

Project 2 – Electronic Voting

1. Definitions:

- **County-** A physical location where all residents will be vote on the same positions / issues.
- **Precinct-** A subset of the regions, i.e., a collection of related precincts forms a county.
- **Voter-** An individual that is casting a vote.
- **Registration Staff-** Those that help the voters register.
- **Voting Staff-** Those that Help the voters cast their vote
- **Senior Staff-** Trusted staff that take on extra responsibility
- **Regional Director-** The highest level staff member of the County

2. Assumptions

- a. The regional director and all senior staff members are trustworthy and non-malicious
- b. All staff members are considered non-malicious.
- c. Voting takes place only on a small, limited set of days.

3. Registration

- a. Registration Staff (Figure 1)
 - i. Registration staff will be drawn first from residents of the precinct. This will facilitate faster registration, as the staff will have a greater chance of recognizing the voter.
 - ii. The non-senior staff handles voter validation and data collection tasks.
 - iii. At any time there must be at least one senior staff member present.
 - iv. Each registration site has at least three senior staff.
 - v. Senior staff members are each equipped with a smart card containing a unique key as well as a secret 8-character password (which they memorize).
 - vi. The senior staff smart cards have a scheduled auto memory reset every 3 months. They must be taken to the County system to be reprogrammed. (this limits the use of stolen smart cards).
- b. System
 - i. Precinct (Figure 2)
 1. The computer system consists of several data entry terminals connected to a central server.
 2. The overall system is logically and physically isolated inside the precinct building. (e.g. no connections to the internet, etc.)
 3. Booting up the system requires the use of two senior staff smart cards and matching passwords.
 4. Shutting down the system requires one staff smart card and a matching password.
 5. The central server uses a mode-1 RAID array of at least 4 disks (data is duplicated on at least 4 disks).
 6. All data stored in this system is encrypted using a key that is formed by the combination of all three senior-staff smart card keys.
 7. Logging into the system to view the data requires the smart card keys and the corresponding passwords.
 8. Removing a disk requires that the system is shut down, and that at all three senior staff smart cards and passwords are used
 9. Session keys set up at the county office between the registration machines and precinct registration server will ensure that only voting machines can gain write access during the voting process

- ii. County
 - 1. Each county has a central site where registration and senior-staff information is stored for all related precincts. This system is physically and logically isolated.
 - 2. Uploading to the central registration system for a specific precinct must be done on-site and requires a combination of all 3 precinct senior staff smart cards and passwords.
 - 3. A Regional director will have a copy of all the passwords and smart card keys at the central county computer (accessible only by the regional director). The report of a lost password or stolen smart card will invoke the following process:
 - a. The smart card is recreated (if lost).
 - b. The regional director looks up the necessary password.
 - c. The regional director travels to the precinct system and resets the password.
 - d. The senior staff whose card or password was lost selects a new password with only the Regional director present.
 - e. The Regional director gives the senior staff the new smart card (if one was necessary).
 - f. The Regional director travels back to the county system and inputs the new password.
- c. Process (Figure 3)
 - i. Registration is done at each precinct, on site.
 - ii. Voters must register at least 1 month prior to the actual election at their particular Precinct. This will give staff time to verify their identity.
 - iii. At the beginning of each registration day, senior staff will boot-up the system.
 - iv. At the end of each registration day senior staff shut down the system.
 - v. Each voter must bring a picture ID, SSN, phone and proof of residence (e.g. Recent Bills). This information will be used to verify the voter's identity and will be entered by a staff member.
 - vi. A digital picture is taken of the registering voter.
 - vii. A senior staff member will verify that the voter information is correctly entered, and swipe their smart card to input the data into the database. The record is marked as un-verified.
 - viii. The voter will be given a smart card. This card will contain an encryption of their personal information (using the 3-part senior member key).
 - ix. The voter leaves with their smart card.
 - x. At the end of each week, the senior staff collectively removes one hard drive from the RAID array and replace it with a blank. The removed drive is taken to the Region's central database and the data is uploaded. As is typical with RAID-1, the blank drive is populated with a mirror of the other drives after it is installed.
 - xi. During the down month after registration but before voting takes place, the identities and address of registered individuals will be verified by the registration staff. If the address/identity cannot be verified, then the voter will be contacted by phone and/or mail, and will be given a chance to set up an appointment to re-register.

