Introduction

This document attempts to outline the functional and nonfunctional requirements for an electronic voting system for the Republic of Ireland.

The requirements detailed below assume a number of things, we assume:

- The Public Services Card (PSC) is fully setup and incorporated into most governmental services, that a large number of eligible voters are in possession of the card and that the process of obtaining the card confirms the person's identity.
- There is not a means of ensuring that a connection over the internet is fully secure, which is guaranteed to ensure no eavesdropping or data manipulation occurs.

An outline of the system we have designed is as follows.

- Registration to vote must take place in the weeks prior to the vote, this can be done online, provided one already has a public services card, or otherwise at a social welfare office
- Candidates or options must also be registered well in advance of the vote also
- Polling stations are provided with several terminals which can be used to cast votes, these machines are not network connected and as such, each machine is preloaded with the list of potential voters and the required details to show them the correct options for their constituency
- When going to vote a voter’s identity is verified with the use of their Public services Card coupled with facial recognition based on data which is on file, similar to the process used at customs in many airports to verify passports.
- Votes which are cast are stored locally on the disk of the machine and encrypted during the voting process
- When a vote is cast, a vote id is associated with the voter's selection and the voter’s identity, this is stored separately to ensure that it is not possible to directly map votes to individuals. It does however allow a voter to use this unique identifier after the counting process to ensure that their vote was counted successfully without sacrificing anonymity.
- Votes are decrypted when the voting is complete, but there is a hash made of the collective data to ensure it cannot be interfered with
- Disks are then physically transported to counting stations, for each polling station a copy of the data must be sent to at least two counting stations to ensure count is correct
- Votes are counted digitally at each of the counting stations and can then be released once verified to be correct

Functional Requirements

1. Registration of User

In order to make the registration of voters as easy and accessible as possible, an additional online registration system should be implemented alongside the current face to face system for those who wish to use it. This will speed up the registration processes and make it much more available to those not close to registration offices. The Public Services Card(PSC) will be a non-negotiable requirement for registration.

The registration process should retrieve the details required to facilitate further system requirements such as verification, eligibility, circumstantial alternatives and polling station management. The data collected at this stage should be the government issued Public Services Card(PSC), using this the data required can be gathered from government services linked to the Public Services Card(PSC) under its current implementation.

Under the current implementation of the PSC; Photo Identity, Proof of Address, and a handwritten signature are collected during the application for the card. We can now assume this data is now available to us and in order to verify identity at registration, only a copy of Photo Identity and the PSC needs to be presented either to an officer in office or uploaded to the online system.

At this point the user should be made aware the PSC will be required to cast their vote at the polling station, failure to meet this requirement will prevent/inhibit their ability to vote.

2. Verification

It must be possible to verify the identity of a potential voter when they visit a polling station, this will be accomplished using the Public Services Card which is currently being implemented, as this card is intended to be used for access to all public services, it is a requirement in order to vote using this system.

Swiping the card at the polling station will trigger facial recognition using the information already available from registration time, similar to the process currently used to automatically verify identity at customs in many airports. Provided this process completes satisfactorily, the person can then cast their vote.

In cases where there is an issue with the verification process, an attendant can manually verify the user using the data available from the registration process. Verification information is stored locally at the polling station, taken from the most recent valid Register of Electors. As a result one may vote at any polling station available to them, options will be based on the constituency of voters primary address, any duplicate votes can then be removed during the Aggregation of the data.

3. Eligibility

Voting multiple times in the same election and unregistered people voting should not occur. To check for eligibility, anyone who wants to vote must use their Public Services Card and the PPS number on it be checked to ensure the person is eligible to vote.

In order to prevent people from voting twice and to prevent ineligible people (e.g. people under 18, non-Irish citizens) from voting, information about PPS numbers and eligibility to vote can be obtained from government records and stored in a data structure, and there will also be a check to make sure that nobody votes multiple times at the same polling station. Both eligibility and whether the person has voted already at this station will be checked before the vote is cast.

If the person is not eligible or their vote has already been cast, it should not allow them to vote and display an appropriate message explaining why they cannot vote. Votes cast by the same person at separate polling stations will be checked and removed at the Data Aggregation stage

4. Anonymity

All stages of the voting process should allow voters to remain as anonymous as possible. All information collected on voters and those registered to vote should comply with the Irish Data Protection Act 2003. Information should only be disclosed on a need to know basis in order to protect the anonymity of who is registered to vote, where a person cast their vote, when a person cast their vote and who the person voted for.

At registration every effort should be made to ensure anonymity. A secure connection should be required in order for a registration to be completed online. An Post must be used to deliver any registrations by post as they adhere to a suitable Data Protection Policy.

At polling stations, polling booths must be adequately spaced to ensure a person cannot see into a booth when at another booth or when coming or going to a booth. If text to speech is being used for accessibility reasons the booth must be placed in a separate room where no sound can be heard from outside. Another possibility is in ear headphone support.

When votes are collected every effort must be made to ensure if polling data is intercepted by an unauthorised person at the polling station or during transit to the data aggregation center that an individual person cannot be linked back to who they voted for.

5. Right to Protest

As submitting a spoiled or empty vote is a form of protest, it must be possible to do this under the new voting system. As a result, during the polling, an option for a spoiled or null vote will be included.

This ensures that the vote is intentionally spoiled and will not be counted toward any option. This vote will be accepted in the same manner as any other votes cast, and will only be differentiated during the data aggregation stage of the process.

Spoiled or invalid votes will be included in the count of total votes cast, however they are not, of course, attributed to any of the voting options.

6. Data Aggregation

Data on candidates can be obtained from government records, and data on votes can be obtained by storing the votes for each candidate in a data structure, and updating the votes each time a vote for a particular candidate is cast, ignoring spoiled votes.

Only one data structure will be needed to store all the votes, and all votes cast will be sent to the computer running the data aggregation program which contains said data structure, which eliminates code duplication and the need to have results stored on multiple devices only to add all the results together at the end which would slow down the voting process.

Once the deadline for vote casting has been reached, the data structure containing the vote data will be passed on to a function that will find the people whose number of votes exceeds the quota, and distribute those candidates' excess votes among the people with lower totals based on preference indicated by voters, repeat the above process until a winner has been found, and return the name of the winner.

This method will eliminate the need for vote counting to be done manually by people, and reduce the possibility of error due to miscounting votes.

7. Authentication of Integrity

It is of vital importance that it is possible to verify the integrity of the data to ensure the validity of the vote. In order to ensure that data is not manipulated before reaching the counting stage, several measures must be put in place to ensure the data cannot be a manipulated at any stage during the voting process.

Firstly, it should not be possible for anyone to have direct access to the data while the polling station is opened, thus, while the voting process is ongoing data should be encrypted when stored to disk.

After the polling station has closed, a hash of that data must be made during the decryption process of the vote information and stored separately. When the data arrives to be counted it is first checked to ensure the hashes still match and that the data has not been modified during transport.

Finally, the counting itself must also be verified, as a result copies of the raw data should be sent to multiple centres to be counted, each count must match to be sure that no tampering has occurred.

8. Polling Station Management

Polling station management is an important aspect to ensure that polling stations are safe, efficient and are operating correctly. A hierarchy of personnel will be tasked with managing the polling station and the people that come to vote.

Each polling station supervisor must complete a risk assessment. The assessment must assess all of the potential risks to the voting data, the polling station personnel and the voters who attend the station. All risks must be considered and policies must exist for each scenario. Possible dangers include crowd surges, flooding, robbery, adverse weather, loss of electrical power and acts of terrorism.

All personnel must be trained and have knowledge of the policies relevant to their polling station. The polling station supervisor must also designate a dedicated assembly point in case of an emergency. Personnel must all know where the polling stations assembly point is. At least one member of staff must be fully trained in first aid, cpr (cardiopulmonary resuscitation) and aed (automated external defibrillator) use.

The polling station supervisor must also complete a access management plan to ensure adequate parking and pedestrian access is available. They must also ensure that a plan for traffic flow is completed to ensure traffic does not become blocked or stagnant which would prevent voters from voting.

9. Registration of Candidates

All candidates must be registered before the day of voting, any candidate who is not registered by then cannot be voted for, and it must be ensured that they are eligible to hold the position they are running for (e.g. all candidates for President must be at least 35 years of age and Irish citizens, and must not have exceeded 2 terms (14 years) as President).

The required information on these candidates can be obtained from government records and entered into a data structure with entries for each candidate, including the candidate's name and the required information (which would include criteria that are necessary for the position, such as being an Irish resident for local elections, and criteria that would disqualify you from the position, such as being convicted of fraud for local elections)

A program could be written to check that all candidates meet all the criteria by taking in the data structure mentioned above, and making sure each candidate meets the requirements for the position they are running for and avoids anything that would prevent them from taking the position, and output a list of the candidates who do meet the requirements onto the screen for voters to choose from.

10. Circumstantial Alternative

As not all citizens are available or capable to come to a polling station a circumstantial alternative should be available (for those applicable within reason). This alternative should apply to citizens afflicted by severe movement inhibiting conditions(the elderly who cannot leave their nursing home / hospital indefinitely, those who cannot leave their home / hospital due to long term medical conditions, etc) and available to civil servants working for the state abroad long term(Diplomat, Defence Forces, etc).

Due to the wide varying range of applicable conditions, an easily available and reasonably effective method for casting / collecting votes should be in place. Due to the far smaller population the alternative must cater for and the focus on availability and accessibility over all else; the alternative does not necessarily have to be as cost effective or time efficient as its counterpart. The alternative still must be secure, anonymised and traceable.

The current circumstantial alternative could be carried over if see to be sufficient (votes cast by post), although a more efficient and secure method should be used. E.g. heavily protected portal.

Non-functional Requirements

1. Accessibility

This voting system must be accessible to a maximal amount of people, which means it must accommodate people who are blind and/or deaf, allowing their voices be heard too

A pair of headphones will come equipped with every portable voting device to allow blind people to hear who they are voting for without letting others know as well. These will be handed to the user by the member of staff holding the voting device (unless the user indicates they are deaf)

The e-voting app and website will have buttons that read out the name of a candidate once you press them so blind users will know who they're voting for, and give instructions (e.g. "Do you want to vote for this candidate? If yes, press once, if no, press twice)

There will also be a button to read out voting instructions (e.g. "To vote for Leo Varadkar, press 1…") to the user, and there will be a button you can press to repeat what was just said in case you missed it (the option to repeat will be given after the end of all messages).

The portable voting devices will have buttons with numbers written in Braille and each number is mapped to a candidate or to the information or repeat buttons, if there are surplus buttons they will remain unused, and all devices will have enough buttons to cover the maximum amount of candidates. Once any of these buttons is pressed, an audio message will be played to the user, exactly like on the app and website.

2. Security

The e-voting system must be as secure as possible in all regards, this is for the security of both users and data. Holding a high standard of security will help in completing some other requirements set out, namely Anonymity and Reliability.

Security can come in many forms, having personnel available at the polling stations as outlined in Polling Station Management is very important as this adds physical security to both the stations systems and the users coming to vote. Apart from physical security, holding data securely is of highest importance.

All data held in the system should be encrypted using a strong enough method to ensure its protection in the event of the data being accessed by unauthorized person,
Systems holding data must be held in a secure location inaccessible to the public and only by authorised personnel.

After the voting stage has been completed, all data must be brought together in a secure manner. The safest way for this to occur is to have storage devices holding the relevant data needed for the data aggregation, authentication of integrity and traceability to occur to be collected by authorized personnel directly from the polling stations and physically transported to the necessary location. To avoid any mishaps, any personnel to come in contact with the data will also have their reason attached and recorded e.g. (Prepared device for transport, Collected from station X, ect).

3. Reliability

All stages of the voting process should be reliable and have backup measures in place to ensure that failures do not interrupt any stage of the process.

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 polling booths will have redundant hardware components so as to ensure the smooth running of a booth even after a hardware failure. If a booth does fail, then the other booths at a particular polling station will be the backups. 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). If a polling station is compromised then an alternative nearby polling station will become the backup. All polling stations will be equipped with a basic UPS (uninterruptible power supply) that must be capable of powering all the polling stations critical systems for at least one hour.

Software on the polling booths must be reliable and must remain operational during voting. A voter must not be able to cause the software to crash or become inoperable for the next voter.

4. Quality

All interactions with the system either by staff or voters must be as user friendly as possible and try to minimise errors.

The interface that allows staff to enter eligible voters details must be easy to understand and must make every effort to ensure data entered is valid and no mistakes have been made. If a mistake is detected the end user should be given an adequate error message, allowing them to quickly locate their error. This should ensure the quality of the data stored by the system and minimise incorrect data.

The user interface must be visually appealing and easy to understand and navigate. Colours used in the interface must be contrasting so that text is easy to read. The user interface must also ensure that the voter confirms their vote and understands what they have selected before confirming their selection. A help button should always be visible on screen to allow the voter to alert a member of staff that they require assistance.

Focus groups will be used and at least 75% will have to be in favour, this will ensure the system conforms with these specifications.

5. Efficiency

The entire process from start to finish must finish in a reasonable time period for the application to be beneficial.

During first use for a specific type of election/referendum the system must be capable of registering every eligible voter in under eight weeks. Every use thereafter for the same type of election/referendum we will assume the system will already have a majority of people registered from the previous election/referendum so it must be capable of completing registration for all eligible in under four weeks.

Each polling station must be capable of verifying and collecting the votes of people at the rate of at least 120 people per hour.

Data aggregation and calculation of results cannot take more than six hours from when the last polling station closes.

If a voter wishes to confirm their vote, the details of their vote must be made available to them within one week.

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.

7. Environmentally Friendly

The e-voting system must be eco-friendly and reduce the amount of waste produced compared to other voting systems. This electronic version reduces amount of paper used for voting ballots by 100% by replacing paper ballots with digital ballots.

However, the alternative of having people carry an electronic voting device and travel to people who don’t have their own device to vote with could cause some pollution if the people travelling to those who cannot attend polling stations travel by car.

This could be reduced by having said people travel short journeys on bicycle or on foot, and for long journeys, carpooling could reduce the number of cars on the road and thus the amount of pollution caused by travel.

There must be someone with a voting device for people without Internet/electronic devices within a 10-kilometre radius of each town/city to reduce the amount of pollution caused by long journeys and maximise the number of people reached.

8. Non-Suggestive

As with all fair democratic votes, this system should be absolutely impartial when allowing votes to be cast. In essence, this means that all options should be displayed equally, without variation based on party, candidate, issue, etc.

There should never arise a situation where one of the provided options is presented more favourably at the polling station, options should be presented equally, without differences in formatting, images quality, etc, and should also be presented in a random order in a random order.

