Project: Secure Virtual Election

Soft Deadline: As soon as possible

The project can be done by at most two persons.

Name1: _____

Name2: _____

This project is about to implement a Java application that exploits secure sockets and Java security components. To be approved on this project, you must demonstrate your program to Pierangelo. The project deadline is soft, however try to respect it, if possible.

1. Problem description

This project is about to implement a secure election protocol. You may read the article *Voting with Two Central Facilities* for a discussion about it. The implementation will provide a secure way for people to vote online, which eliminates the need of physically being present at designated election locations.

Since online voting will not replace general elections unless there is a protocol that both maintains individual privacy and prevents cheating, the ideal protocol must meet these requirements:

- Only authorized voters can vote.
- No one can vote more than once.
- No one can determine for whom anyone else voted.
- No one can duplicate anyone else's votes.
- Every voter can make sure that her vote has been taken into account in the final tabulation.
- Everyone knows who voted and who didn't.

Your design should use two central facilities: Central Tabulating Facility (CTF) and Central Legitimization Agency (CLA). CLA's main function is to certify the voters. Each voter will send a message to the CLA asking for a validation number, and CLA will return a random validation number. The CLA retains a list of validation numbers as well as a list of validation numbers' recipients to prevent a voter from voting twice. Then, the CLA completes its task by sending the list of validation number to the CTF. The CTF main function is to count votes. CTF checks the validation number against the list received from the CLA. If the validation number is there, the CTF crosses it off (to prevent someone from voting twice). The CTF adds the identification number to the list of people who voted for a particular candidate and adds one to the tally. After all the votes have been received, the CTF publishes the outcome.

2. Election protocol

The following excerpt from *Voting with Two Central Facilities* describes a secure voting protocol. You may implement this protocol or any other protocol that fulfils the above mentioned requirements.

The following protocol uses CLA to verify voters and a separate CTF to count votes.

1. Each voter sends a message to the CLA asking for a validation number.
2. The CLA sends the voter back a random validation number. The CLA maintains a list of validation numbers. The CLA also keeps a list of the validation number's recipients, in case someone tries to vote twice.
3. The CLA sends the validation numbers to the CTF.
4. Each voter chooses a random identification number. She creates a message with that number, the validation number she received from the CLA, and her vote. She sends this message to the CTF.
5. The CTF checks the validation number against the list it received from the CLA in step 3. If the validation number is there, the CTF crosses it off (to prevent someone from voting twice). The CTF adds the identification number to the list of people who voted for a particular candidate and adds one to the tally.
6. After all votes have been received, the CTF publishes the outcome, as well as the lists of identification numbers and for whom their owners voted.

Note: all communications should be secured by using SSL/TLS.