4. Voting

- a. Voting Staff (Figure 1)
 - i. The voting staff is identical in structure to the registration staff, with one key difference: The staff should **not** be drawn from the residents of the precinct. The goal is to limit recognition of voters the day of the event.
 - ii. To do this, we simply rotate the voting staff. They can even use the same smart cards and passwords. All passwords are reset at this time.
- b. System
 - i. Precinct (Figure 4)
 - 1. The registration machines are modified to boot-up and shut-down with the new senior-staff's smart cards / passwords.
 - 2. All registration data is still present, encrypted with the previous senior staff's smart card keys.
 - 3. Only the vote recording machines have write access to the vote table.
 - 4. The vote recording machine has no read access to the vote table.

5. Session keys set up at the county office between the voting machines and precinct vote server will ensure that only voting machines can gain write access during the voting process
- ii. County
 1. This voting storage system is physically isolated (i.e. in a separate room with separate staff) from the registration server, which contains only the encrypted personal information.
 2. There is a wired network connection from the voting system to the registration server, used strictly for authentication.
 3. Only the validation and tally staff have read access to the vote database. Write access is limited to the validation bit.
- c. Process (Figure 5)
 - i. Voters queue up in a designated area outside or just inside the precinct building.
 - ii. The voter enters a separate, physically isolated room.
 - iii. A voter is authenticated by swiping their smart card on an ATM like device. The digital photograph taken during registration displayed to the voting staff, and the staff compares the person to the picture. Also, the server checks the personal data from the smart card, making sure that it corresponds to a verified registration record. If both verification tests are passed, then the server returns a 'valid' signal to the voting machine. The voting machine will then allow the voter to proceed.
 - iv. The voter makes the desired selections.
 - v. The voting is complete after the smart card is swiped one final time.
 - vi. The voter's record in the database marks that the voter has voted, but the vote is stored separately from the record of personal information.
 - vii. The vote is stored with a randomly generated nonce, both of which are encrypted with the 3-part senior staff key.
 - viii. Staff members will monitor the voting progress remotely. They cannot see individual voting selections, but can see the state the user is in (e.g. Authentication, voting, completed). A voter will be informed if they don't complete the entire voting process before they leave the isolated room.
 - ix. The smart card is collected as they leave.
 - x. At the end of the day, the voting server is synchronized with the county server using the same process as the registration step (if this isn't the final day for voting). Otherwise the entire system is taken to the County building. Votes for a particular precinct are stored together in the same table.

5. Validation (Audit)

- a. Auditing can take place at the precinct or county levels.
- b. Authentication facilitated through the use of the vote storage system and the method used to generate a nonce for each vote. While it is possible that duplicate nonces will be generated, it is assumed that this will be statistically impossible due to the size in bits of the nonce values.
- c. The voting server has the encrypted votes, each with an associated nonce.
- d. To validate a particular vote, we decrypt the record and check the nonce to see if (a) it matches the precinct in that the vote came from and (b) that it was actually used. If either (a) or (b) are false, then the vote is marked as invalid.
- e. If more than one vote from the same precinct appears with the same nonce and each duplicate vote is the same, then one of the votes is kept and the others are marked as invalid. If the votes don't match, then they are all marked as invalid.
- f. The number of valid votes is compared to the number of registered voters for each precinct. If the number of votes is larger, that means that the nonce order must have been predicted and some votes were fabricated, or that some voter records were lost. **In this case we can do nothing but record the anomaly.**

6. Tally

- a. First, all the data is validated
- b. All valid votes are tallied.

7. Comments on confidentiality, Anonymity and potential weaknesses

The main weaknesses in this system are evident in any reasonable voting system: namely, checking whether a person registering is a valid voter, and ascertaining which votes cast are valid and which are not. The first problem

cannot really be simplified without requiring some sort of invasive and expensive procedure. Ensuring identity requires some sort of proof, birth certificate, tax records, etc. Biometrics could potentially be used to ensure that people do not try to register or vote twice, but there are two big hurdles for the use of biometrics. First, the systems are likely prohibitively expensive for something as infrequent and universal as voting. Spending thousands of dollars per system at thousands of precincts for something that happens annually is probably not justified. Also, civil liberties come into play because using a biometric requires that every voter give the government data (a fingerprint for example). The potential for function creep is enormous, and many might be discouraged from voting. Therefore, even though they are fallible, regular records were employed instead of biometrics to check voter identity.