This extends to all portions of the voting process, no particular allowances can be made for voters of any particular persuasion, and any staff or personnel should not represent their personal views while providing a service at a polling station.

9. Traceability

In order to ensure all votes are accounted for, the system should allow for cast votes to be traceable to its owner at the the voters discretion after the results have been set while still holding voter's anonymity.

After a user's vote has been cast, the user should be given a unique key, where their vote is linked to that key, yet their identity remains unknown unless the user requests their vote.

If a user requests their vote it should only be retrievable when the user gives both the key and some other piece of information required for the retrieval, this other piece of data could be a multitude of things for example their Public Services Card number, a predefined password, a second given key not stored or linked to the data, etc.

To ensure future anonymity this traceability should only be available for a period of time after voting e.g. 6 months or so, until this function is no longer seen as necessary, after that point the data should be disposed of properly.

10. Cost Effectiveness

Other than efficiency, cost effectiveness is another requirement and advantage e-voting systems have over paper balloting systems. In order to ensure its cost effectiveness the system must be three things: paperless, power efficient and require less manual labour.

Paperless:
By utilizing the potential of the Public Services Card and storing votes and user information digitally, paper is no longer a requirement for voting to function. This abolishes the cost of paper and makes voting more eco-friendly.

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 greatly reduced and with improvements in power efficiency over time as practices and technology improve, future power savings can be made.

Less manual labour:
By overall reducing the number of personnel involved in the process major labour costs are cut. The largest of these reductions is in the tally of votes, by performing the tally electronically over employing hundreds of personnel to count votes costs can be greatly reduced.

Introduction

For this Software Engineering assignment, we, as a group, have created a set of requirements for a future e-voting system to be used in Ireland. The set of requirements has been made following a referendum-style vote in lieu of a general election. As we have chosen this method, we only have to consider votes where one candidate was chosen out of the total number, instead of a ranking system (like the current system in place).

The system has a database which contains information about eligible voters and their e-voting accounts. This database is not only used by the system, but also by the government employees, during election processes. The government employees use the database to mark people who voted physically, at a polling station.

Voters create their accounts only once, after they have turned 18 years old, and they can use them for the rest of their lives, after the accounts were validated by government employees.

Requirements

Functional

1) **Reject multiple voting online:**
   The system should not allow users to vote online more than one time per election session. An error message will be displayed if a user tries to vote a second time.

2) **Reject voting both physically & online:**
   The system should know and record which users voted and which didn't vote. The system's database will also be used in polling stations, and will record the voters who have voted there. This will be used by the e-voting system to check if the user, who is logged into the account, has already voted elsewhere.This way, if someone already voted at a polling station the system will not allow that person to vote again online.

3) **Voter anonymity:**
   The system shall keep the identity of the voters anonymous, except general information like gender, age and the county the voter lives in. The system will access this data only for statistical purposes, but the voters cannot be linked to their vote.

4) **Voter eligibility:**
   The system should allow only authorized users to vote. Authorized users are people who have turned 18 years old, have registered into the system's database and, after the information was verified and validated by government employees, they were provided with an active voting account.

5) **Vote integrity:**
   The system shall not allow any modifications to a vote after it was cast. It will also forbid the deletion of an already cast vote.

6) **Information regarding election candidates:**
   The system should display all the candidates in a row, in such a way all of them are seen equally and entirely on the same page, so that no one is disfavored. This way no other action (like scrolling or zooming out) will be required.

7) **Voting cast:**
The system should allow users to select one or more candidates and then, to submit their decision. In case a user chooses more than one candidate, the system will mark the user as if he/she voted, but the vote will not be taken into consideration.

8) **Voting results:**
The system should display at the end of the election session, after the physical votes were also counted, detailed results (in a graphically-friendly way), such as showing on a map which candidate won in different counties/regions and presenting charts with the final results.

9) **Creating queries based on the election results:**
The system should allow users to create queries for statistical purposes. For example, what is the percentage of male voters who voted, what percentage of people voted out of the total number of existing voters, age distribution, gender distribution. See Functional Requirement 3.

10) **Help section:**
The system should have a section containing frequently asked questions, instructions on how to vote and one or more contact numbers and emails belonging to the maintenance staff.

11) **Message reminder:**
The system should send a message reminder to the users one hour before election closes.

12) **Account types:**
The system should have two different types of accounts: the user account and the admin account (changes user passwords if needed, add election data prior to elections).

13) **Data security:**
Data sent to and from the system must be encrypted at all times. Also, redundant paths to the system must be provided in order to prevent malicious attacks, such as Distributed Denial of Service.

14) **Voting period:**
The e-voting system should only be open for voting at the same times as the polling stations. If the vote is to take place over multiple days, the voting feature of the system should be operational from the opening of the stations on the first day of voting to the closing of the stations on the final day of voting.

Non-functional

1) **System portability:**
The system should be portable, so that any authorized user who has a device with an internet connection could vote.

2) **System performance regarding users:**
The system shall support at least 100.000 simultaneous users.

3) **System performance regarding timing constraints:**
The connection to the system should not take more than 5 seconds, provided users have internet connection.

4) **Graphical interface:**
The system must have a nice, simple and user-friendly design (graphical user interface), in order to attract as many people as possible to vote using the system.

5) **System reliability:**
The system must be 99.9% reliable regarding the saved data. All the information stored by the system must be backed up at any time to ensure that no recorded votes will be lost due to unexpected situations, such as loss of network communication, server failure or others.

6) **Election results availability:**
The results and the tools for creating queries should be available at least 48 hours after the election process ended.

7) **Modularity:**
   The system should be designed in a modular way, such that adding new features later on could be easily implemented.

8) **Voting attempts:**
   The system should allow a user three 5 minute attempts to vote. A user can be logged in for maximum 5 minutes at a time. If he/she reaches 5 minutes in a session the system will automatically log the user out and a warning message will be displayed. If the voter does not submit a vote after three attempts he/she does not get an additional chance to vote again.

9) **Updating data in the database from multiple sources:**
   The system shall have a mechanism which ensures that the same data cannot be updated/created, in the system's database, from multiple sources at the same time. For example, this mechanism should block the attempt of a voter trying to cast two votes, one from the polling station and from the online system, at the same time. See Functional Requirement 2.

Team members' contribution

We all equally discussed the requirements and made them as SMART as possible and we divided them into the Functional and Non-functional categories.

Introduction

In this project we propose to design and implement a new E-voting system for Ireland. We are focusing on components – machine and software. To implement the procedure we follow the Scrum procedure method. To do that we identified these requirements which we needed to have:

Design

In our modern democratic society one of the most important things is freedom to choose something better for everyone; for example, the process of voting is very important where people can choose a new leader for their country. The process can be made easier with an EVM (Electronic voting machine), where voters can be sure that their voting process will be quick and intuitive, their vote will not be manipulated and privacy will be maintained at all times.

Each voting machine will be surrounded by partition walls to ensure privacy. The machine will consist of a touch screen of the dimension 1280 x 1024, an electronic scanner which will take a passport or a public services card as a form of identification, a camera above the screen to scan the voter's face and lights at all corners of the screen. The system will provide an easy and intuitive voting process for voters. During voting, the screen will be split into two parts and the candidates will be represented by simple descriptive boxes which can be dragged from the left hand side of the screen to the right.

At the conclusion of the election, the system (DBMS) will be able to produce the results. The results will be displayed in a table where the candidates will be ranked by the number of points they received. From this the final result can be obtained.

Verification

Functional:

- There will be a flashing light on the scanner to indicate that it is ready to receive either a public services card or a passport. The identification must be placed face down on the scanner platform.
- The scanner extracts the passport number from the passport or the public services number from the public services card and uses this information to verify that the voter is registered to vote and is to vote at this polling station.
- The verification system will ensure the identification is in date by examining the expiry date of the identification. If the identification is in date it will extract the image on the identification and it will be stored locally. If the identification is out of date the identification will be rejected.
- The extracted image will then be used in conjunction with the facial recognition camera to verify the voter is both registered to vote and is who they are claiming to be.
- The facial recognition camera will be triggered by the identification scanner. The lights surrounding the screen will light up to eliminate any shadows on the voter's face.
- The camera will provide a live feed of the voter and it will try and match the voter to the extracted image from their identification.
- The voter must make eye contact with the camera and hair must be tied back if necessary.
- The display screen will show a live feed of the process. The camera can move its angle to best capture the profile of the voter.
- Once the voter is verified, the system will delete the records of the public services card/passport and the images of the voter for privacy and security purposes. The voting section will then be displayed for the voter.

Non-Functional:

- The cameras verification feed should need no longer than 10 seconds.

E-Voting Process

Functional:

- Once the voter's identification is verified the screen changes from the live camera feed to the primary voting screen. This screen must be split in half with a scrollable list of all candidates on the left and a hollow frame of a list on the right; this is the voting list.
- Each candidate will be represented by an interactive rectangular icon. This icon will have an image of the candidate on the left hand side and information regarding the candidate. Such as the name of the candidate, party and the party logo.
- After a short hold-down touch of the list element it will shake to indicate to the user that it's ready to be moved to the right list. This hold-down action is necessary to avoid accidentally moving a candidate to the right list while trying to scroll.
- The right list is of fixed size to fit a maximum of 10 candidates to work with the point calculation function. If a user tries to add an extra candidate to a full right list the system will provide clear feedback as to why they can't add more than 10.
- Once a list element (candidate) is added to the right list, a small red X will appear in the top right corner of the element's frame to allow the user to quickly remove that candidate from the right list. . The candidates lower in ranking to this candidate will be moved up 1 position.

- Alternatively, if the voter would like to simply rearrange the candidates instead of removing one they can once again do a short hold-down of the candidate and can reposition them, similar to moving app icons on a smartphone.
- Once the voter has their desired candidates in the correct order they press a "CAST VOTE" button at the bottom of the right list. This brings up a finalised list of the candidates and their positions so the voter can clearly see who they're voting for and how many points they're giving them one more time before they confirm. The votes are then sent to the main server where the points are assigned and calculated. See more in the Point Calculation section.

Non-Functional:

- After confirming the vote, the voter is shown very clear feedback that their vote has been accepted.
- Clear instructions in the middle between these lists tell the user that the candidate list elements need to be dragged from the left list to the hollow list on the right.

Vote Calculation

Functional:

- Once you confirm your list of candidates, your votes (candidate ID and position) are sent to the main DBMS (Database Management System) and the scores calculated.
- You must select a minimum of 1 candidate and a max of 10.
- Candidate 1 gets 10 pts, Candidate 2 gets 9pts, and Candidate 3 gets 8pts etc.
- Points = 10 – candidate Position + 1.
- This can be stored in an immutable Dictionary.
- Dictionary [candidateID] += Points.
- Each candidate has an ID which is its key in the dictionary.

Accessibility

Functional:

- The system will ask the voter if they'd prefer to vote in English or Irish.
- A solution for blind voters would be to allow to vote using voice recognition. An audio guidance system would guide the voter through the entire process using earphones. At the voting stage, the guide would read out the name of the candidate and allow the vote to be cast. After every candidate name, there is a 5 second pause for the vote to be cast. The first time going through the candidates, the voter picks their first preference by tapping anywhere on the screen to stop the guide on a candidate and then asks them to tap once again to confirm and twice to decline if they chose that candidate by mistake. This continues up to a maximum of 10 candidates. This allows the blind to vote independently protecting their voter privacy. Alternatively, as this is a long process, the voter can have a companion to cast a vote for them in the normal manner.
- Another solution is for the blind voter to record their vote on an audio device. This is then later cast as a vote in the presence of a government official. This is not private.
- The writing on the screen should be big for people with slight visual impairment.
- Avoid unnecessary information that might confuse voter. Make the information around the station and on the screen as simple and clear as possible to avoid any confusion

Education

Non-functional:

- There will be a demo or an induction system before the election to make sure that everyone will be able to use the E-voting system. This could be found online.
- The entire vote will be taken according to the National Election Author (NEA) time framework.
- During the voting process there is a persistent help button in the bottom left that the voter can click on at any point during the process to help them.
- On the partition walls there will be printed instruction on how to use the system.

Safety

Functional

- In the case of an emergency, there is a persistent X button at the top right hand corner of the screen to allow the voter to terminate their vote at any time.
- On the opening screen, it will notify the voter of the function of the X button. Once pressed it will ask the voter to confirm that they want to terminate the voting process - a question “Are you sure you want to terminate the voting process?” with 2 accompanying buttons below, confirm in green and cancel in red. If the confirm button is pressed the identification will be ejected. If decline is pressed the voter will be able to continue with the voting process.

Non-Functional

- Once the voter confirms the termination of the voting process the identification should be ejected in less than 5 seconds.

Introduction

As part of our first graded assignment we were asked to write the requirements for Ireland's national e-voting system.

We had to come up with a list of twenty "important" requirements; which had to be explained in detail under the SMART scheme. They also had to be divided into Functional and Non-Functional requirements.

Each requirement has been ranked in order of importance based of a group discussion.

System details

The E-Voting system is an electronic version of Ireland's current voting system that improves it with the use of an electronic voting booth and a server that counts votes in real times.

The system includes two servers, one for storing a database and calculating votes and another one for backing up data, a voting station in each constituency, multiple voting booths in each voting station and a numerous amount of employees for security, maintenance and form checking.

The server must be stored in a secure location. The location should have security and maintenance available at all times. Voting stations should also have security and maintenance.

First a citizen must register to vote from a Garda station. After registering the citizen will receive a confirmation of registration form. The confirmation must be shown at the voting station to receive temporary login details to access the voting station. An employee will use the confirmation to request login details from the server. This is so it's possible to check who has voted and who hasn't. The login details are assigned a random ID so it is impossible to see who has voted for a candidate keeping the votes anonymous. The citizen uses the login details to access the voting booth where the citizen is presented will all candidates from the same constituency as the voting booth. The citizen votes for the candidates in order of preference, the same as the current day ballot. The votes are submitted to the server to be counted in real time. Votes are stored in a database to ensure that each vote has an ID, making it possible to check that all votes are certified. Once the voting closes the elected candidates are retrieved from the server.

Functional vs. Non-Functional requirements

Functional requirements:

1. At the end of each round, the system must determine the winners.
2. The system must be able to count the valid votes in real time.
3. The votes must be stored anonymously by the system.
4. The system must store the data in a secure server.
5. The system must handle live corrections and cancellations.
6. The system shall have enough capacity to hold the data and manage the data quickly.
7. Every user must receive an anonymous ID (random) by the system upon presenting the registration form. To use the system, the user must be authenticated.
8. The system must be able to perform validation to ensure correctness.
9. The system must run on a dedicated machine.
10. People with impairments shall be able to use the system.

