Identifying Architecturally Significant Requirements

31.10.2017

— **CS3500 Software Engineering**

Team L

Ács Dávid - 117106523

Gonzalo Carranza Pérez-Tinao - 117106527

Palcu Liana- Daniela - 117106643

Martinez de Rute Maria - 117106133

Allocation of Responsibility		
Source	Requirement	Reason
P. 51, R. (last require mema	The machine needs to have an administrator mode that can be accessed with the administrators smart card. Additionally, administrator has to authenticate with one of the biometric sensors.	Administrator **mode** of the system; persons having an administrator's card can act as a system administrator **(user role)**
P. 129, R. 16	**Admin Privileges** Has right to register a voter and candidates, assigns public key for encryption and unique registration ID, edit information and check status/results. Voters use their URID(unique registration ID) to log into the system. To ensure one vote per one person this ID is then marked as "VOTED" in the database/receipt of vote. This also prevents unregistered voters from attempting to vote. The system can be accessed and managed only by using admin security password which is only known to the administrator in that district (it should not be set to a default password). Further preventing unauthorised access to the system.(Non FUNCTIONAL)	Defines **user responsibility** for the **admins**, stating that their responsibility is to manage the system.
P. 34, R. 1.	We would use multiple servers for counting votes. There would be a server for every county which then connects to a server for the province which then connects to the main country wide server. At each stage the server will count the votes that have been submitted and pass it on to the next server which will compile the votes and add them to the votes from the other servers so when reaching the main country wide server, it only should add the vote counts from the four provinces together to get the total vote.	One of the **major processing** steps of the election is counting votes and a hierarchical order of the servers establishes a **chain of responsibility.**
P. 54, R. 3.	[...]The machine should be able to automatically contact a technician should any crashing occurs. All technicians that do work will be required to provide reports and documentation for all the work they applied to a machine. Any administrator or engineer passcodes would be unique to the engineer, providing authentication and the ability to trace any modifications made. [...]	**User roles** are defined, in the requirement and their **responsibilities** are described (technician should provide reports)
P. 144, R. 7.	**Identification** The system shall identify candidates through scanning their passport. There are already softwares available to implement passport scanning and it would be convenient as	**Commercial packages** for passport scanning.

	(almost) every citizen in the country will readily have a passport available. [...] These softwares should also easily be available COTS. [...]	
P. 104, R	**Vote Count (Functional)** Ultimately, the most important thing about an election/ referendum is the final result. The total amount of votes for an election candidate, be it in a first past the post election etc., is an extremely vital part of the election process as a whole. [...] With our proposed E-voting system, we will ensure that a faster more efficient method of counting votes, which will be much less prone to error or miscalculation, will be required. Since we have proposed to use MySQL to store the votes, it seems only logical to use the built-in mathematical functions in order to process the huge volumes of data stored in each database. This would also afford substantial statistical information to be made available to the election officials for. [...]	The functionality of counting the votes is the **responsibility** of the MySQL database management system **software package**, more precisely the mathematically functions written in SQL.

Coordination model		
Source	Requirement	Reason
P. 55, R. 5.	[...] Fingerprint recognition is the most common of biometrics, especially regarding biometric authentication on computerized systems. [...] Ultrasound Readers, although more expensive than optical or capacitive readers, provide much more accuracy and will provide a great deal of security to the Voting system. [...] Alternatives could include another form of biometric such as a retina scan, or could come in the form of physical documentation such as passport, driving license, birth certificate etc.	The requirement mentions fingerprint and retina scanners/**sensors**. **Ultrasound Readers** should be prefered due to their **accuracy**.
P. 61, R. 18.	[...] With a digital voting system, there are concerns of data corruption, bandwidth, and transportation. Because of this, a data redundancy system must exist. For storage of information, each booth must have multiple drives in RAID to protect against drive damage. [..] Votes themselves should be sent over a secure, physical data line with some form of redundancy to ensure that the vote was sent properly, and a checksum to verify the received vote.	**Avoiding corruption** of data, ensuring **correctness** of transmission.
P. 25, R. (bottom of page)	**The system must be able to perform validation to ensure correctness.** The system shall have the following validation: frontend validation, which checks the data and ensures it is valid before sending it to the server, backend validation, which confirms that the data sent to the server was received correctly before storing it in the database and user-validation, which will make sure the voter confirms the candidates that are selected are correct. The validation should only take 2 seconds to complete and have no major impact on the response time of the system.	Checking the **correctness** of data, specifies the **time constraint** on the validation duration.
P. 137, R. 2.	**TCP handshake connection** To keep voting as secure as possible, to not allow packets to be dropped we will use a three-way handshake. TCP is at this point in time the most widely used transport protocol and the most secure. We want to assure there are no packet drops as this insures all votes make it to the server. [...]	Communication **protocol** of the system is TCP.
P. 130, R. 18	**Database records should be verified prior to tallying.** While the system should be designed to prevent errors wherever possible, the data must still be verified after voting has finished. This should be done at each polling station, and at the regional and national levels where applicable. This would include identifying and reporting any corrupted or malformed records, any duplicate entries, etc.	Completeness, correctness and consistency.