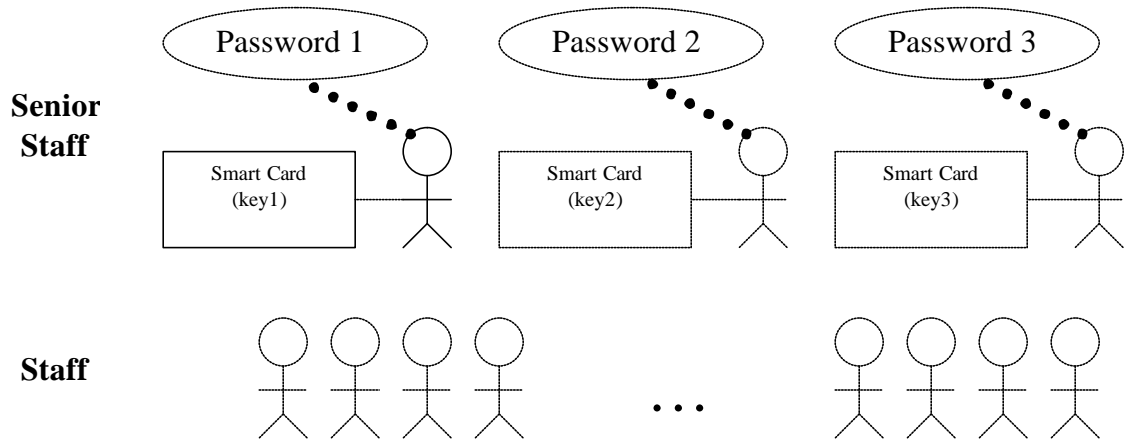
Ascertaining the validity of votes in the auditing process is another difficult area requiring tradeoffs between confidentiality and integrity. In this case, since maintaining a secret ballot (i.e. that a particular person's votes cannot be learned) is paramount, some degree of integrity was sacrificed for the confidentiality of voters. For instance, it would be possible to store a hash of personal information with each vote so that an audit process could verify that each vote came from a valid person. However, to figure out a person's votes, one could just hash their personal information again and compare it to all the vote records until a match is found. A many to one hash would make it so that a group of votes would match to a voter instead of a single vote, but then there is not a reliable way to invalidate all the bad votes. It was determined therefore, that each vote should have nothing derived from personal information recorded with it, ensuring confidentiality of the voter. This, of course, makes perfect auditing impossible.

Some auditing can be accomplished, however, by including a nonce with each record of a vote. The nonce, a randomly generated number that is statistically guaranteed to be unique, will ensure that a set of votes cannot simply be copied. If two votes have the same nonce, one must be invalid. In order to synchronize the nonce usage among a disconnected distributed system (i.e., the precinct systems) the nonce set must be unique for a particular precinct. This means a particular vote can be traced to a subset of voters (all voters in a precinct), but not to an individual voter.

Also, read and write access will be limited so that votes cannot be copied directly, or written to the vote database by anything other than the vote recording machine. All regular users of the voting database will only be given read access so they cannot add or alter votes. Also, the recording machine will only be given write access so it cannot copy votes. There is the issue of someone physically connecting a computer that pretends to be a vote recording machine in order to gain write access, but that is very unlikely due to the trouble and the presence of other voting staff. Also, integrity is maintained by the registration process and voting process to ensure that only valid voters can gain access to the vote recording machines in the first place. Smart cards, security procedures, passwords, and an isolated computer system are used to secure registration and voting. Backup storage systems and a central server make sure that votes or registration information is not lost or corrupted after the fact.

Thus, the system is able to maintain a very high level of confidentiality since no personal information is linked to votes, and also a fairly high level of vote integrity is achieved through smart cards, the registration process, and voting procedures. For a trace of a vote through the system, see Figure 6.