Non-Functional requirements:

1. An accurate list of the candidates for each constituency shall be stored in each voting machine.
2. The system shall have a RAID 5 configuration to prevent data loss and for backup purposes.
3. The system shall be 99.9% up and running during the elections.
4. The system's server shall be in a secure location with excellent connectivity to most of the voting stations.
5. The system shall be reliable: the data cannot be corrupted.
6. The system's server should have a database that stores all the votes.
7. The response time of the system shall be no greater than a minute from the voting action.
8. The system shall have a user-friendly Graphical User Interface (GUI) that provides confirmation message to the user before submitting their votes.
9. The system shall have a website that provides information.
10. The system shall be made maintainable by providing accurate documentation.

Requirements

This section holds a description for each requirement previously mentioned.

- **At the end of each round, the system must determine a winner**.
  The aim of the system is to produce a winner once all the votes have been calculated. The system has to compute the candidate with the most votes and return his/her name. In the rare case of a tie, the system will accept votes only from the House of Representatives, where each state delegation gets one vote.
  It also has to show a live graph of the elections containing the percentage of votes for each candidate. The graph gets updated every time a vote is recorded.

- **The system must be able to count the valid votes.**
  Only valid votes are accepted by the system. A vote is considered valid when all the fields have been properly filled. A vote must not be tampered or corrupted, if that is the case, it will be discarded.
  The votes must be checked (verified) and counted as soon as they get sent; this allows less computation time instead of counting them once the voting round finishes. Counting votes immediately is crucial as the live graph API relies on it.

- **The votes must be stored anonymously by the system.**
  The identity of a voter must always be anonymous, this prevents bribing, selling votes, and other illegal actions. In case of hacking, this also guarantees that the voter's privacy isn't violated. The vote must be kept secret at all time.

- **The system must store the data in a secure server.**
  The server must be secure as we don't want anybody to tamper with the votes, leading to an inaccurate poll and, in extreme cases, an unjust win. The access to the server must be restricted and only allowed to people with administrator rights. Every connection must have an SSL certificate. The server must be able to encrypt the data with the *Advanced Encryption Standard* (AES) algorithm. Another efficient encryption algorithm that can be used in the future is *Honey Encryption*[1].

[1] https://courses.csail.mit.edu/6.857/2015/files/tyagi-wang-wen-zuo.pdf

- **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 shall have enough capacity to hold the data and manage the data quickly.**
  The server shall be able to store 100GB of data. 50GB will be allocated to the database containing all the results. The remaining 50GB allocated hosting the OS as well as the programs required to run the system. An SSD will be used and read/write times must be a minimum of 0.5ms per 4kb read and 0.2ms per 4kb write.

- **Every user must receive an anonymous ID (random) by the system upon presenting the registration form. To use the system, the user must be authenticated.**
  At each voting station, there must at least 1 member staff per voting machine available to verify the user's registration form before allowing them to use the voting machine. The user must then receive a unique anonymous ID which will be used instead of a name when casting their vote. Each voting machine must be able to verify these IDs before allowing votes to be cast. A user without an ID will receive an error upon trying to select their candidates to vote for.

- **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.

- **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. None of the other voting booths shall be affected on the off chance one of the booths crashes.

- **People with impairments shall be able to use the system.**
  The system must be usable by the majority of users who have hearing impairments, visual impairments or are handicapped. At least one member of staff per voting station must have basic sign language, every voting station must be wheelchair accessible and the voting machine itself must have a screen reader capable of audibly guiding any user with visual impairments through the voting process. The voting process may also be completed on behalf of the user by a companion as long as the following criteria are met: the companion must be at least 16 years old, must be neither a candidate nor an agent of a candidate and may not help more than two electors at an election. A voting officer must be present and give permission before allowing a companion to vote on the behalf of the voter.

- **An accurate list of the candidates for each constituency shall be stored in each voting machine.**
  The voting unit will display only candidates that are within the voting units' constituency. The requirement is fulfilled when no other candidate from outside the constituency is shown. The voting unit will know which candidates to display based on a database which identifies the location of which the candidates are based in.

- **The system shall have a RAID 5 configuration to prevent data loss and for backup purposes.**
  The systems server will have a RAID 5 configuration with another local server to prevent data loss. Data loss can be detected by comparing the data from one server to another. Both servers will have a dedicated backup generator each, this will keep the servers running 99.9% of the time.

- **The system shall be 99.9% up and running during the elections.**
  The system should be operational for 99.9% of the time during the election. The down time of the system should be no more than an hour. The system should be constantly observed to ensure that it is still performing.

- **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 system shall be reliable: the data must not be corrupted.**
  The system should be 99.9% reliable, data corruption should be kept at a minimum of 0.01% and must be validated and checked to avoid corruption. Corrupted files should be replaced by their accurate counter-part from the backup server.

- **The system's server should have a database that stores all the votes.**
  The system shall store the votes in a database. In order to take full advantage of the fact that the system is electronic it is only logical to store the votes electronically. The easiest and most efficient solution to this problem is to implement a database which has the capacity to store the votes of all registered citizens. The database shall be kept in a secure government location and will have backups of itself in case of damage or unforeseen errors.

- **The response time of the system shall be no greater than a minute from the voting action.**
  Once a voter has chosen the candidate(s) they wish to vote for and confirmed their selection then the voting machine must send the vote, along with the randomly assigned voter ID, to the server. After arriving there it must be confirmed that there is no vote with the same ID as well as going through security checks to confirm authenticity. Finally, it is stored in the database. Given the security steps that must be taken to ensure that the vote itself has not been tampered with then this length of time is acceptable.

- **The system shall have a user-friendly Graphical User Interface (GUI) that provides confirmation message to the user before submitting their votes.**
  The GUI of the voting booth must be user-friendly, meaning that options, navigation and controls must be clear and specific. The GUI must only give relevant and detailed information to the user. The candidates should have a photo of them present next to each of their names. To minimize mistakes, the user shall be prompted with a confirmation box containing their selected candidates once they click the button to submit their vote. The confirmation should display two options, one to submit and one to cancel. The user should be notified that they have submitted their vote when they do so. The cancel button should return them back to the voting screen.

- **The system shall have a website that provides information.**
  The system should have a website with relative information for the election. This website will be primarily used by people who are in need to learn how the election is run and how to vote. The website should provide information on how to use the voting machines as well as how to register to vote. An interactive map must be shown on the website for citizens to find their local voting station. The interactive map must display the correct address of each voting station. The website should be user-friendly, displaying all sections clearly in the site navigation.

- **The system shall be made maintainable by providing accurate documentation.**
  The system must be documented with great detail to ensure staff can maintain the system. The documentation must explain how each component in the machinery works as well as how each operating system operates on the voting booths. The documentation must declare standard precedents for registration. The documentation must extend to the coding of the server and the voting booths by leaving comments in the code. Documentation must be clear on how to detect any faults in system. Documentation must give a clear walkthrough on how to install and use a voting operating system.

What is the System?

Our system has been designed to make an E-Voting system in Ireland a logical and user-friendly reality. It is based around the idea of each user having an individual account that they can log into using various methods that suit the user's individual needs. To obtain an account a user must be above the legal voting age and have applied for and collected their unique, individual voting card with subsequent voting id from their local Garda station where they will have completed either the facial recognition test or the fingerprint analysis so that they will be able to access their own personal account.

A user may then create their own personal online voting account that will allow them to vote in upcoming elections/ referendums etc. To do this they will have enter their unique voting code or scan their voting id and pass either the fingerprint analysis or facial recognition tests. They can then link their account to their email or mobile phone to get information on upcoming or past votes.

To log into their account, they must first scan their unique voting id card which was issued upon sign up and then they must pass the facial recognition task or fingerprint analysis that will be available on their own computer/smartphone/ tablet etc. We have made the presumption that all devices will have working fingerprint analysis/facial recognition technology to make this idea workable.

Each county in Ireland has a server which collects and counts the votes from that county which are then passed onto the server which represents that county's province. Each province has their own individual server which takes in each of its county's votes and passes them onto the country-wide

Requirements

Sign-Up:

1.
An initial registration into the e-voting system will be required by every citizen upon the age of 18. This is a physical registration to take place in a government building. e.g. Garda Station. A government issued ID will be required for the process. We are implementing a 2 factor security system for login.

2.
Firstly upon arrival to one of the institutes the individual must provide photo id and all basic personal info. e.g. name address occupation etc.
Once the individual has passed the first step they must then take a 3d photo of their head to be used in 3d facial recognition along with that a finger print is taken to be used for fingerprint recognition to be used alongside the facial recognition when it comes to voting day. This will insure that only the voter themselves can use their vote and prevent them from voting twice as well.

3.
Once the individual has completed these steps they will be issued with their own unique card with their own personal code attached. This will be used as the individuals voting id. This will be the initial line of security when voting followed by the second factor (facial recognition) or (finger print). Second factor is up to the voters discretion which they want to use. This is assuming in the future all computers and phones will have fingerprint and or facial recognition technology built in to make this possible.

Requirements

How to Vote:

4.
Vote on laptops or phones with the assumption that all futuristic laptops and phones have facial recognition and or fingerprint technology builtin.

5.
If the individual doesn't have the skills or equipment required to vote online or if they rather vote in person at a polling station you can vote in one of the few polling stations that will be available.
The voting process will be the exact same in these polling station but with a how to vote guide posted to help people having trouble.

6.
First step to voting is scanning the voting id you were issued when signing up.
This will then prompt you to look at the facial recognition built in into your computer or phone or place your finger on the fingerprint scanner to confirm your identity. Which method used is at the users discretion.

7.
Once the programme has confirmed your identity, the screen populates the different options to select what election you want to vote on e.g referendum or general election etc.

Each vote that an individual can vote on will also have more info about the vote that the individual is about to vote on.

8.
Once the individual is ready to make their selections checkbox selectors will be found beside each option Clicking these checkboxes will make that selection and clicking it again will deselect that option.

9.
For visually impaired individuals attaching headphones to the device they wish to vote on will prompt an audio process. In this process the options will be read aloud to the individual accompanied by a number to represent them. Once the individual has heard all options they reply with the desired number and that makes their selection.

10.
Once the individual has made their selections, final answer page will appear which displays the selections they have made and allows the customer time to view their selections and to correct any potential errors.

11.
Once the individual has confirmed their selections on the final answer page, they will be sent a confirmation email to say they have voted and also they will be notified in this email that they will not be able to vote again, if they log in again they will only see what selections they have already made.

Requirements

Security:

1. **User Account**: When a person turns 18(legal voting age) they must go to Garda Station/Public Office where they get an ID card with a unique code that only works for them. This card and code will allow said person to create an account online which allows them to vote in upcoming elections/referendums.

2. **User Authentication**: When logging into a person's account a person must enter their unique code, swipe their voting card in a card reader, scan card via a camera on the computer or using facial recognition technology a camera analyses their face and logs them into their account and they're allowed vote.

3. **Ensure 1 vote per person**: To ensure a person can only vote once there is timer once they log in giving them 10 minutes to vote and when they have submitted their vote they are not allowed return to the page. If they try to log in and vote again they are shown a message saying they have voted already and would they like to see their selection/result of the vote. This can be done using basic __ technology which stops users voting continually. If you run out of time voting you will be logged out and you will not have voted. If you now want to vote again, you must go to a physical polling station and explain why you didn't vote.

4. When you have voted you will get **text/email confirmation** of your vote detailing you on your selection and giving you a live update on how the polls are looking at the time.

Requirements

How to Count:

Multiple Servers:

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.

For example, the Cork server counts all the votes in Cork and passes it onto the Munster server which takes the votes from Cork, Limerick, Waterford etc and adds them all together before passing them on to the Country wide server which takes the counts from Munster, Ulster etc and adds them all together to get the total count.

2.

For added Security there could even be a recheck at each server stage to ensure you get the correct number of votes from each county. Each server would count the total votes it has received so far before passing them onto the next server. This would reduce errors in counting and reduce the possibility of mistakes being make. It would also allow for easier recounts and an accurate spread of the results from different areas.

3.

If crosscheck does not match, the data is recalculated at each end and then resent over the network to be checked again, if another failure is met, manual intervention takes place.

4.

If a county is particularly large e.g. Dublin there could potentially be multiple servers like Dublin North and Dublin South. This could increase productivity and create a faster, more efficient service.

5.

The majority vote wins outright (even in the case of a 51%/ 49% split).

Requirements

Data Storage:

1.
2 independently running servers shall store the vote tally in a database run by competent administrators.

2.
The time, source IP address and User ID of each vote is stored in the database table.

3.
Once the data has been confirmed as correct, hardcopies are stored for future reference using reliable and modern hard disks.

4.
Information (name, D.O.B, sex, religion, education, income bracket, address, family situation) is stored for each user along with the vote tally, this information may be used in census' following the election for statistical and analytical purposes.

Outline of E-Voting in Ireland.

The e-voting process is to be carried out on e-voting machines. E-voting machines will be placed in each constituency, the number of which to be decided by the number of people per constituency.

The e-voting machines shall be monitored by security camera to ensure against machine tampering, voting coercion, vandalism and other illegal activities that may occur. E-voting machines shall be housed in a designated polling station, for example a council building.

Every registered and eligible voter shall receive a voting slip via the postal service. This is a system that is already in place and will be extended to include a unique barcode on each voting slip to be scanned by the e-voting machine in order to gain access to the e-voting system.

A voter must use this unique barcode and their PPSN to gain access to the e-voting system thus, confirming voter identity.

Information campaigns via several media such as social media, television adverts, posters etc. shall be made of the attention of the eligible and registered voting population in order to make them aware in the period prior and coming up to the referendum or election as to how the e-voting process works.

The voter will also receive the option of watching a short tutorial following gaining access to the e-voting system, however, prior to casting their vote.

The voter will receive concise and clear instructions with each step of the e-voting process.

The voter may adapt the user interface settings to their preference.

E-voting machines will be accessible in terms of both machine and system. Disabled voters and/or voters requiring use of a wheelchair shall be able to cast their vote independently. Voters with visual and/or hearing impairments and voters with autism and/or mental disabilities should find their voting process unhindered.

The e-voting process is flexible. It may be used for referendums and/or elections.

Voters must confirm their vote at the end of the e-voting process. This will ensure each voter may cast their ballot only once. It will also declare their unique barcode used and void. The voter will receive the option of a receipt being issued. This is proof of their vote being cast. This is the end of the e-voting process.