Binding time decisions		
Source	Requirement	Reason
P.132, R.5	**English/Irish Language version.**The system shall also support an Irish language version of the interface. This will cater to those living in Gaeltacht areas and for those who merely wish to interact with this system through Irish. This shall be implemented much in the same way that ATMs do. Upon the first interaction with the user, the system will ask if the user would like to proceed in English or Irish. This system shall also be available for at least 99.9% of the machines in the country.	Before you begin to vote you have possibility to choose between two **languages**:Irish and English; two regional different languages.
P.71, R.1	**Desktop application and mobile application** [...].The desktop application will support operating systems such as Windows, Linux and MacOS. Also, the system can be implemented as a mobile application.[...].The mobile application will have a similar interface as desktop application and will be built to be supported on platforms such as Android, IOS and Windows Phone.	The system provides **portability** on different environments even it is a desktop(Windows,Linux,Mac OS) or a mobile (Android, IOS, Windows Phone) application.
P.78,R.5	**Electoral District Selection** - The website must be able to establish the user's electoral district(information saved in the database server, in relation to his/her username) and propose only the candidates of that particular district.	During the **run time**, the system should adapt his **functionality** according to the user's electoral district.
P. 126, R. 10.	**Dynamic between elections and referendums –** The software must be dynamic for different scenarios, for referendums all that's needed are simple yes/no answers from voters where Local and General Elections can be more complicated.	The software is providing the ability to **configure** the election type by using an interface for polling staff.

	Therefore, the interface must be able to cater for these different circumstances. The software must also provide the ability for these circumstances to be configured, this could be done remotely or by providing an interface for polling staff to configure the election type but also other minor configurations.(Functional)	
P.92,R.14	Function: **Changeability** Description: Ability to update or change features of the e-voting without affecting the components of the e-voting machine. [...] Action: Make incremental changes testing at each step to make sure the e-voting machine is working correctly.	The system should be capable **to extend his** functionality by updating or changing his features without affecting other components.

Choice of technology		
Source	Requirement	Reason
P.54, R.4	**A secure connection must be maintained between the Voting Machines and the Secure Database.** [...] HTTPS or a similar protocol must be used to guarantee a secure connection that can protect the voter's data. [...] Fibre Optic connections should be used to provide fast and reliable connections for each of the Voting Machines, as it is currently the fast method of data transfer. [...] TCP connections will be used as the transport layer protocol for the voting data. [...]	**HTTPS protocol, Fibre Optic connections** and **TCP connections** are specific technologies chosen to assure a secure connection.
P.77,R.2	**Voice Over and Speech Recognition -** In order to provide equivalent user experience for people with disabilities, the e-voting website must have a Voice Over feature which reads out-loud the content of each page. The user must be able to use a Speech Recognition tool to navigate on the platform and select his/her preferences.	For people with disabilities it is used a **specific technology** such as Voice Over and Speech Recognition.