Precinct Staff



County Staff

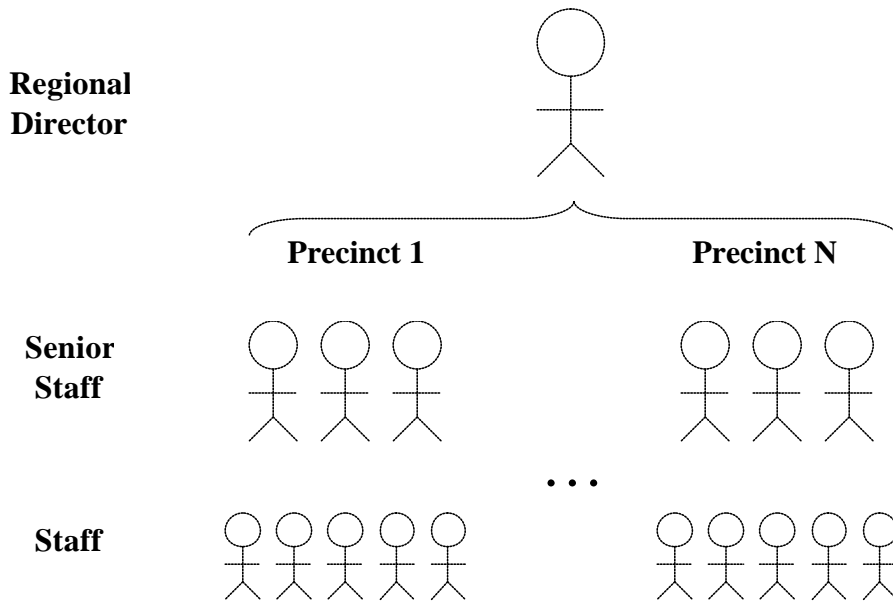


Figure 1. Staff Structure

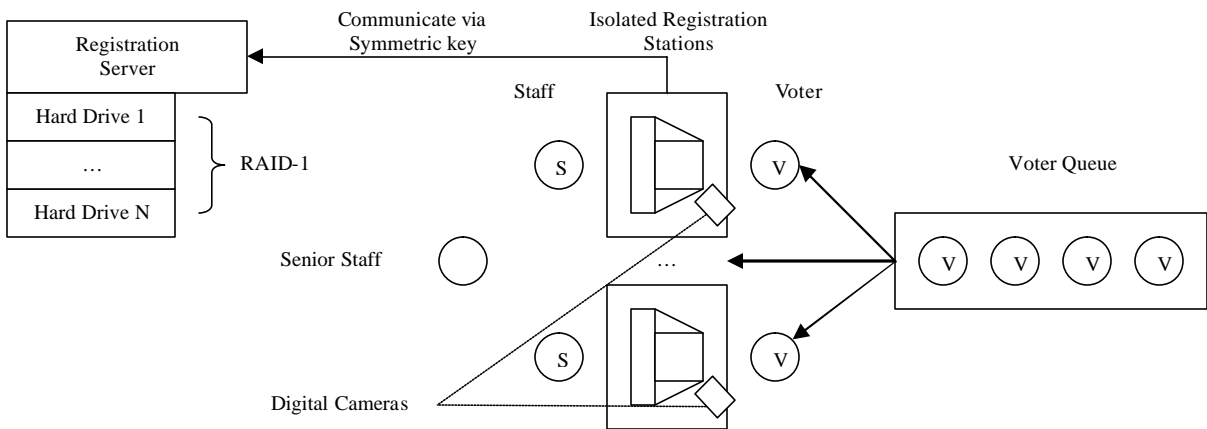


