Return Codes allow voters to check against their voting cards if the encrypted vote received by the server contains the selected voting options, again without breaking vote secrecy.

- Recorded-as-Cast

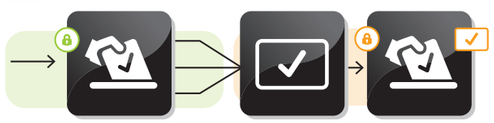
Receipts allows to voters to verify if their votes have been stored in the ballot box by checking a public Bulletin Board.



INTEGRITY

- Ballot Box Integrity Check

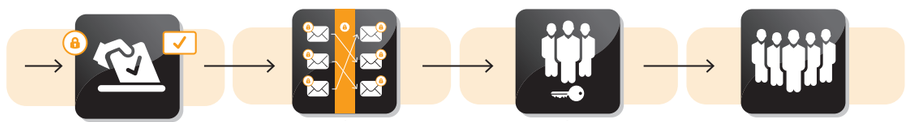
Ballot box integrity can be verifed by using the Bulletin Board, digital signatures and mathematical proofs of the votes.



UNIVERSAL VERIFICATION

- Counted-as-Recorded

Mathematical proofs produced by the Mix-net and decryption processes provide evidence of the accuracy of the counting process and therefore, the accuracy of the results.



- Bulletin Board Audit

Mathematical proofs produced by the Mix-net and decryption processes can be published in an Immutable Bulletin Board to facilitate public audits.