Functional Requirements

Voter confirmation

- The system shall allow the voter to be able to confirm clearly how his/her vote is being cast.
- The voter shall be given a chance to modify his/her vote before committing it.
- Following voter confirmation, the barcode used to login to the e-voting system is declared *used* on the system. Thus, voter fraudulency is prevented.

Voter eligibility

- Voters must be authorised. If someone wants to vote, this means people must be:
    - 18 years of age or older,
    - Residents in Ireland and,
    - Registered to vote
- To ensure voters are authorised, the voter's PPSN shall be checked against a database of PPS numbers which are considered eligible.

Flexible Voting System

- The voting system must be flexible and must allow for more than one ballot question format:
    - Referendum ballots, where the voter must only select one option (e.g. Yes or No).
    - Election ballots, where the voter must select at least one option and number their options in order of preference.
    - Open-ended questions.
- The system must be aware of which format the ballot question is in and must be able to store each type correctly.

Single Vote

- When a user first begins using the e-voting system, the system must verify that they have not already voted.
    - If they have already cast a vote, the system must prevent them from continuing.
- The system must keep records of who has already voted in a poll. These records shall be centralised and accessible by all e-voting machines.
    - This ensures that individuals cannot vote multiple times by going to different polling stations.
- If a machine cannot access these records, it shall not accept further votes and shall display an Out-of-Order message to users until a connection is re-established.

Voter Identity

Proof of the voter's identity must be provided by the voter to protect their vote and ensure it is not used by someone else.

- The voter shall be provided with a voting slip via post, a system that is already in place. However, the slip now has a barcode that paired with the voter's PPS number can be successfully used to vote once.
- The PPSN will verify the voter's identity and the unique barcode will ensure against *vote-coercion and vote-selling*.
- The voter must scan the barcode and input their PPS number separately into the e-voting system.
- The PPSN and the barcode will be verified by the e-voting system. This will ensure voter identity security.

Anonymity

- Records of votes must contain no information that could identify the voter.
- Although records are also kept of who has voted, there shall be nothing that connects these records to each other.
    - Therefore, machine serial number and timestamp must not be kept in these records so that connections can't be inferred based on the machine and time of vote.

Power Efficiency/Cost Effectiveness

- The machine should have minimal energy requirements, and should be able to operate on battery power if necessary.
- If the machine entirely runs out of power, it should maintain a persistent snapshot of its state which can be retrieved when powered up again.
- The machines should be *cost-effective*, costing less than to employ someone to count the votes over five voting cycles.

Memory Capabilities

- The machine should use a memory medium that is cheap and widely available, and that can persist without power.
- The memory should be large enough to hold both the record of activity and vote count.
- The memory for vote counts and records should be kept separately from the memory which holds the machines software and configuration, and it should be removable.
- All information stored on the memory should be encrypted by both the machine itself and the centralised server.

Non-Functional Requirements

System Accessibility

The software must meet the needs of the user in terms of accessibility without compromising confidentiality of their vote.

- The system shall provide an interface that caters for all physically-challenged voters.
- For visually impaired or blind users, the system shall provide an auditory mode using text-to-speech.
- The displayed content shall be adaptable i.e. text enlargement and specific colours used for colour blind voters.
- Screen brightness should be adjustable so it does not cause difficulty to users with autism and/or epilepsy.
- The system shall also provide textual content in both Irish and English.

Machine Accessibility

The process of voting shall be as easy as possible for all users. Each polling station shall provide specialised equipment for disabled users.

- For visually impaired voters, a braille keyboard and touch pad shall be provided, along with other braille input/output devices.
- There shall be voting kiosks at an accessible height to make voting easier for wheelchair users in every polling station.
- The disabled voter shall be able to cast their vote independently.

Failure Handling

- In the event of an error on an e-voting machine:
    - It shall not be recorded that the user has cast a vote.
    - The user shall be notified that their vote has not been counted and shall not be allowed continue the voting process at this machine.
    - The polling station shall be notified that a problem has occurred with the machine.

Tutorial/Demonstration of Use

- There must be a tutorial available to voters on how to use the system. Instructions on how to use the e-voting machine should be available at each polling station.
- Each e-voting machine should also have the option to play a video tutorial of using the system. An audio version of this must be available for visually-impaired voters. The tutorial shall include the following steps:
    - Identification,

    - Selecting and deselecting options (in the case of both elections and referendums),
    - Confirming or cancelling/discarding your vote.

Order of Display

- To take advantage of the digital medium, the system shall display voting options/candidates in a randomised order for each voter.
    - This dispels worries in elections/referendums that the order of options influences voter decisions.
- In the preparation for a vote, an option shall be available to authorities to record the frequency each ordering was displayed.
    - These records shall contain no information of what option(s) were selected and shall only serve to prove that no ordering was displayed significantly more/less frequently than the others.

Closed System

- The system should operate on a proprietary, closed network, not linked to the internet.
- There should be no ports or any other facility for physical access to the hardware other than the connection to this network.
- The machine itself is to be enclosed in such a way as to make it difficult to access any of its components.

Robustness

- The machine should handle most failures by taking a snapshot of its state and ceasing operation: *we prefer ensuring correctness over maintaining minimal functionality*.
- However, the machine should stand up to significant physical wear and damage.
- The machine, under normal conditions, and should be able to last 20 years without replacement.
- Since bugs in the software of the machine could represent tampering, the machine should make minimal efforts to recover from such failures.

Auditable

- The system should maintain a record of its activity, to allow for auditing after votes.
- The record should consist of both snapshots of state and a of log actions.

    - This data should be anonymised sufficiently to prevent identification of voters, but should be detailed enough to rigorously analyse with the intention of detecting tampering.
    - Each entry in the record should be cryptographically secured by both the client voting machine and the centralised server, and tagged with the time.

User Interface

- The system shall provide an easy-to-use user-interface.
- The system shall not disadvantage any candidate while displaying the choices for example, by requiring the user to scroll down to see the last few choices.
- The system shall be accessible for all users. Therefore, the system shall account for blind voters, users that require wheelchair access etc.

Transparency

- Voters should be able to possess a general knowledge and understanding of the voting process.
- Voters should receive instruction prior to using the e-voting system of the requirements and steps of the e-voting process.
- The system should provide simple, concise instructions for each step of the e-voting process.
    - The voter should know with 100% certainty what has been achieved with each step of the e-voting process.

Distribution of Authority

The administrative authority will be distributed among more than one entity for the purpose of:

1. Security Reasons
    - No single entity should know or control the entirety of the e-voting system.
2. To Avoid Collusion
    - Authority should be distributed amongst multiple administrators who are known not to collude among themselves e.g. among different political parties.

Convenience to User

- The system shall allow the voters to cast their votes quickly, in one session.
- The system should not require any special skills or intimidate the voter ensuring equal access to all voters.
- The voter should not be restricted to cast his/her ballot at a single-poll site in their home constituency.
    - Therefore, the voter shall be able to cast their ballot from any poll-site within the nation.

Receipt of Vote

- The system offers the option to issue a receipt to the voter following voter confirmation.
- This receipt may be used for the voter's own records.
- This receipt can be used to ensure that *vote-coercion and vote-selling are prevented*, so that the voter can verify their vote at any time and also contend, if necessary.

System Components

Abstract:

e-Voting describes a concept whereby individuals can cast a vote electronically. In the system proposed here, e-Voting may be conducted remotely, or at an electronic polling station. This model can reduce government expenditure on maintaining a large number of venues (e.g schools) as polling stations, and encourage a greater percentage of the population to vote.

Components:

Remote e-Voting:

- By utilising the widespread access to internet devices, this e-voting system will allow votes to be cast without individuals being physically present at a polling station.
- Individuals open a facility on their device and cast their vote.

Electronic Ballot at Physical Polling Stations:

- Physical polling stations in this proposed will be designed similarly to traditional polling stations but will use an electronic ballot to be filled in by voters.
- Due to the availability of remote e-voting, there will not be as many physical polling stations as there is at present.

Requirements

---

1. Identification (Functional)

Specific- Every individual person will have personal information as a unique identifier to be able to vote.
Measureable- All identification will be stored by the e-voting system on a secure database.
Attainable- Every individual person have personal information that is unique to them.
Realistic- The e-voting system shall store all personal information relevant to the individual.
Traceable- All personal information is easily traced back to or held on from the individual.

2. Authentication (Functional)

Specific- Every individual shall be checked to ensure voting eligibility before voting.
Measureable- Individuals shall take no longer than 10 seconds to be authenticated to enable voting if eligible.
Attainable- All individuals shall be authenticated before they can vote when using the web application for voting online.
Realistic- Software holds authentication means for all voting individuals and physical-ware in which all individuals are authenticated by the personnel to ensure voting eligibility.
Traceable- All software enabling voting will contain an authentication means for all individuals who wish to vote online.

3. Anonymity (Functional)

Specific- Every individual shall contain an anonymous state during the voting process.
Measureable- No personal information shall be disclosed during the voting process regarding any individual who is voting on the web application.
Attainable- Personal information from the individual voting will not be provided during the process.
Realistic- It shall not be required by the individual to present personal information during the voting process.
Traceable- Individual shall be anonymous from beginning of voting process till the end of selection.

4. Encryption (Functional)

Specific- No one should be able to determine how any individual voted.
Measureable- Every individual's vote shall be encrypted before and after when they vote during the voting process.
Attainable- Once the individual is in the voting process, the vote casted shall be encrypted.
Realistic- No personal information is provided and only the vote casted is encrypted to ensure no back traceability.
Traceable- All individuals are sessioned to ensure encryption when casting the vote.

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.

6. Eligibility (Functional)

Specific- Ensure every individual is eligible to cast a vote.
Measureable- Every individual, when using the web application, will be informed if they are eligible for voting.
Attainable- Once the user tries to login for vote casting, they will be informed by the registry of electors if they are eligible for voting.
Realistic- All individuals who wish to cast a vote on the web application will be processed to check if they are eligible for voting.
Traceable- All individuals personal information is stored securely by the register of electors to ensure eligibility for vote casting.

7. Distributed(Multiple Servers) (Non-Functional)

The E-voting system shall use a total of 640 distributed servers which is broken up into 20 dedicated servers in each of the 32 counties in order to make the system 99.9% reliable and 99.9% available at any given time.

Specific- There shall be 20 dedicated servers located in each of the 32 counties to support the population of Ireland.
Measureable- The servers will handle all requests in no longer than 5 seconds.
Attainable- Servers should be 99.9% reliable and 99.9% available to use at any given time.
Realistic- The servers will store all votes casted and handle requests.
Traceable- Required by the E-voting system.

8. Robust (Non-Functional)

The E-voting system will be able to handle the population of Ireland without delays of more than 5 seconds when votes are being submitted. This system will be able to handle any errors or crashes and will deal with them accordingly.

Specific- The E-voting system shall handle the population of Ireland over the age of 18.
Measureable- System will not delay for more than 5s when votes are being submitted and votes will be secured immediately.
Attainable- The system shall be 99.9% available and 99.9% reliable.
Realistic- The system will securely store all votes casted by the people of Ireland.
Traceable- Required by the people of Ireland in order to vote efficiently.

9.Accuracy (Functional)

The E-voting system shall record and count all votes accurately.

Specific- The system will store and count all votes casted by the people of Ireland.
Measureable- All votes submitted on the E-voting system will be stored in a secure server.
Attainable- Every user of the E-voting system has the option to vote.
Realistic- All votes will be correctly stored and accurately counted.
Traceable- Required by voters to ensure votes is successfully submitted and counted to accurately represent results.

10. Vote Control (Functional)

The system will not allow for more than one vote to be submitted by an individual.

Specific- Every user shall not be able to vote more than once to avoid a bias result.
Measureable- Users can be checked to see if a vote has already been submitted.
Attainable- Every user's account determines if they have voted or not. Determining their ability to vote.
Realistic- Determining if a user has submitted a vote can be performed without compromise of Security and Anonymity.
Traceable- Required by E-voting system to ensure accuracy of results submitted by users.

11. Time Control (Functional)

The system will accurately be available to use by voters between 07:00 and 22:00 on any specified day.

Specific- The E-voting system will have an exact time period for operation. This time window will open at 07:00 and close at 22:00 giving exactly 15 hours for users to submit their votes.
Measureable- The system shall be active between 07:00 and 22:00 in which votes can be submitted strictly in this time period.
Attainable- E-voting system will open at 07:00 and close at 22:00 using Greenwich Mean Time(GMT) in winter and Irish Standard Time(IST) in summer.
Realistic- Voters will have a time frame of 15 hours to submit their votes.
Traceable- Software for the e-voting system will contain accurate timings for its time period which are local to its users.

12. Results (Functional)

The E-voting system shall provide an overall result when voting has ended. These results are distributed and displayed accordingly.

Specific- The system shall provide an accurate account of all votes casted onto a detailed graph.
Measurable- The result of all votes submitted by users can be viewed.
Attainable- Votes submitted by users will update the system count which can then be displayed.
Realistic- Votes submitted will be displayed when the voting time period is up.
Traceable- Required by everyone to receive an accurate representation of the overall result.

13. Backup (Functional)

The E-voting system shall backup all votes submitted by voters to maintain accuracy and reliability in the occurrence of any errors or crashes. ie. Server crashes, loss of internet connection.

Specific- A backup of all votes will be stored securely in order to avoid data loss.
Measureable- All votes casted by users in the E-voting system will be copied and archived.
Attainable- Data originally stored on the distributed server will also store a copy.
Realistic- Information is stored and copied amongst distributed servers to achieve accurate results and avoid data loss.
Traceable- Information lost can be traced back and replaced with its copy to contain its initial data.

14. Interoperability (Non-Functional)

E-Voting Application shall be able to run on all modern devices that can run a web browser from 2013 to date of election. Example Set: iOS, Android, Linux, Windows, Firefox, Chrome, etc. The interface shall be constant on all devices including physical stations.

15. Performance (Non-Functional)

The E-Voting Application shall load in no longer than 5 seconds at peak usage time. ie. On the day the voting takes place between the hours, 07:00 - 22:00.

16. Modifiable (Non-Functional)

The application will have an easily modifiable interface that can be used for several types of votes. ie. General Elections, Referendums, etc. The interface should have sections such as candidates names, parties, users vote, etc.

17. Simple User Interface (Non-Functional)

The user interface should be simple and intuitive for users from all walks of life. Based on the standards of websites that have the highest usage rates. ie. Google, Youtube, Facebook, etc.

18. Multi Language (Functional)

The web application shall support multiple languages through a simple drop down menu, the languages included should be the first languages of all registered voters.

19. Accessibility (Functional)

The web application will have support for people with impairments such as hearing and visual impairments. This support will include speech recognition and audio instead of text options, etc.

