Online Voting System Discussion

Prototype

Doug Blewett

doug.blewett@gmail.com

Why We Need Online Voting

- **All voting systems that depend on paper based ballots suffer from loss, error, and possible manipulation.**
- **The manipulation occurs as the paper based ballots must be counted with human intervention. Rejects are always above 1% and sometime as high as 6%.**
- **Paper is inherently prone to damage – crumpled, stained, poorly scanned – all cause counting problems.**
- **The counting itself is also too time consuming. Some elections go on for months.**

Why We Need Online Voting

- **We want to preserve the current voting system where people can opt to go to the polls. Well designed online voting preserves the voting system methods and practices.**
- **The voter registration process currently collects enough information that is required to identify online voters. We want to preserve community control.**
- **We can secure each ballot cast by adding a human readable ballot number. The number identifies the ballot as a legal ballot.**
- **The tabulation (counting) of ballots has gotten out of control. Electronic ballot collection and storage will speed tabulation and restore confidence in the system.**

Online Voting Data Flow

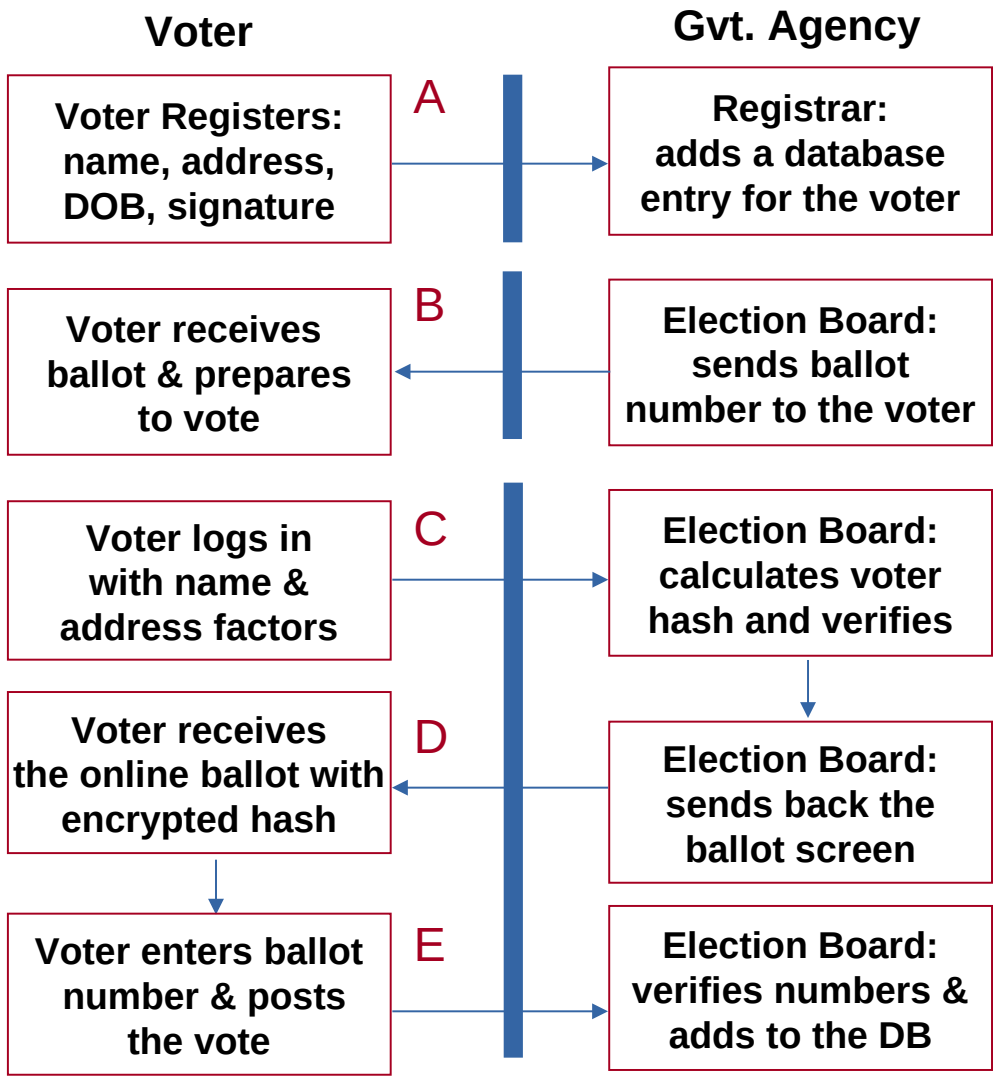
A. Voters register to vote as usual: registrar, DMV, etc.