P.103, R.7	**Storing Vote.** There are a number of different ways this can be achieved, but as we are leaning more in favour of using open source software, our main resource would be to have a MySQL database running on each machine. A number of intuitive scripts (Python or PHP) will be used to access and store each of the votes. [...]	**MySQL database** has been selected to store the number of votes.It has been chosen because it is an open source software.
P.128, R15	**Future of User Identification:** Biometric Identification. Departing from token based identification systems a combination of Fingerprint Identification, Retina Scanning and Face Recognition could provide a secure and streamlined way of identifying voters.[...](FUTURE FUNCTIONAL)	It is proposed that in the future to be another way of identification by using different technologies such as **Fingerprint Identification, Retina Scanning** and **Face Recognition**.
P.10,R.6	**Future Proofing.** It is key that the system is adaptable in order to make room for further development in the future. As a result of this, software, hardware, and procedure, should all be considered modular and open to further development. If, for example, biometric data were made available as a widely usable security feature, it should be possible to implement it into the voting mechanism with minimal changes to the software or hardware. Hardware upgrades such as fingerprint or retina scanners should be simple to integrate into the verification process as a result. This also applies to the voting process, if in the future it becomes possible to ensure absolute security while connected to a network, i.e. not allowing any new vectors of attack due to the connection to a network. Then it should be possible to make use of the network to transmit the data from polling station to counting center, without the need for polling stations to be air-gapped.	All software and hardware components should be open to further development due to the **evolution of technology**, for example, biometric data or fingerprint or retina scanners.

Data model		
Source	Requirement	Reason
P.25, R.1	**The system must handle live corrections and cancellations.** This requirement is relevant as people may want to change what they selected, either by correcting it or deleting it. A live change can be made only during the process of filling the voting form. Once the vote gets sent, it will not be possible to modify it anymore. In the case of a cancellation, the system must require another voting form to be completed.	The system should be **persistent** once you have sent the vote in order to avoid errors in modifications.
P. 80, R. 11	**Availability** [...]Outside of the voting period, access to the website to view candidates, edit account password and access tutorials should be warranted. [...]All other visible website displays are consistent and do not change for the website. For example, candidate information is visible before the window, during it and afterwards. Otherwise, the database access is granted and can receive the necessary voting submissions. At the point where the timer has reached its limit, the database will stop receiving the vote submissions and commence computing the election results. The website will thus return to its original interface view with no drag and drop options available anymore.	**Processing steps** All the users have access to the website, the database will be receiving the votes until the end of the voting time period, then the elections results are compute.
P. 56, R. 7	**System for Instant Runoff Voting for President** [...]In the voting process itself with use of the user interface, the candidates will be ranked by the voter. The ranking will be transferred to a priority list with a unique identifier for this voter when they finished and confirmed their vote. After the vote is confirmed the vote is sent a packets over a dedicated network with secure protocols.	The votes made by the users are transfer over a secure network. **Information flows**
P. 143, R. 4	**Local Network** [...]The more stations, the more ethernet connections we will need, and the database must be able to handle a large information flow from up to 30 machines in a large venue. [...] This part of the architecture is an absolute must to be implemented, as we	A large **information flow** is going to be transfer from the voting machines to the database.

	need a secure way of transferring information from voting machines to our database. Without it information could be lost, corrupted or tampered with.	
P. 71	**Change your previous vote** The system, as the traditional voting, will only allow one vote per user. When the user's vote has been made, the server will not give the user the option to vote again. [...]	All the people can vote only one time, and in order to the **persistence**, the user can not vote again.

Mapping among architectural elements		
Source	Requirement	Reason
P. 27	**The system's server shall be in a secure location with excellent connectivity to most of the voting stations.** The system's server should be protected and in a location, that has the best connectivity to most of the voting stations. Staff must ensure the security of the location. Connections should be tested to trace the best connections to find a location for the server.	The stations around the country should have a good connection so is necessary to find the best way for the **network coordination**.
P. 26	**The system must run on a dedicated machine.** Each voting booth will run on its own dedicated machine separated from the server. Each machine shall be running its own instance of the voting program and shall have no interaction with any other machine. Each machine shall have identical hardware specifications and shall have near identical response times within 1ms of each other. Each machine shall have equal priority to access the main server's network. [...]	Regular synchronization, **communication** between each machine and the network.
P. 57, R. 8	**System ensuring one person, one vote verification.** [...]At the database, the random Id connected to the pps number and biometric will add a flag or notification that indicates the voter has voted for this election timeframe for this specific election(in cases where local elections or referendums are also being held). [...] This flag or notification will be sent to the biometric	A way to ensure that one person votes one is **communicate** the flag to the biometric scans. **Communication** between local voting machines