20. Vote Verification (Functional)

The user will have a confirmation screen showing the user’s chosen votes, that loads no longer than 10 seconds after vote submission. This way no confusion should arise as to whether the correct vote has been registered or not.

System description

The main components of the voting system are physical voting machine and the main server containing all voting data. Voting machines are connected to the server using satellite connection.

Voting machine

Each voting machine is comprised of the custom computer (CPU, RAM, hard drive, motherboard, networking module), touchscreen, physical input buttons, smart ID card reader and biometric sensors. All the components are protected by a sealed steel case.

Server

Server will be located at a secure site and will have enough storage and processing capacity to handle the voting process. The data stored on the server will be list of eligible voters, biometric data for voter authentication, actual votes etc.

Voting process

Before voting, each user will have to authenticate with the combination of smart ID card and biometric authentication(fingerprint or facial recognition). After successful authentication the user can vote using the touchscreen or physical buttons. The vote is anonymized and sent to the server over the satellite connection.

Functional requirements :

After a successful authentication, the machine shall check if the user is eligible to vote.

Voting machine must have a facial recognition system that is capable of correctly identifying the person with 99.99% accuracy in less than 3 seconds.

Voting machine must have a fingerprint sensor that is capable of correctly identifying the person with 99.99% accuracy in less than 2 seconds.

Voter must be able to choose between available biometric sensors(facial recognition and fingerprint) when authenticating.

Voting machine must have a networking module that enables direct connection to the server via satellite. The connection with the satellite must be at least 99% reliable in every geographical position and weather condition.

The machine shall check if the user currently voting has any proxy vote linked to his profile.

The text font and the button size must be resizable with the usage of 2 physicals buttons (+) and (-) for visually impaired people.

Every time a person votes, as soon as the vote is confirmed the information is sent in realtime to the server storing all the votes.

To protect the anonymity of the vote, it will not be linked to the person who voted.

In order to be usable by visually impaired people, the machine must have headphone and buttons with braille. The different screens will be able to be read the informations to these people and they will be able to interact with them.

At the beginning of the voting process, each person will have to choose which language they want to use (English or Gaelic)

Before finalizing the vote, a confirmation message will be displayed to the person to close his vote.

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.

Non-Functional requirements :

Voting machine must have a card reader that is capable of reading data from smart identification card in less than 100ms at the distance of 5cm. The dimensions of the card reader must be 10cm by 10cm.

Voting machine must have a 13” capacitive LCD touchscreen with the resolution of 1920 by 1080 pixels.

A list of all the eligible users for voting has to be stored in an online database.

The user interface needs to have a high color contrast in order to have the information stand out and be easily readable by anybody, including colorblinds.

The voting process should not be take more than 5 steps for the user, from the authentication to the voting confirmation screen.

The machine should be physically protected with sealed steel case. No external inputs should be accessible, no USB port available for instance.

All information exchanged between the machine and the various external databases will have to be encrypted in order to protect it and to preserve the anonymity of the votes.

All data on the hard drive must be encrypted using the AES algorithm with 256 bit key size.

In the event that the touch screen is not responsive, the machine must be fully operable using only the touchpad and keyboard of the machine.

Any eligible voter must be able to cast his vote anywhere in the country or in any of the Irish embassies around the world.

In case of a connection drop to the internet, the access to the machine must be locked until the connection comes back.

Requirements

1. **The PPS Number shall be used as a form of user authentication.**
   The Electronic Voting system should rely on an automated system of confirmation and authentication, rather than human ability. Identification codes, unique to every registered voter, should be able to be scanned by a machine and confirmed as a voter. Registered users will use their Personal Public Service Number as a Unique ID that grants them access to vote. The Personal Public Service Number, which will be referred to as the PPS Number for the requirement, is already a unique identifier used by the Irish Government for certain services and avoids the creation of a unique ID. The PPS Number usually remains the same throughout a person's life, meaning the same ID shall be used at each election. Although there may be security concerns, the PPS Number consists of 7 random numbers and 1 or 2 letters, with no direct way of decrypting a PPS Number to a certain voter without access by a government agency. The PPS Number is already used on Medical Cards, Public Services Cards, Social Services Card and various other documents. Children born in Ireland are registered with a PPS Number at birth, ensuring that our unique ID system will still be relevant in future generations. Immigrants living in Ireland as citizens can also apply for PPS Numbers, in much the same way they can register to vote in the traditional system. Laser Scanners will be used to retrieve the PPS Number from the correct form of ID, including Medical Card, Public Services Card, however the ability for physical input on a number pad will be accepted. The PPS Number can recall details about the voter, including their age. Automatic registration to all citizens over the age of 18 could therefore be achieved. This will boost the participation of younger voters in elections and streamline the service for the elderly who may be illiterate in the paperwork required. Irish citizens living abroad may also apply for a PPS Number, and should voting abroad become law in the 2018 referendum, then they shall have access to a unique number that grants them the right to vote.

2. Votes will remain anonymous throughout the entire process.
The Irish Constitution declares votes for the Dáil and for the President are both to be done by secret ballot. Electronic Voting is legally required to ensure the anonymity of the voters. As a result, there will be no indication by viewing the voting data, who voted for what. The databases of who voted and the votes themselves will be entirely separate. Timestamps could be used to merge the two forms of data together to create a near-accurate representation of voter alignments, so the Voting data will be randomly arranged to ensure no recreation can take place. The PPS Numbers are to be treated as confidential information and will be only used to retrieve statistical data about the election. These statistics are under the responsibility of the Electoral Commission to protect the privacy of the voters from third party organisations. E-Voting shall still take place behind a curtain or closed door in a very similar fashion to traditional voting. This will protect a Voters choice during the voting process. Any Voters with disabilities or those who use Text-To-Speech must be an appropriate distance from a queue of voters to prevent them overhearing. The authentication data (PPS Number and Biometric) shall only be stored on the machine until the vote is submitted and confirmed. The Client will then be updated in the Government Database to confirm that they have voted. Once the update is successful, the local

data is cleared from the machine and is irrecoverable. Should the need arise for a technician or engineer to review the machine, either the voter may have the option in the interface to ‘cancel’ their vote, or if an attempt to vote was unsuccessful due to connection problems, the machine should automatically clear itself of any of the voter data.

3.Measures will be taken to prevent any malicious disturbance to either the hardware or software.

The Electronic Voting machine itself should be presented as a ‘black box’ to any voter – in which that outside of the tools used for user input and Display/Audio, there should be no visible hardware that the user could hamper with. The inner hardware of the machine must be blocked from interference, either by encasing it securely so that it cannot be accessed without specific keys and experience, or by making the hardware hidden completely in a secure location, and streaming the data to a screen in another room where users can vote. Either way, to access the hardware of the E-voting machine, one would require both physical keys and software passwords to gain access. A use of both technical and physical security can provide high levels of security. The UI should have appropriate handlers for error crashing, and won't display any Operating System information, database information or any program code. 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. For when the technicians themselves will be voting on the machine, it is important that they themselves can’t cause any disturbance while being users of the machine. Heavy amounts of quality control and testing will be undertaken before any E-voting is used in official elections.

4. A secure connection must be maintained between the Voting Machines and the Secure Database.

For obvious reasons, it is important that the connection between the machines and the database is reliable from any obstruction and cannot be retrieved or manipulated by a third party. All data must be encrypted on the voting machine before being sent by the connection. HTTPS or a similar protocol must be used to guarantee a secure connection that can protect the voter’s data. To prevent unnecessary bandwidth usage, the data used by the interface allowing users to vote (Pictures of the candidates, the options in Audio, different languages etc.) will be locally stored on the machines. Verifications can be done with regular checksums should the voting machine need to retrieve the voting 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. This will limit delays as much as possible, as well as promote much needed Fibre Optic infrastructure to the country. TCP connections will be used as the transport layer protocol for the voting data. TCP is suited for applications that require high reliability, and flow control and error recovery prevents the loss of any votes due to connection difficulties that could arise due to bad weather, remote location or congestion on the network. In the case that there are serious

congestion problems or should a connection abruptly end, it is important that the voter information is not lost completely. As such, the voter will be not be instructed to leave and instead be told to wait until the upload is complete. If the delays take so long that the connection drops, the voter data will be cleared from the system and an engineer will be alerted to the issue, in which case the voter may be instructed to re-enter their vote, or be escorted to a working machine.

5. A Biometric authentication is installed with each Voting machine to prevent voter fraud.

The PPS Number serves as a way of ensuring there are unique voters and no one can vote twice, however voters could manipulate or coerce the PPS Number from unsuspecting victims. A Flaw of the PPS System is verifying that the PPS Number is bound to a certain user (E.G a 26-year-old man may have stolen a 76-year-old female's Medical Card and retrieved her PPS Number). Therefore, a biometric authentication which is bound to a user's data and PPS Number will reduce the possibilities available for criminals to attempt voter fraud. Fingerprint recognition is the most common of biometrics, especially regarding biometric authentication on computerized systems. Fingerprint recognition is common in many secure facilities, and many voters are already familiar with the practise. Its popularity will make the acquisition of the fingerprints more attainable and their use better accepted when compared to other biometrics. 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. Investments such as these will prepare the E-voting system for the long-term future without worries of their system becoming outdated or obscure. Alternative forms of authentication in the case where a fingerprint cannot be provided (due to injury or medical condition) will be provided. However, the alternative method of authentication will be covered by the appropriate authorities, and you may not enter a public E-voting system should you not be able to provide your biometric without government documentation., 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.

6. System for Single Transferable Voting for Dáil

A system will be set up to provide a the ability to be utilised in the election of Teachta Dáil in a single transferable electoral system.

In the initial boot up of the machine it will display the option to select between the type of system being used. After selection the STV option an administrator will be asked to insert the candidates for the specified constituency. This person or people who will be inserting the

candidates into these lists will have to be vetted. The candidates themselves should be allowed to inspect this process.
In the voting process itself with use of the user interface, the candidates will be ranked. 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.

At the Central database the anonymous votes will be stored until after the voting ends. After polling closes the central database will calculate the ranked votes and distribute them to the respective candidates in the constituency with equal representation to the candidates, splitting secondary votes fairly. The actual transfer process will have to be reported to the administrator who can provide it to the media and public.

7. System for Instant Runoff Voting for President
A system will be set up to provide a the ability to be utilised in the election of the president in a instant runoff vote, simpler version of STV.
In the initial boot up of the machine it will display the option to select between the type of system being used. After selection the IRV option an administrator will be asked to insert the candidates for the race. This person or people who will be inserting the candidates into these lists will have to be vetted. The candidates themselves should be allowed to inspect this process.
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.

At the Central database the anonymous votes will be stored until after the voting ends. After polling closes the central database will calculate the ranked votes and eliminate the candidate with the lowest vote from each list if highest priority . The actual transfer process will have to be reported to the administrator who can provide it to the media and public.

8. System ensuring one person, one vote verification.

After a voter has selected the ranking of their preferred candidates and confirmed their vote, it is created as a priority list. The priority list linked to this constituency and local area and random id is immediately sent to a central database. The amount of data sent by the machine to the central database will be limited in size for a specific amount of time.
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). The vote will be processed/calculated only after polling closes.
This flag or notification will be sent to the biometric 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.
If the cases occurs where a voter tries to vote again the local registration and confirmation system will simply notify the person seeking to re vote and log it to be used in a review of the security and effect on the actions of voters in a e-voting system.

9. Voter registration

The process for voting is reliant on a biometric database and PPS number. When the voter enter a polling station they will need to confirm their identity. Each unique PPS number is linked to the voters biometric record. The voter will be asked to know or have their PPS number before being brought before a fingerprint scanner. The scanner will ask for their PPS number and fingerprint to identify that the scan matches with records. If successful a unique pin or code will be provided for the voter to use at a voting booth, a flag will be attached to a new anonymous record created for this individual. If unsuccessful the voter will be notified to ask a technician for help and logged for further review of the e-voting system.

In a successful confirmation of voters identity the voter will go to the voting booth or not in either case where the voter hasn't confirmed their vote the system will timeout after a specific time and the voter if they try to use the same code will be asked to confirm their identity at the biometric scanner. This will also be logged for further review of the e-voting system. In reconfirmation the voter will with their details reconfirm their identity to match the anonymous record, a new flag will indicate the voter has tried again to vote, this will be logged.

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.
A commission has stated that a dedicated line will be created to make sure their can be a minimum level of interference from outside sources and other traffic on the line. 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.

11. Services in various languages.

To help the voters and to ease their voting process various languages will be at offer from which the voter can choose a language which they are most comfortable in. The services will be offered in 5 languages as follows, English, Irish, French, German and Polish. Information such as flyers, instructions and the voting machines will all be available to these languages. As well as that a short 10 second demonstration video will be shown in all these languages played one after the other to help the voters in what to expect and how to go about casting their vote. The user will be required to select the language they would like to use once they arrive at the voting machine. A translator from each of these languages will be required to translate the content needed for the voting system from English to the additional languages. It will be then be distributed to all polling stations and fed into all the voting machines.

12. Scanner must be directly connected to voting machine, otherwise voting machine can’t tell who voted.

A scanner will be directly connected to the voting machines to ensure a legitimate voter can vote. The scanner will take the voters fingerprint to check for correct voter. If the voter is legitimate it will log the voter in the machine. Then the voter can vote thereafter. The fingerprint will act as a login credentials. A scanner will be connected to each voting machine. Every time a person logs in to the voting machine they will automatically be ticked of as voted. The scanner will only read either the voters left thumb or the right index finger. A standard 500 dpi+ scanner will be used as this is the dpi used by law enforcements to scan. This will clearly differentiate fingerprints that may not be able to differentiate using lower dpi. The scanner will only be

activated before a voter logs in and after a voter has logged out. So it can be ready for the next voter to be scanned.

13 . Confirmation and ability to undo before voting.

On our voting machine we will have a confirm button. Once a voter has made their preferred selection of candidates they will need to confirm. The confirm button will serve the purpose of confirming the voters vote and casting it. In addition to that an amend button will also be located on the voting machine once the selection is made. This button will serve the purpose to amend the voters selection before confirming. The amend button will allow the voter to re-select their preferred candidates before they confirm their selection. After re selecting their choices by the amend button they will be shown the confirm button again, which they will need to confirm. However once they confirm they will not be able to amend their choice as it will be voted, once the confirm button is pressed. After confirmation the voter would be logged out of the voting machine and vote would be casted.