Figure 2. Registration System

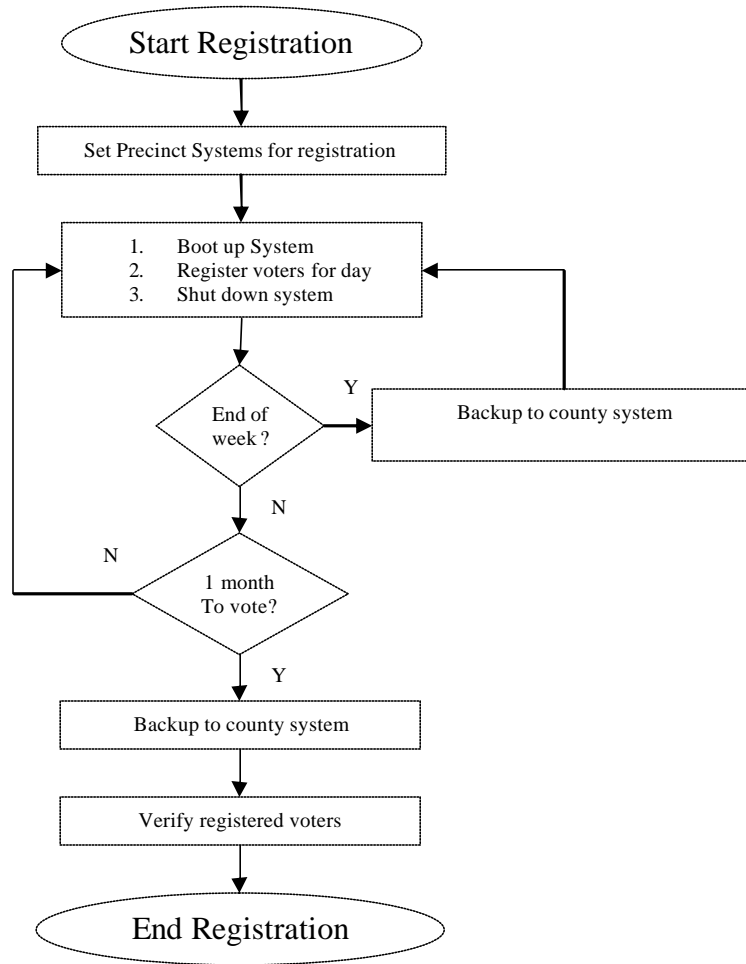


Figure 3. Registration Process

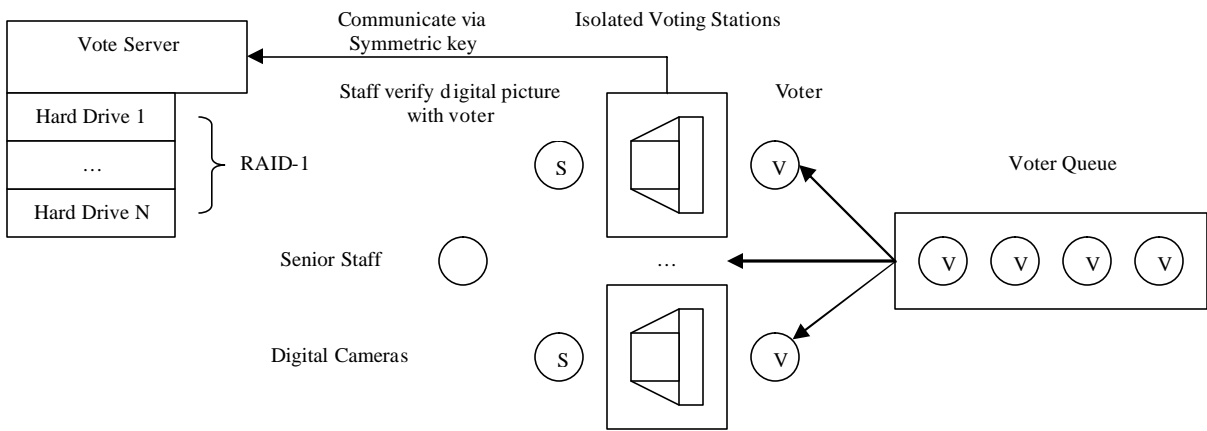