B. The registrar sends numbered ballot to the voter to start the process (one way, registration hash is in the ballot number DB)

C. The voter logs in and a hash is calculated from login data and verified – legal voter.

D. The election board sends the online ballot with encrypted hash

E. The voter enters the ballot number into the ballot screen and posts the vote



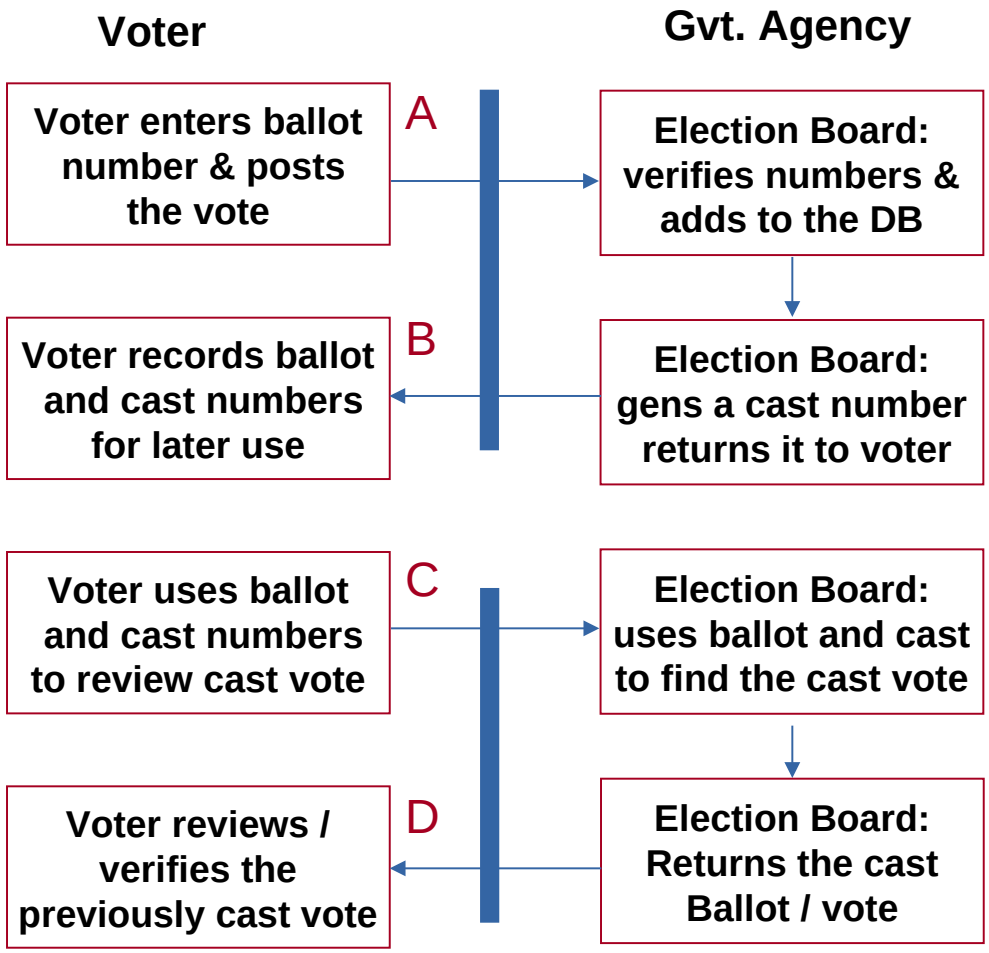
Reviewing / Verifying a Prior Cast Ballot

A. The voter enters the ballot number into the ballot screen and posts the vote (see the previous slide)

B. The election board gens and returns the cast number for the vote

C. The voter submits the ballot and cast numbers to review the cast vote

D. The election board returns the previously cast vote for verification and review



The Ballot Number Database

The ballot number database contains four items: cryptographic hash of the ballot number, cryptographic hash of the user registration data, a time stamp of the last activity, and a flag denoting if the ballot number has been used.

- **The hash of the user voter registration data is what is called a "one way" hash. It produces a number from the data, but cannot be used to produce the data from the number. The hash is further encrypted in an enclosing hash (double hashed) when sent over the Internet. The internal hash is never exposed.**
- **Data fields:**
  - Cryptographic one way has of the ballot number
  - Cryptographic one way hash of registration data
  - Time stamp of the last activity
  - Use flag (has this number been used)

The Cast Ballot Database

- **The cast ballot database contains: the ballot number, the cast ballot number, and a list of all of the choices the voter made on the ballot.**
- **The cast ballot number is an encoded number that identifies this cast ballot. It is cryptographically encoded to make it opaque to the voter. An AES encoding of the index is a good example of what can be used for the cast ballot number.**
- **Data fields:**
  - Ballot number
  - Cast ballot number
  - A list of the voter choices on this ballot