14. Device must be sturdy, protected glass, make it difficult to break.

The voting machine will be fitted within a wall. Where the user can only see the screen, scanner and the buttons associated with the machine. 4 buttons will be located on each side of the screen. All the connections to the machine such as power cable, Ethernet cable disk drives and etc will be located behind the wall where the voter cannot be entered. Only the technician and engineers will be allowed access to the voting machine behind the wall. A protective glass will be attached to the machines screen to make the screen protectable from any damage that may be caused. Hence making the voting machine more sturdy and difficult to break. The fitting will somewhat be similar to the fitting of ATM machines on the street. This will make sure the voting machine stays safe throughout the elections and into the future elections.

15. Easy to Understand System, simple UI

On our voting machine we have a straightforward interface for the users. The users will be available to see a demonstration video either on the elections website or at the polling stations. At first a simple screen is shown where it asks the voter to select a language of their choice and then to scan their fingerprint. Once that is done it will show the user the list of candidates who are competing alongside their respective picture. This will give a clear view to the user who they wish to vote. All the candidates will be shown on the same screen. The font will be of Times new roman and size 14. So it can be clearly read by the user. The interface will be similar to and along the lines to the interface used in the ATMs. A simple dark blue colour will used

as the background and the writing will be in white. In this way it will stand out more to the user and the reading will become a bit easier to read. Likewise the pictures will be of good quality so each candidate will be identified clearly. In this case we will limit the confusion that may be caused between candidates.

16. Accessibility

The voting system must be accessible to any Irish citizens with physical or mental disabilities. All guidelines for disability compliance are set by the National Disability Authority of Ireland. A voting terminal would be categorized under the NDA's requirements for public access terminals, which includes both Priority 1 and Priority 2. Priority 1 requirements are to ensure that people with impaired vision, mobility hearing, and cognition are able to use the terminals. Some examples of this include ensuring that the UI is reachable and in sight by people of all heights, building booths with adequate space for wheelchairs, and designing the UI in a way that allows users with restricted or no vision to operate it. To accommodate the visually impaired, all booths will be outfitted with headphone jacks with audio prompts, and braille buttons to operate the machine. The screen itself should be resistive, so that it may be operated without necessarily having a body part come into contact with it, and have a frequency that will not pose a problem to users with epilepsy. In order to enable access by users of much more dramatic disabilities, it may be necessary to create multiple types of booths with different amounts of space, supports, and screen heights. Also under Priority 1 is language understanding. The booths should be programmed to operate with as many different languages as seen reasonable. This is to ensure that all voters can operate the machines without any concern of misunderstanding. Priority 2 requirements will make the terminals more accessible to users with mental and cognitive impairments. The system should allow sufficient time for slow users, and provide a way to cancel at any time during the voting session before their vote has been submitted. Also, there should be no dramatic differences between the user interfaces from one terminal to another.

17. Front-End Hardware

The voting terminals can be thought of to be very similar in operation to an ATM. The primary point of operation should be a resistive touch screen, with minimal ficker. As mentioned earlier, the terminals should feature an array of buttons that also allow total operation. The user will also have access to the fingerprint reader, as well as a pin pad to enter a PPS number. A device for scanning an official document such as an ID or passport may also be included, but this is not necessary for the given security requirements. Because some users may need assistance using the terminal, there should also be a button to call an attendant. It is critical that the terminals themselves feature absolutely no speakers of any kind, to ensure complete confidentiality. For users with disabilities, there should be a clearly marked and well-located headphone jack where

the voter may plug in a pair of headphones to receive voice prompts. As an added protection and convenience, headphones should be provided by attendants at the voting locations.

18. System Hardware and Data Transfer

The biggest complication with E-Voting is that new problems are introduced that did not exist with physical voting. One of these problems is insurance of the valuable vote counts. 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. It must be clarified however, that these drives are solely for the operation of the systems, and must not be able to store any information from individual voting sessions, other than general usage statistics. 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. Aside from this, there should be multiple central servers that manage the individual voting stations. If there are any major discrepancies between the counts from either server, it will be easier to track down the problem. Lastly, each booth should have some form of a UPS to protect against power outages and surges.

19. Booth Design

While the electronics of the voting stations are the main focus, the physical design of the booths is critical in order to make the new voting system reasonable. First, all booths need to be to some degree collapsible. The actual electronics system should be as compact as possible so that it does not take up a high volume of space, and the booths themselves should have the ability to be easily assembled. The compactness in necessary in order to allow the voting stations to be transported easily and safely in high volume. A design like this will make it easier to control the layout of the booths, so that different booth styles can be available for accessibility, without the need to build various types of terminals. The booths should allow the voter to vote in complete privacy, and also have enough space for a chair, as not all voters vote quickly or are able to stand for extended periods of time. There should also be no way for unauthorised personnel to access any of the ports on the machine at any time.

20. Polling Locations

Some of the biggest factors necessary to making E-Voting work occur outside the units themselves. A big concern that arises with E-Voting is that every poll location, regardless of the voting system, will always need staff members to keep the process running smoothly. However, unlike typical polling locations, the ones utilized with the E-Voting system will require people with much higher qualifications. Before, poll operators could be average people who volunteer,

but these poll operators would need to be well-trained enough to troubleshoot any technological issues that may occur throughout the voting process. Depending on the problem that arises, it may be necessary to have staff members with full IT training in order to deal with issues quickly. The second biggest concern is connectivity. Because voting would now be sent over a secure web connection, many locations that were once used would now be ineligible. Polling locations would need to be properly checked ahead of time, and retrofitted if necessary to allow very large amounts of data to be sent to the central server.

System Specification

Task Description: Gather requirements for a national e-voting system for Ireland.

System Scope: This combined hardware and software system is an e-voting system for the Republic of Ireland. The main requirement of the system is to allow voters to cast their votes electronically without the need to fill out physical ballots in a predetermined location as is the case currently. The system will facilitate both types of voting currently in used in Ireland, being Proportional Representation(PR) and First Past The Post(FPTP). Due to its electronic nature the system will allow users to vote within a wider time frame than previously, say seven days. The system will also allow for unlimited change of mind up until the voting deadline. Users will be able to vote in three different manners, depending on the election/vote in progress. Be it a national election which is PR, a European election which is FPTP with multiple candidates or a referendum which is a simple yes/no FPTP vote.

System Reasoning/Description: Security and validity of a vote cast are of the utmost importance in an e-voting system. Therefore, the conventional e-voting systems of today that use a web based application with encrypted keys for individual voters is not nearly secure enough. After researching all potential web based systems, we have concluded that to be truly secure the system must utilize bio-passwords (being fingerprint or retina scan). That being the case, we have decided a government issued smart device is most secure route to follow. Each device will have bio-password reading capabilities. This will ensure that only the voter registered to that device can access the system and cast a vote, ensuring the integrity of the election/vote. The device will accommodate each type of voting currently practiced in Ireland. The use of an open web based system for the devices to connect to raises many security issues. Because of this the Irish Government will have to launch a number of satellites to provide a country wide closed WIFI system for the devices to access. In this way the actual system will be protected from outside attack or interference. Several fixed place voting locations will need to be maintained in each county depending on county size. These locations will contain voting machines modelled after the smart devices. In case of voters losing the devices or not signing up to the program. This will be necessary to accommodate older voters and to keep public backlash to a minimum.

Functional Requirements

1. All votes will be cast from government issued voting devices and from polling stations found in towns and cities.
    a. To ensure security and anonymity, every citizen eligible to vote will be issued a voting device by the government on which to cast his/her vote.
    b. In each town and city, a polling station will also be setup to accommodate those who have lost their government issued voting device, don't know how to operate them or simply wish to cast their vote the "old fashioned" way.

2. The system will use government issued voter registration numbers and user bio-passwords (i.e. fingerprints) for authentication.
    a. To ensure that each voter only casts his/her vote once and that no voter's vote is cast by another individual, the government will issue a voter registration number to each citizen eligible to vote, which will be a unique number linked to that person's bio-password (i.e. fingerprint). The individual will only be able to cast his/her vote once he/she has supplied both the government issued voter registration number and his/her bio-password.

3. The system will facilitate Proportional Representation (PR) voting.
    a. PR is used for national elections. As such, the system needs to support that type of voting system.
    b. PR requires that if x% of the voting body voted for a specific party, then roughly x% of the seats must be occupied by that party. Therefore, the system will keep track of the number of seats available in government and the percentage of the voting body that voted for each party. The system will also be able to perform basic arithmetic's to determine the number of seats that each of the parties are assigned.
    c. PR uses transfer votes, whereby if a voter's primary candidate doesn't win, his/her secondary candidate gets his/her vote instead, etc. Therefore, the system will keep track of each voter's primary, secondary, etc. up to denary options. The system will also be able to reallocate votes as necessary.

4. The system will facilitate First Past The Post (FPTP) voting.
    a. FPTP is used for referendums. Furthermore, as Ireland is part of the EU, it participates in European elections, which also use FPTP. As such, the system needs to support that type of voting.
    b. FPTP requires the party/politician or option that reached the highest number of votes to be the winner. Therefore, the system will keep track of the number of votes each party/politician or option received. The system will also be able to perform basic comparison to determine the winner.

5. The system will use two separate GUIs to easily accommodate both PR voting and FPTP voting.
    a. PR requires 1 or more than 1 (up to 10) options to be chosen. Therefore, the system will allow the user to select 1 to 10 (or the number of options, if the number of options is less than 10) candidates and put them in order, with the first candidate being his/her primary option, etc.
    b. FPTP requires exactly one party/politician or option to be chosen. Therefore, the system will allow the user to select 1 party/politician or option.

6. A bio-password will link a voter to a constituency, depending on type of the election.
    a. A bio-password will need to link a voter to a particular constituency in the case of national or European election so the user is linked to the correct choices.
    b. In referendums this functionality will not be necessary as constituency does not make a difference to the substance of the vote, however the information may still be useful for statistical analysis.

7. The correct politicians (including names and party affiliation and pictures) will be displayed, depending on the constituency.
    a. Once the bio-password links a user to the right constituency the system must display a list of the correct candidates for that constituency. With a picture, name and party affiliation.

b. The correct display of information is especially is especially important in a PR system where users will cast multiple votes in order of preference.

8. When a referendum is being held, the full text of the referendum will be displayed.
    a. In the case of a referendum rather than a national or European election the GUI will need to change and give a simple yes or no formatted choice to the user. The full text of the proposed referendum must be displayed above the the choice buttons. This is to ensure voters can read the full text before making their decision.

9. The system will allow the user to confirm his/her selection and will give an “Are you sure?” message to which the user must commit before the vote is cast and the his/her decision is saved.
    a. There should be a double approval before a vote is cast. The voter can make their selection then click “continue”. This should trigger an “Are you sure” message. If positive the voters choice/s should be displayed and approved one more time before their choice/s is locked in.
    b. This functionality is necessary to ensure voters do not cast votes that were not their intention. The system must be ironclad in terms of the exact right vote being cast by the user. Otherwise the system will face public backlash.

10. The system will accommodate all potential user ages (i.e. 16-130).
    a. The system must be ergonomic in its design and accommodate all potential user ages.
    b. The potential age brackets are 16-130. The voting age will most likely be lowered to 16 next year which is why we have chosen this as the lower bracket. By the time this system is introduced there may well be 130 year old people in Ireland. And even if it's only one the system must accommodate them.

c. This would be implemented by having magnifying and text reading functionality in the system. Also buttons should be large and separated by a good margin to allow for the infirm.

11. The system will ensure votes remain anonymous.
    a. Voters anonymity is a priority for the system to ensure the safety of voters and to prevent any interested third parties in stealing voters personal information and influencing their vote.
    b. System must provide 100% anonymity otherwise voters will be reluctant to use automated voting stations.

12. The system will log a user out if he/she is inactive.
    a. To prevent someone else from voting from a particular user's account the system must logout the user after a certain period of inactivity.

13. A state-wide satellite internet connection will be available in all regions of Ireland for a stable and secure voting for all residents.
    a. Full internet coverage is absolutely necessary for people from all over the country to vote, the primary reason of poor turnouts in voting is poor accessibility, therefore by providing full internet coverage every single resident will have a chance to cast their vote.

Non-Functional Requirements

1. The system will be able to accommodate all potential users at the same time (i.e the entire population of Ireland, which will be 5 million).
    a. In ideal circumstances the system should be able to handle all the votes cast from every registered voter on the voting day without crashing.

2. The system will have enough storage capacity to hold all vote information and vital details about previous votes.
    a. System should have enough space to accommodate and keep record of all previous votes for statistical analysis and in case the need for recount should arise.

3. The system will maintain a database of bio-passwords for the entire voting population (both Irish and European).
    a. The bio-passwords would be used every time a user wishes to log into their government issued voting device and having a database of all of these would make logging in easier for users.
    b. The bio-passwords need only be for the voting population as it would be redundant to have them for users that cannot vote.

4. Bio-passwords will be as close to 100% accurate as possible.
    a. Users should have no problems logging into either government issued devices or polling machines and having the bio-passwords be as accurate as possible would ensure this
    b. Having the passwords be as accurate as possible would cut down on users redoing their bio-passwords if they keep getting it wrong on attempted log in.

5. If the user has not touched the screen for 60 seconds, the system will log them out.
    a. To ensure no person other than the appropriate voter has access to the account currently logged into the voting machine, if the voter forgets to logout.

6. The government issued devices will be rugged and have a highly sensitive transmission error detection system to ensure accuracy when it comes to counting votes.
    a. The government issued devices should be rugged as to ensure they are not damaged easily, which would avoid having to send out replacements to users.
    b. Every vote needs to be counted, so every error that may arise should be detected in order to ensure that the user knows about it and correct it if need be.

7. The system will be highly scalable to account for population growth and immigration.
    a. Ireland has an average of 2.0% population growth every year so the system should be able to be adjusted for this growth on an annual basis.
    b. Ireland is a hub for immigration, especially in Europe, and the system needs to be accountable for this kind of scalability. Foreign users cannot vote in Irish elections but they can in European elections, if they are European.

Overview

The purpose of the system will be to conduct all elections of Ireland. The system will allow citizens of the country to vote in a secure, anonymous and reliable way for the candidates of the ongoing election. The system will allow the introduction of the candidates and the rules of the election by authorized election officers.

The system will have several modules, notably the server side of the election system and the client side. Two or more instances of these modules will collaborate during the election. Please note that there can be more than one instance of the server part of the system, which must be able to communicate between them and to share the workload among them. Obviously there will be more than one client component in the system, all of which will connect to one of the servers available.

The server side will be operated by the system administrators and government officials of the system and they can set up the available choices during the election. The client side of the system will be operated by the voters of the country.

Correct functionality, availability, security and robustness are among the most important requirements of the system, since without these qualities the product is worthless in the eyes of the public, the government and practically all stakeholders of the system.