Figure 4. Voting System

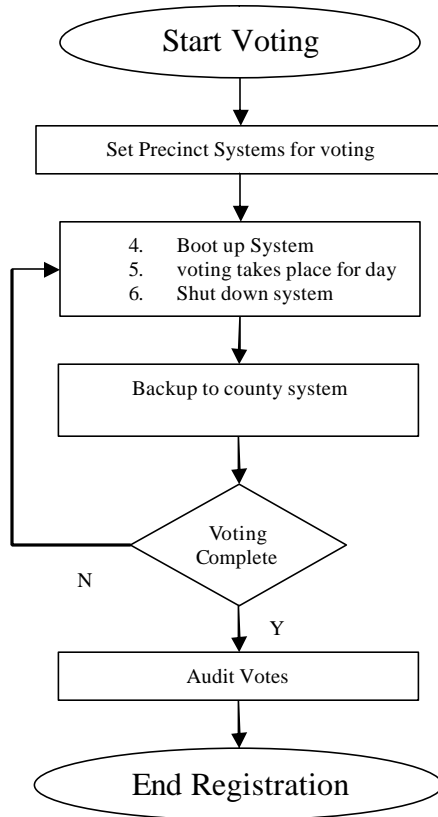


Figure 5. Voting Process

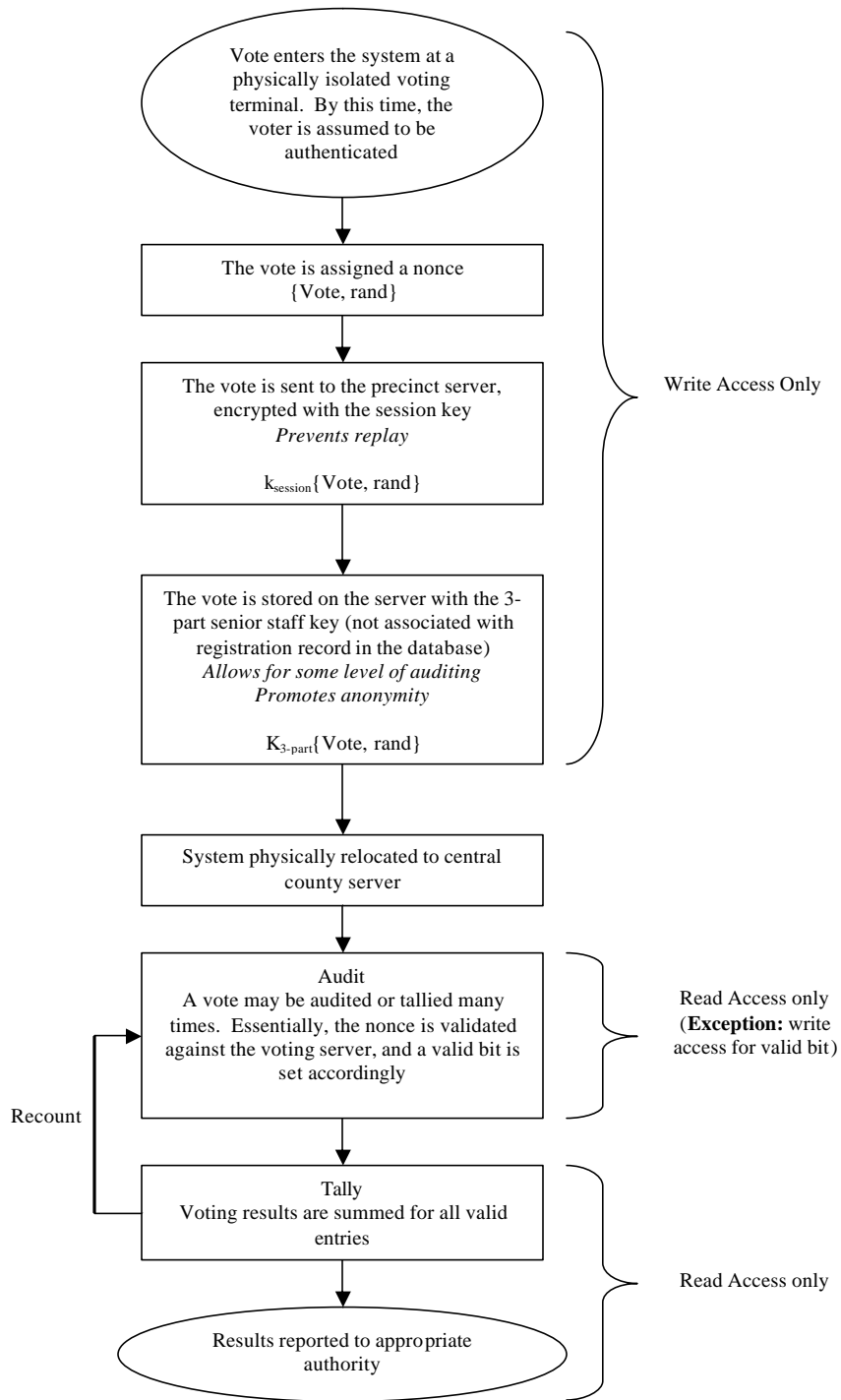


Figure 6. Vote Trace