	scans of the constituency to prevent anyone to vote again as that voter This is all reliant on a dedicated line to ensure fast and reliant communication between the local voting machine and a central database. [...]	and the central database
P. 58, R. 10	**Network for E-voting system** The entire system for e-voting will require the need for fast secure and reliant communication from the local voting centres and the government's central database. [...] This dedicated network will ensure that communication will be fast. The network will not need to be support significantly heavy data transfers as data used by each voter will not be significant, but near consistent transfers from each centre. The network will need secure protocols for data transfer.	**Network coordination** for the system should ensure a good and reliable **communication** between the local centres and the central database
P. 73,	**Perform audits** All operations should be stored on a secure hard disk. Any vote or change should be stored in at most 1ms. You can't delete the information during election, it is only for append and read. There must be at least two hard disk in which the votes are stored to ensure the counting in case of failure.The information of the number of votes for every candidate should be refresh every second on the disk.	**Regular synchronization** on the disk, **communicate** and store the information on differents hard disks.

Management of resources		
P.72	**Support for physical voting:** The system can be **installed both** at home and in the voting station for those users with problems accessing the system from home either because they do not have a computer or because they prefer someone who advises them when using the new voting system. For the voting stations the user must access the system using the provided passwords and through facial recognition. The assumption about facial recognition is that each of the citizens' faces will be scanned when they create their ID, and that scan will be used in the authentication process to verify the identity of the citizen.	The system can be installed in different **devices** and also in voting stations
P.12 R.10	**10) Cost Effectiveness:** [...] **Power efficiency**: By ensuring systems not currently in use are either switched off or in a sleep state and working as power efficiently as possible while in use; power costs can be	All systems will be **Power efficiency** and not to suppose

	greatly reduced and with improvements in power efficiency over time as practices and technology improve, future power savings can be made. [...]	an unnecessary cost both monetary and environmental.
P.8 R.3	**3. Reliability:** During registration user **data** is collected at predefined registration centers and **stored** in a database. If the registration center is compromised an alternative nearby center will become the backup. The database that stores the user data should have adequate backup databases in different geographical locations to minimise the risk of data loss.[...] [...]All data/votes collected at a polling station will be **stored** to minimise the chance of **data** loss (eg with the use of a RAID)[...]	All the data will be stored repeated in differents database to minimise the chance of data loss (**memory footprint**)
P.46 R.5	**5. Minimise users' time on web application (Non-functional):** Specific- Minimise the amount of time individual spends on the web application Measureable- Allow 3 minutes for user to vote when in the voting process Attainable- Once user is in the voting process, limit the time spent to 3 minutes Realistic- An individual will have 3 minutes to vote when selecting their candidate to ensure extra time if required by the individual Traceable- The app hosts require minimum congestion by limiting time spent on app to ensure robustness.	With the amount of connections this system is required the system will only allow a short period of **time** to the user to make the vote
P.146 R.12	**Backup:** The system shall create and maintain **regularly scheduled backups** of each of the local databases. These backups should be renewed every **15 minutes** and should remain safe in the case of a **power outage**. It should also be able to run simultaneously to the other database functions. This could be difficult to implement as the backups would need to occur at the same time as many different database queries without affecting the efficiency of the voting devices. **Scheduled backups** are needed in case of any corruption of the data in the tables. [...]	**Scheduled** backups in case of any problem occur during the system is on.

CONTRIBUTIONS

Dana: I find requirements for binding time decisions and choice of technology categories.
Gonzalo: I find requirements for Management of resources.
David: I identified the ASRs in the categories Allocation of Responsibility and Coordination model.
Maria: I find requirements for Data model and Mapping among architectural elements.