Server side of the system

This part of the system is responsible for authenticating the voter, validating and counting all the votes of the election. The server side of the system must be deployed to a physically secure location and on a private network.

This part of system is made of up multiple modules: a module which stores data, such as a database management software, the email subsystem, and another application which enables the authorized users to perform operations on the system and to view statistics, logs and perform audits. The requirements of the server side of the system are specifically tailored for stakeholders that interact with this part of the system: system administrators and government officials.

Client side of the system

The client side of the system will be a piece of software which will communicate with the server side of the system, in order to convey the choice of the user in a structured way. The client side can be any piece of software that respects the interface of the server side of the system. This will allow us to extend the system by creating new types of clients, which can easily be incorporated into the existing system. The requirements of the client side should reflect the needs of the voters regarding interaction with the client side of the system.

Functional requirements

Desktop application and mobile application

The client side of the system should be an application on desktop, like a program which you can download on the internet and then, being connected to the internet you can begin your session of voting. The application will be an executable file which you can use without an installation and you can delete afterwards. The application desktop must be available only during the voting session. The desktop application will support operating systems such as Windows, Linux and MacOS.

Also, the system can be implemented as a mobile application. By using a mobile application, the flexibility of voting increases, because 86% of Irish consumers are using smartphones according to www.businessworld.ie and it can lead to an increasing numbers of people who vote.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 should comply with the current constitution of the country.

The system should be based on the electoral statutes of the country. The electoral system used in Ireland is single transferable vote. This type of electoral system is designed to achieve proportional representation and preferential voting. A voter's vote is initially assigned to his or her favorite candidate, and if the candidate has already been elected or removes, all the other votes are transferred according to the voter’s preferences.

Must provide a result

The system, after the voting period has expired, shall make a count of votes. The system will show the votes of each county separately and then the final votes showing the exact number of votes each political party has. All of this process would be represented with graphs and statistics where users can observe the results in detail and more visually.

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. The system will allow the user to change their previous vote in case the user regrets the previous election or confused by selecting. Once the vote was taken, the system will redirect you to a page where the user can find the option to modify the vote.

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.

Authentication

Authentication is made always by id card. Citizens should have on their computer a slot to enter the id. Also, the system should has another way of authentication in complement to the id. The system should be able to do facial recognition if the person who is voting goes to an official place or to generate a personal password that is given by email before the election, in the case that the person votes from home. For that reason there is a database with the necessary information of citizens, their email or the facial recognition, which are made when their id is issued.

Email subsystem

An emailing system should be in place to provide means to quickly notify users. This email system could be used to remind users to vote, warn them about potential dangers (phishing attacks), and to send notification and confirmation to them. For example: after the user completes a voting session he/she should get an email announcing that the his/her vote has been recorded.

The need for the emailing system arises from the fact that fast, country wide, communication is needed for the complete system to work. In special cases, personal messages have to be sent to the email addresses of the voters, such as when we are confirming the registering of a vote of a user. The assumption is that every voter should supply a valid email address where they can be contacted.

Tutorials

The client side of the application must contain tutorials explaining the functionality of software. These tutorials should be simple videos or interactive demos clarifying the use of the voting system. By including these tutorials we can avoid a great deal of confusion on the voters' part. When a user starts the voting session, he/she will be presented with the possibility of taking the voting tutorial or not.

If the choice is yes, then the tutorial itself will load and appear on the screen guiding the user through the whole process by an example election. The interactive tutorial would require the user to select candidates and to submit a correct vote. The tutorial needs to be short and concise, a user must be able to complete it less than 5 minutes.

Finishing session

Network failures are inevitable, and since we cannot control the networks of the voters, we can mitigate the effect of a network failure by saving the progress of the voter in the voting session. This solution is only required in the following situation: the voter connects to the network and starts a voting session. After the user finished ordering the candidates, a network failure occurs and the vote cannot be registered in the central database. In order to not force the user to complete the voting process again, the client program will save the current status of the voting and send the result to the central database when there is an internet connection.

Database

Every county should provide its database for collecting information and centralise its data. Every database will hold the votes registered for every candidate in every election. It will be encrypted and will not be accessible directly by anybody. After the election was finished, the votes stored will be deleted and it will be kept only the results of each election to be able to make statistics after that. Every database from every county will be connected to a main database which will collect all the results. The main database will collect only the number of votes for every candidate.

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.

Non-functional requirements

Should be robust

The system should be enough robust to support all the activity in case that all citizens are connected to the application to vote. The whole country could vote at the same time. Each server must be able to serve 100 000 clients simultaneously.

The time to restart after failure should be at most 2 hours for hard problems, but for minor problems it should be at most 10 minutes.

The percentage of events causing failure should be less than 0.00001%. The probability of data corruption on failure should be less than 0.001%

Security

The security must assure that anybody couldn't break into database during the election and afterwards, until the data will be deleted. The system must store the recording data into encrypted files so that anybody could be able to read the identification information along with their votes. These files will be deleted after the election ends and all the data was centralized and sent to main centre. Security of the system will be tested through pentesting which means a professional will try to infiltrate the system and to document his/her findings.

Availability

The system must be available 99.99% of the voting time to the use, to ensure that everyone can vote when they want. The application should be available for the citizens at the moment that the period of vote starts until the moment that voting time finishes. In case that failure for unavailability occur it should be solve in less than 2 minutes to ensure that a person does not spend more than 3 minutes voting.

Reliable

The system should be reliable. The probability of unavailability should be 0.01% at most. Create fault tolerance is necessary to ensure that the application are constantly available. The failover should be an isolated process for the end user. The failover solution should guarantee that if the server or internet connection is offline, traffic is automatically re-routed to a secondary server or provider.

The mean time between failures should be at least 24 hours, the same time that the users can vote with the application.

Must handle exceptional situations

The system should handle some exceptional situations such as no current or others natural disasters. The system should store all the operations in that case.

The system has to be formed with at least two hard disks and a secondary server which will work in case that an exceptional situation occur. If one of the hard disk fail, the system has another one, in which all the votes are stored too.

Extensibility

The system must be capable to add new features. The idea is to have common interface and all the clients must implement this interface. For example, in the future all the technology will be based on virtual reality. You can vote in virtual reality, this means you can be at home with a pair of VR which will simulate an environment similar with a voting booth. To implement this, the interface should contain only what actions a voter should perform. The behaviour should be implemented separately by every client.

Easy to setup

The system would be easily deployable through a executable file, where the person in charge of the installation should only has to follow some steps without having to take much time. It would be a executable file with which the installation should be practically automatic. After installation there should be a configuration section where the person in charge of the installation can make the necessary settings as required.

Cheap to maintain and to buy

The buyers (Government) would like the system to be cheap. Should be cheaper to maintain than the traditional voting, meaning less man-hours. The total cost of the maintenance should be 60% of the maintenance of the traditional voting system currently in place. For example, it should be $100 000/month. It is a non-functional requirement since it does not describe what the system does, but describes the cost of the system maintenance.

Should be easy to use

The client side of the system should need minimal computer skills for being able to cast a vote. With the simple use of a mouse and the keyboard or the touchscreen, a user should be able to cast his/her vote in less than 10 mouse clicks or taps on the screen of the smartphone. The client side of the system should run without installation, simply by double clicking on the icon of the program in a GUI based operating system.

Fast to respond

Users want the program to react fast. The program in this context mean the client side of the program and the piece of software on the server side that the government officials use. The program should be able to receive new UI operations in 0.1 second after the user made an interaction with the program in 90% of the time. In the remaining 10% the program should react in 1 second. UI operations include, clicking or selecting something on the screen. Network operations should complete in less than 5 seconds on a stable network connection. If the program takes more than 2 seconds to complete an operation then it should announce the user with a notification or a progress bar to indicate that the system is busy.

Support for disabled people

Since the client side of the system will be used by all inhabitants of the country, we need to ensure that disabled people can use the system without special help. Persons with vision, hearing or mobility problems need to receive help from the client side application in order for them to be able to vote with ease. Disability support should include magnifier, high contrast mode, text to speech capabilities and voice recognition (only for home voting).

What is the system?

An online voting system, which can be accessed anywhere around the world, from any device connected to the internet or a private network via their web browser. Each citizen who is eligible to vote is given a pre-made account consisting of a username and password. Citizens can collect their username and password from their local garda station up to 2 weeks before the vote. Users can then log in and vote from anywhere in the world using their account during the 24-hour voting session. Each citizen's account also has a location associated to it, based on their home address. As a result of this location attribute citizens are only shown candidates from their area when voting. Users vote using a drag and drop feature. The first candidate selected and dropped to the vote area of the screen is given top priority and every chosen candidate thereafter has their priority indented by 1. Once a candidate is selected they cannot be selected again. This ensures that no choice is skipped or duplicated.

Functional Requirements

1) **Log-in functionality** - Eligible voters must be able to use their username and password in order to log in the e-voting website. The usernames are unique identifiers containing the person number. A standard password is an at least ten characters string containing at least one symbol, one digit and one uppercase letter. The user must be able to change his/her password by logging in the e-voting website at any time except for the 24 hours voting session. The passwords and usernames are stored in a secure database server-side. If a user forgets their password, they must go to a local garda station to have it reset. Similarly if a user enters their password incorrectly 10 times in a row the account is locked and they can have it unlocked with a new password at a local garda station. Any one account can only be logged in on one device to ensure that a user does not login on multiple devices, preventing other users from accessing the site.

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.

3) **Multilingual website** - The content of the website must be offered in both Irish Gaelic and English. The user must be able to easily change between the two provided languages. This applies to the Voice Over and Speech Recognition features as well.

4) **Tiered voting** - The user must be able to rank the candidates in order of his/her preferences starting from one to the number of available candidates. The site provides auto-increment for the rank values implicitly.

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.

6) **Edit and Submit Features** - In order to encourage a responsible, well thought vote, the user must be given the chance to edit his/her preferences during the 24 hours voting session. A user must be able to enter and leave the website multiple times and the latest selections will be saved for the next log-in. However, once the user submits his/her final version, the vote will be safely registered and no other modifications can be encountered. The user must be given no proof of his/her submitted preferences (in order to not be used for vote selling). The system must assure that each eligible voter submits at most one vote.

7) **Administrative rights** - Besides the regular users, the system should support system administrators, which can log in to the website at any time before, after and during the voting session.
   An administrator can **add and remove candidates** before the voting session has started. The website should be easily editable if any changes occur in the list of candidates.
   They can get **system informations**: number of active users, number of waiting users, response times.
   They can perform different **tests** before and during the voting session (i.e. try to submit a vote which will be of course invalid, simulate a given number of users using the system at the same time).
   They can **start the voting session**, making the website available for everybody to log in.

8) Tutorials

The system should provide two tutorials, **short videos containing animations** for the users in order to help them in using the interface if they have problems. These videos should be replayable at any time.

First tutorial: Should be accessible on the login page, a video **explaining each field of the login page**. (where to enter the username and password).

Second tutorial: Should be on the page containing all the candidates, a video **animating the drag and drop feature**, giving an example of how one or more candidates can be selected, without giving advantage to any candidate (symbolic example of some random candidates), and how to undo a selection by simply dragging and dropping a selected candidate back to the original position. Also, in the tutorial, there must be stressed the fact that without submitting the vote, the user's vote will not be taken into consideration and once submitted it can no longer be changed or reverted).

9) Time limit

The system should allow a user to stay **no longer than 20 minutes** on the website.

Timer: After the user accesses the website, he/she has a timer which starts counting down from 20 minutes. When there are 2 minutes remaining, the user must get a warning that in 2 minutes he/she will be disconnected.

Timeout: After 20 minutes, if the user is still connected and no vote has been submitted, the user is disconnected from the server, their choices being saved, but no vote being submitted, and other users are given a chance to connect. There should be no errors in the system if a timeout occurs. The disconnected user can log in later and should see the order of the chosen candidates as it was previously selected, having the same 20 minutes to submit the vote.

10) Summary

Purpose of displaying election results on website and publishing to media. Having the vote count stored in a database as votes are submitted, each constituency's candidates total number of votes will be published after the results are calculated and can be accessed via logging into the website. At the end of the 24 hour voting window, result computation involving gathering totals will be commenced. No later than one hour after the window has closed will results be released by way of media outlet communication and access to results on the e-voting website.

For the total number of votes counted, each constituency's total number of allocated elected representatives should be decided by standings of total votes acclaimed by each candidate. This should take into account the order of preference of votes submitted as well, meaning that where there is even votes of first preference, second preference votes should be assessed and so on. A total number of elected representatives from each party should be displayed and published giving light to what party can claim majority in a government seating arrangement, by way of which party has the most elected representatives. Party percentages should be computed for the entire country and individual constituencies. For every depictable piece of results information, the way in which each will be presented should be a graph or table.

Non-Functional Requirements

11) Availability

Beginning at a specified time, a 24 hour timer will be sanctioned to allow voting and access to the e-voting website to take place. The specified time should be decided by the governing intermediate body in the election who also has access to the database so that vote submissions may begin in tandem with the 24 hour window. Outside of the voting period, access to the website to view candidates, edit account password and access tutorials should be warranted. The only difference in the website when the voting window commences is that voters are presented with drag and drop options to fulfil their voting opportunity. 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.

12) Site capacity

The system should **support 100,000 regular users at the same time**, and no more. Any other user who tries to access the website when the capacity is full should wait.

Full capacity reached: In case the system reaches the maximum number of users which can be connected at the same time (100,000), the system should not let any other user to log in until there is a free space.

Waiting users: The system uses the first come first served principle. If full capacity is reached, every other user who tries to log in should receive a corresponding message and an estimate waiting time (calculated in function of the time remained of the logged in users and the position in the waiting list).

13) Security

The system should be a secure one: **protecting data** from attackers, and also **restrict unauthorized users** from accessing the website. The system should check if it is **a real user or a robot** trying to access the website, and should use **encryption** for password security.

Data protection: Ensure that every vote is recorded and cannot be changed once submitted (votes should not be edited or deleted without detection). Also, the user informations in the database (username, address) should not be modified or deleted during the 24 hours voting session. Passwords can be modified at a local garda station. Nobody should be able to see if an individual already voted or how the individual voted. The regular users are restricted to see other users informations (username, password, address), while the system administrators can access these data.

Unauthorized users: The system should limit the access only to authorized users, allowing access only to system administrators and users who are eligible to vote and have a secure connection, provided they pass the login phase, and restrict any other unauthorized users.

User validation: Before giving a user the possibility to vote, after the login phase, the system should check if it is a real user or a robot trying to access the system, using “captcha” (present the user pictures and make him/her select some of them using logical thinking e.g selecting all the images which contain animals) or voice detection for disabled people (asking them to read outloud a text, which is displayed on the screen and also read out loud before, with mixed-in background noises for security purpose).

