**CSCI-6908 - Individual Research**

**CERTUS Voting**

## Requirements Document

**Supervisor:** ProfessorMichael Clarkson

**Team:**

|  |  |  |
| --- | --- | --- |
| Ahmad Kouraiem | ahmadko@gmail.com | 703-477-8333 |
| Dmitriy Karmazin | dkarmazi@gwu.edu | 202-758-6826 |
| Hirosh Wickramasuriya | hirosh@gwmail.gwu.edu | 202-594-5448 |
| Steven Frink | sfrink1@gmail.com | 518-478-5880 |

## Requirements Document Plan

1. System Purpose

2. Functional Requirements

* User type
* Assets
* Importance
* User stories

3. Security Requirements

## 1. System Purpose

CERTUS has been derived as a simplified basis for Du-Vote: Remote Electronic Voting with Untrusted Computers with key system components and architecture designed for easy compatibility and conversion to the latter in the future. We will implement a simple “double envelope” voting protocol rather than the full Du-Vote protocol.

The purpose of this system is to implement CERTUS. The ultimate goal is to build system modules and graphical user interfaces that will be capable of delivering functional requirements described in the section 3 of this document compliant with security goals and resistant to threat analysis sections of this document. The system must be implemented in a secure manner following the principles of CIA.

The final system will be a fully functional voting system, although not all components of the system (detailed below) will be made fully secure in this project. The unfinished pieces will be designed as “black boxes”, so that another team could effectively complete the work in the future.

## 

## 2. Functional Requirements

**2.1 User types**

The system will be referring to four types of users:

1. Administrators - arbitrary user role who can manage other users and delete election. Cannot vote and observe election results
2. Election Authority - users with extended rights on creating and managing voting polls
3. Voters - regular users with the right to vote
4. Invited voters - users who have been invited by other users to sign up to the system, and yet, did not claim their accounts

**2.2 User Stories**

The importance of user story/functional requirement is indicated by:

* M - Must have
* S - Should have
* C - Could have, but not necessary
* W - Won’t have now, but would like to add later

|  |  |  |  |
| --- | --- | --- | --- |
| **User Type** | **Asset** | **Imp.** | **User Story** |
| Administrator | users | M | Can manage system users, assign/revoke their rights, edit limited user information |
| Administrator | election | M | Can delete an election |
| Election Authority | election, election password, candidates list | M | Should be able to create a new election, enter required election parameters, enter password for this election, and specify election availability either to all users (public election) or enter list of emails of users who can vote (private election) |
| Election Authority | election, candidates list | M | NEW ELECTIONS ONLY: Should be able to edit own elections’ parameters, except the password, enter required election parameters, and specify election availability either to all users (public election) or enter list of emails of users who can vote (private election). |
| Election Authority | election | M | NEW ELECTIONS ONLY: open elections |
| Election Authority | election, candidates list | M | NEW ELECTIONS ONLY: Should not be able to enter identical candidates into candidates list |
| Election Authority | election, voters | M | NEW AND PRIVATE ELECTIONS ONLY: should be able to add and remove users eligible to vote or invite users, emails of which could not be parsed, to register to the system |
| Election Authority | election, voters | M | OPEN AND PRIVATE ELECTIONS ONLY: should be able to add users eligible to vote or invite users, emails of which could not be parsed, to register to the system |
| Election Authority | election | M | OPEN ELECTIONS ONLY: close election (multiple times) |
| Election Authority | election | M | CLOSED ELECTIONS ONLY: reopen election (multiple times) |
| Election Authority | election, election password, tally | M | CLOSED ELECTIONS ONLY: enter election password, start tallying process, and publish election results |
| Election Authority | election | M | View number of people voted in the election so far |
| Election Authority | bulletin board | M | Should be able to view the statistics (How many voters did vote in general) while the election results are not published or election is not deleted. |
| Election Authority, Voter | election results | M | Should be able to view the results of the elections after they have been published. |
| Public | user account | M | Must be able to register as a new user in the system |
| Public | voter private key | M | Must have a choice of:  - automatically generating key-pair protected by the user login password and receiving protected private key by email upon registration  - automatically generating key-pair protected by a separate specified password and receiving protected private key by email upon registration  - upload own public key to the system |
| Invited User | user account | M | Receive email invitation to register in the system |
| Invited User | user account | M | Register to the system in accordance with invitation received by email |
| Invited User, Voter | user account | M | Restore access to the system if forgotten password |
| Administrator, Election Authority, Voter | user authentication | M | Should be able to authenticate to the platform P using username and password |
| Voter | user account | M | be able to change personal information |
| Voter | user account | M | be able to change password |
| Voter | voter private key | M | Update private key by using one of the options:  - automatically generating key-pair protected by the user login password and receiving protected private key by email upon registration  - automatically generating key-pair protected by a separate specified password and receiving protected private key by email upon registration  - upload own public key to the system |
| Voter | election | M | Receive email notification when private election this voter can vote in has been started |
| Voter | election | M | Should be able to view and pick the election this voter is eligible to vote in |
| Voter | candidates list, election, vote | M | Should be able to access the list of candidates and pick candidate to vote for |
| Voter | candidates list, election, vote | M | Should be able to view encrypted choice of candidate |
| Voter | token, voter private key | M | Input the private key into the token |
| Voter | token, voter private key | M | Use password to decrypt private key before using token to generate signature |
| Voter | vote | M | Should be able to input encrypted choice of candidate into hardware token and receive generated signature |
| Voter | vote | M | Should be able to vote |
| Public | platform | M | Can run a platform P |
| Public | token | M | Download and run token for MacOS, Linux, Windows |
| System | election, election key | M | Use unique private key for each election |
| System | System | M | Reconnect to database if connection has been dropped. Reconnect to RMI server if connection has been dropped |
| Administrator, Election Authority, Voter | platform | W | Authenticate using social networks |
| Voter | vote | W | Should be able to revote |

## 3. Security Goals

This section lists the security goals for the CERTUS Voting System.

1. The administrators can manage other users profiles, assign/revoke their rights.
2. Only administrators can delete any election.
3. Election authority can edit only their own elections.
4. The system should publish the results of the election after the election has been stopped.
5. Each election authority/voter must be associated with one and only one unique key pair in the system.
6. The system should require administrators, election authorities, voters to authenticate before using platform P.
7. The system should restrict voting only to voter users.
8. Only the election authority should be permitted to open, close, reopen, publish and edit an election.
9. Voters should be able to vote in any public election.
10. Voters should be able to vote in private election only if they have been explicitly invited to the election.
11. The system should restrict the voter to access candidate lists only when an election has been opened.
12. The system should restrict the voter to submit his/her vote only when an election has been opened.
13. The system should protect the voter’s choice from being exposed to anyone except the voter
14. The system must verify the authenticity of the vote before tallying.
15. Results of an election has to be accessible only by election authority and voters that have a right to vote in the election.
16. The system should accept requests from any platform.
17. No user should be able to submit a vote on behalf of another user (user identity is assured with username, password and hardware token).
18. The communication between the user and P, P and S should be secured.
19. Any private information associated with the users must be kept secret.
20. Election authorities should not be able to specify candidates with identical names
21. Users should have a choice of using their own key pair or protecting key pair by a password, other than login password.
22. Each election has to protect it’s votes by a separate key pair, protected by a password, specified by an election authority.
23. Users should be able to edit their own profiles only. Profile editing includes: editing personal information, changing password, generating new keys.
24. Users should not be able to change email address they have used to register to the system.
25. System should never transmit or store private keys, which are not protected by password.
26. System should never store users and elections passwords in plaintext.