Chapter 1

Naming conventions

Name	**Definition**
Voter	A voter is a person allowed to vote by the laws of the state.
User	Any user of the system, not necessarily eligible to vote.
Eligible user	A person with specific rights granted by having knowledge of a secret, which allows him to use an extended set of functions.
Client	The part of the system that allows users to vote.
Bulletinboard	The part of the system that registers votes and stores most of the the election data
Authority	The part of the system that provides eligible users with functionality to setup, start, stop or collect information about the election.
Ciphertext	Encrypted data interpreted as text.
Node	A computer running either the client, bulletingboard or authority software.

Chapter 2

Requirements

The requirements are categorized according to the FURPS+ model.

2.1 Functional requirements

Identifier	**Requirement summary**
Features	
FR 1.1	The system must allow voters to vote.
FR 1.2	The system must allow eligible users to configure an election prior to the start of it.
FR 1.3	The system must allow eligible users to start and stop an election.
FR 1.4	The system must allow eligible users to obtain the result of an election.
FR 1.5	The system must allow voters to confirm that their vote has been registered by the bulletin board server.
FR 1.6	The system must allow users to check whether they are eligible to vote.
Interoperability	
FR 2.1	The system's source must be easily understandable to wide amount of software porfessionals.
FR 2.2	All system modules require Jolie to run?.
Extendability	
FR 3.1	Each system module must be replaceable without changing the other modules.
FR 3.2	System modules must communicate across well defined interfaces.
Composability	
FR 4.1	All communication between system modules must be verifiable.
Manageability	
FR 5.1	The system must be administrated by a set of eligible users.
Maintainability	
FR 6.1	The system source code must be well commented and documented.
Security	
FR 7.1	The system must take measures to ensure that ones ballot is always anonymous.
FR 7.2	The system must be correlation? resistant.
FR 7.3	Communication between the bulletinboard and the client, as well as the bulletinboard and the authority must be secured, such that the result of the election can not be modified by unintended actors.

2.2 Detailed Requirements

FR 1.1 - The system must allow users to vote
The system must be able to capture votes for all eligible people, such that it is taken into account when the ballots are counted. It must be possible to overwrite ones ballot as long as the election is still in progress, by the exactly same process as voting the first time.
It requires the following input to vote:

- The identifier of the election option.
- The personal identifier of the voter.
- The password of the user.

FR 1.2 - The system must allow eligible users to configure an election prior to the beginning of it.
The system must allow eligible users to configure certain options in the system. These options include, but are not limited to, the election options, the keys used for the cryptographic parts of the system and when the elections begins and ends.

FR 1.3 - The system must allow eligible users to start and stop an election. The election is started by setting up the election, specifying a start time. The election is ended in the same way, however it must be possible end it earlier than specified in the setup configurations.

FR 1.4 - The system must allow eligible users to obtain the result of an election. The system must allow the authorities to obtain the result of an election. This can be done only after an election has finished and only by providing the decryption key. The system must not in any way allow the holder of the key to decrypt anything less than the sum of all votes.

FR 1.5 - The system must allow users to confirm that their vote has been registered by the bulletin board server.
The system must not allow others to confirm whether a certain voter, other than themselves, has voted. The voter must have knowledge of the ciphertext sent to the bulletinboard to check whether he has voted. If the secrecy of the ciphertext is violated, the system can not prevent others from confirming that the voter has voted.

FR 1.6 - The system must allow users to check whether they are eligible to vote. By providing the user credidentals, the user must be able to check whether he is eligible to vote.

FR 2.1 - The system's source must be easily understandable to wide amount of software professionals.
The system must be written in a way which the average software professional can easily read and understand, in order to make the system more transparent. A more transparent system is, easier to verify sine more people will be able to understand the how the system work and thus be able to verify it.

FR 3.1 - Each system module must be replaceable without changing the other modules.
A system module is defined as either the client, bulletinboard or authority software. If a module is changed and still uses the same interface, it must not be necessary to change the other modules.

FR 4.1 - All communication between system modules must be verifiable.
Since the system shall be used to decide how many people has voted for the different candidates and/or parties, an error in the system can have a very large impact. To increase the likelihood of the software developers catching any mistake the system must be as transparent as possible. Furthermore it should be possible to verify the communication between the modules. It is important that if one module sends a message to another module, the message is the same when received.

FR 5.1 - The system must be administrated by a set of eligible users.
Some functionality of the authority software must require a secret key to access?
(FR 7)
All security requirements does not take into account the possiblity that the user is getting spyed on physically or by other software on the client computer while voting.
FR 7.1 - The system must take measures to ensure that ones ballot is always anonymous.
The system must not allow anyone, not even the eligible users, to find out what a specfic voter has voted. This must be ensured by securing the communication in all channels that contains data containing information about the connection between the user identifier and the vote. This also includes that all communication containing secret data is always encrypted such that only the intended recipent gets the data.
FR 7.2 - The system must be correlation? resistant.
The system must be designed in such a way, that a voter can not be forced to vote something against his will. This includes the following requirements.

- It must not be possible to find out whether a specific person voted without knowledge of the secret ciphertext sent.
- It must not be possible to find out whether a specific person overwrited his vote, even with knowledge of his prior vote ciphertext.
- The election must run for several days or weeks, to make sure that a voter has enough time to overwrite a vote forced against his will.

FR 7.3 - Communication between the bulletinboard and the client, as well as the bulletinboard and the authority must be secured, such that the result of a system function can not be modified by unintended actors.
An unintended actor is a person or a program which modifes the outcome of a system function by actions not intended as defined in the system requirements. This includes editing the messages sent between the nodes, such that the receiving node is not able to determine whether it was modified or not. This requirement does not include prevention of sapotaging of messages between nodes.