Encryption: All the passwords in the database should be first encrypted and then stored.

14) Equality

It is important that every candidate is presented as equally as possible on the page. This is to prevent users being encouraged to selected a certain candidate knowingly or otherwise.

Candidate Layout : To ensure no candidate is in a preferable location on the screen all candidates layout are randomised on page load.

Candidate Location : Each candidate must be displayed on the same page (no toggling between page 1 and page 2 etc.)

Candidate Size : Each candidate's size on the page must be equal.

15) Database

The database should be easy to maintain and update before and during the voting session, storing accurately the user informations and the exact number of votes.

The system should support two separate databases. One which stores user information :

I.e username(id), password(encrypted), location, date account was registered,voted(T/F). It is important this database does not have any link to how the user voted.

Username	Password	Location	Date registered	Voted
BMc2584	Sdadfu827aD#	4 South Lawn, Togher, Cork	25/4/17	F

The second database is not connected to the first to ensure voter privacy/security. It contains analytical information about vote participation (number of entries in the table) Vote location(User's registered location, not location where vote was placed. Also does not give user's full location just a broad location.),Date and time voted,Vote choice,System used to vote.

Vote ID	Location	Date and Time	Selection	System Used
1	North Cork	11:04 26/4/17	1,3,10	iPhone

16) User interface

Friendly, **simple**, **easy to use** interface for everybody.

Friendly: No special computer skills should be required in order to vote. Nobody should have major difficulties selecting the order of the candidates(using the drag and drop feature) and submitting a vote.

Simple: Login page asking for only the essential information (username and password). After login, a page containing all the candidates is presented to the user, and a list (initially empty) of the selected candidates in order of preference. Also, the user should see clearly a timer showing how much time he/she has left. The system should give a warning when there are only 2 minutes remaining.

Easy to use: The user can select the order of the preferred candidates by simply drag and drop in order to avoid possible errors (e.g. incorrect indexing for the candidates). A submit button should be available, and after pressing it a message is shown, warning the user that once the vote is confirmed, it can no longer be changed. The submit button should be available only if one or more candidate is selected, thus avoiding an empty vote. The user has the possibility to go back and edit the choices between login sessions, however once a vote is submitted it cannot be edited and users are warned of this when submitting. If the submit button is pressed, the vote is stored and the user is logged out automatically.

17) Accessible System

It is important that the system is widely available to users. This means that devices (PC,smartphone, tablet) should all be usable if connected to the internet. This means not only will the website be available but also for smartphones and application version of the system will be provided. This app will be compatible with the 5 most recent versions of iOS and the 5 most recent releases of the most popular Android OS. Similarly multiple users should be able to vote using the same device this means that a vote casted is tied to account and not device. The user should be able to submit their vote using just one login session unless their time limit is reached.

18) Response times/ performance

Website pages will have to be reloaded if the user is logged in to the website before the voting window commences to see the drag and drop options when the voting window commences. Upon the 24 hour limit starting, logging in to the website should be possible from any internet browser with a connection to the internet. Login success should be heavily reliant on the users' connection quality

as there should be no discrepancies in response times from the central server unless the site capacity quota is met. At best, login should be granted within 500 milliseconds. If an internet connection is suffering poor bandwidth or slow speeds, there will be a timeout period in which data transfer can be done but not after the timer has expired. In this case, the information from a browser(user) will have to be resupplied. Common networking principles will be used as usual, like the requested webpage acknowledging requests from users. Before and after the voting period, users will not be restricted to a login time limit. During the voting window, a timer will be put in place of twenty minutes to enable the central server and database to handle traffic to the strength of the site capacity. At the point at which the timer expires, users will lose access to the page and will be required to login once more. This is also the case for when the window shuts at the end of the 24 hour period. Losing access means automatic reloading of the page and returning the user to the login page.

19) Error Handling

The system should be able to handle errors of every variation. If a user loses its connectivity before submitting his/her vote, the selection of the user should be saved. The database should remain unaffected by attempted data insertion where a network connection is not fully operational. Where an attempted vote is submitted from a user's browser to the central server but there is a breakdown in network connection, a process of validation is run at the server side to verify the legitimacy of the data that has made it to the server. If data is found to be incomplete or corrupted, the data(vote) is not sent to the central database and no data is stored. What instead happens is the page is reloaded to its previous state if login details are still consistent in the session details of the browser(user)-server(voting authority) connection. In this way, the database is never receiving illegal information. There is a strict deadline for vote submission and any data received after that deadline at the server, no action is cast and no further data makes it to the server.

20) **Evolvability**

If any voting procedure or law changes, the website must be easily updated to adapt to these changes. Furthermore, the website must be designed in order to easily make use of new available technologies which can improve the voting procedure in the future (e.g. If retina scanning becomes widely available on users' devices, the application must be easily modified to allow also log-in using retina prints, which implies the database can store additional information).

Domain Analysis

A collection of components which co-operate in an organised way to achieve some desired result – the requirements.

Our E-voting system has 3 main components – Machine, software and human

We can define the human component of the system as Stakeholders. A stakeholder is an individual, group of people, organisation or other entity that has a direct or indirect stake in the system.

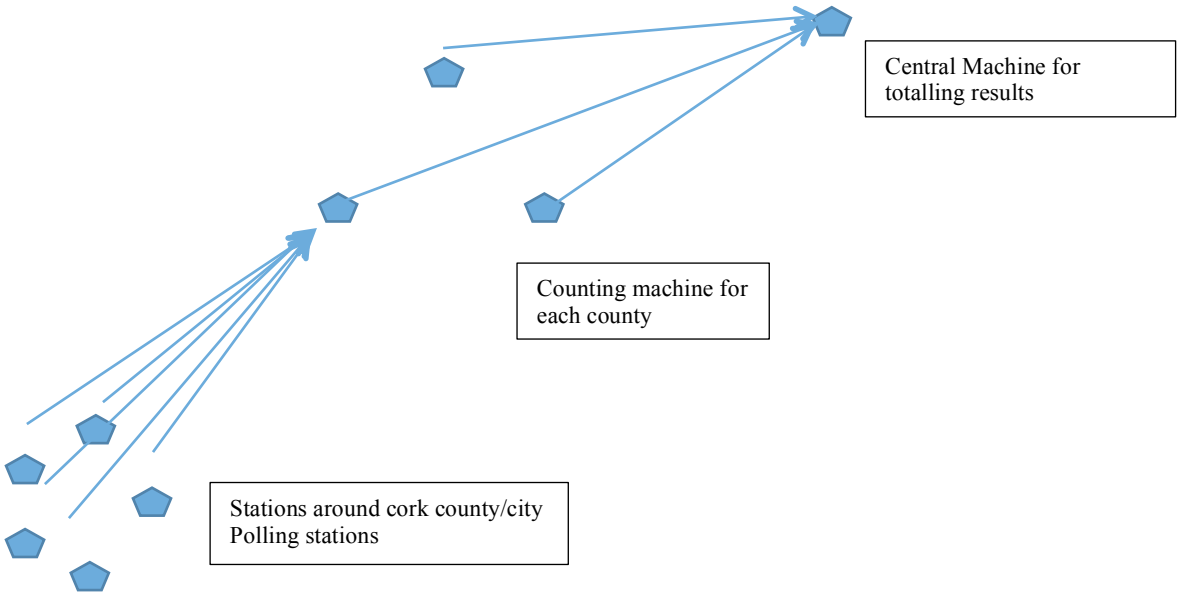
The stakeholders for our E-voting system include:

System buyers:	Irish government
End users:	The voters
Maintenance staff:	The people in charges of maintaining the system
Standards bodies:	The entity that ensures the system meets required standards to be used in an Irish election
Training staff:	Staff for training users and supervisors in the use of the E-voting system

The Machine component includes the machines at each polling station we people cast their votes and a central machine that takes all votes and counts the ballots

Software Component involves all the security protocols and accounting and sorting algorithms required to implement the system.

Our Bespoke Solution for the Irish government is based on the same structure as the internet edge and core. i.e. we have machines at each polling station that make up the "edge of the system" each polling station then sends all ballots cast to a local machine for their area which counts and stores all results. Once all ballots have been counted. And results calculated the local machine sends its data to a central machine that returns all results from around the country in the case of an election or it can count all the results to get the result of the entire country in the case of a referendum



The E-voting system will be suitable for all types of Irish elections from local government elections to national elections to a referendum.

System Legacy

Electronic Voting in Ireland was first proposed in 1999 by former Fianna Fail Minister Noel Dempsey in 1999 but were not brought in until May 2002 on a trial basis. This trial basis saw 42 out of Irelands 158 constituencies use electronic voting machines for a general election, with the intention that it would extended nationwide for future elections. Also in October 2002, electronic voting machines were used in seven constituencies for a referendum on the Treaty of Nice. Following these trials, a confidential report expressed serious concern over the security of the voting machines. According to this report the validity and integrity of the ballot could not be guaranteed with the equipment and controls used. The Department of the Environment disagreed with many of these findings, reiterating that the machines were secure and that the presence of voting officials prevents tampering.
In March 2004, the Irish government established the Independent Commission on Electronic Voting and Counting at Elections to examine the proposed system. This was later dissolved in 2006. The commission did however, issue a series of reports reviewing the proposed system and comparing it to the existing electoral system. The commission recommended the voting and counting equipment stating that with minor modifications the embedded software is of adequate quality and that the voting machine and related hardware components are of good quality. However in October 2006, a group of Dutch hackers, showed how similar machines to the ones purchased in Ireland could be modified by replacing the EEPROMs with Nedap –Firmware with EEPROMS with their own Firmware.

In April 2009, Minister for the Environment John Gormley announced that the electronic voting system was to be scrapped. The 7500 voting machines purchased by the State at a cost of €51 million from Dutch firm Nedap were held in storage until June 2012 where they were sold for scrap for €70,267 by KMK Metals Recycling Ltd. With additional storage costs of €3.2 million brought the total. Then Minister Phil Hogan was quoted “I am glad to bring this sorry episode t5o a conclusion on behalf of the taxpayer. From the outset, this project was ill-conceived and poorly planned by my predecessors and as a result it has cost the taxpayer some €55 million.”

Thoughts on Legacy.

It can be seen that Irelands only attempt at an E-voting system failed miserably on the basis that the voting machines, relative hardware and embedded software posed serious security issues. Our learning form this shows that it is imperative that security amongst the main issues to consider when designing our system.

Functional Requirements

1	Function:	Vote Validity
	Description:	Ensure that each user only votes once and cannot vote again upon leaving and logging in again.
	Input:	Current user ID.
	Source:	ID received upon user login.
	Output:	Successful if vote cast correctly or create an error log if not.
	Action:	Default output is successful unless User has tried to Vote multiple times in which case an error log will be created.
2.1	Function:	Data Integrity
	Description:	Ensure that each vote is recorded as in tended and cannot be tampered with in any manner once recorded.
	Input:	List of cast votes.
	Source:	List dynamically created as votes are cast contain both valid and spoilt votes to ensure no spoilt votes are tampered with.
	Output:	If vote tampering create an alert to the system administrator notifying them of an illegal action.
	Action:	Create and alert notifying which votes have been tampered with and create a log of the event.
2.2	Function:	System Integrity.
	Description:	Ensure that the system cannot be reconfigured during operation.
	Input:	Type of election being run.
	Source:	System Administrator selects the correct election algorithm to be used.
	Output:	System runs using the selected election algorithm only and cannot be changed until after votes can no longer be cast.
	Action:	System runs using selected algorithm if algorithm is changed create and alert to the system administrator and an error log.
3	Function:	Ballot Design.
	Description:	Provide different styles of ballot for the different types of election. Local, National, Referendum.
	Input:	Election algorithm.
	Source:	Selected by system administrator.
	Output:	G.U.I showing the correct ballot style for current election.
	Action:	Default system creates G.U.I. and enables user to vote. In case of an error create log and send alert to system administrator saying which machine and user needs help
4.1	Function:	Error Logs.
	Description:	Create Logs of any errors or unauthorised access or spoilt votes.
	Input:	Unauthorised access to votes/system or error in runtime/spoilt votes.
	Output:	Generate a log file of the error.
	Action:	Each log should contain detailed information about the error. Such as which vote was tampered with, time the error or unauthorised access occurred, I.P. address of the user accessing the files.

4.2 Function: Spoilt Votes.
Description: Maintain a list of spoilt votes along with all votes cast and ensure that there is no tampering with the spoilt votes once stored. Create an error log of spoilt vote.
Input: User vote.
Source: Submitted ballot form.
Output: Error log of spoilt vote.
Action: Add vote to list of votes cast and list of spoilt votes. Ensure vote cannot be tampered with if spoilt vote is accessed again generate error log.

5 Function: Language Choice.
Description: Offer user a choice between Irish and English when filling out ballot
Input: User chooses preferred language at start of voting process
Source: Election algorithm
Output: Generates the G.U.I. in preferred language

6 Function: Registration
Description: Maintain a list of voters that have been identified and are eligible to cast votes.
Input: Verified user identification.
Output: User Login details.
Action: Generates a database of registered voters with a correspondingg Login where each voter may only register once.

7 Function: Login
Description: Allows each registered voter to log in once, generates a random id To keep their vote and identity separate and brings them to the voting Module.
Input: Log in details.
Source: Generated at voter registration.
Output: A unique vote ID number generated upon login which ensures Votes remain anonymous and voter and vote are separated providing Anonymity.
Action: Verifies with login that voter has registered, separates identity and Vote and allows access to ballot casting.

8 Function: Casting Ballot
Description: Voters must be presented with all the correct voting options.
Input: Voters input their selection.
Source: G.U.I created for the election
Output: Requests that user verifies the vote
Action: Clearly presents the voters options and allows them to make their Vote and records their selection.

9 Function: Vote Verification
Description: Voter will be asked to review and confirm their vote and given the Chance to make modifications if desired.
Input: Confirmation and/or modification of vote.
Output: Receipt of confirmation of final vote being cast.
Action: Voters intent is cast.

10 Function: Vote Storage
Description: Method in which votes are stored and tallied.
Action: System batches periodically, no vote will be lost, the votes Are sent to an area's local machine, vote tally occurs, all local Machines transfer their tallies to a central machine that provides the Country's final vote tally.

11 Function: Vote Analysis
Description: A means to audit the stored votes. .
Action: It must be possible to ensure that all votes are accounted for and to verify these votes, the number of votes and the number of voters Must be consistent, an audit trail must be kept that will keep track of every vote and offer a means of authentication and back up in the Case of a system failure or contest regarding the vote.

Non-functional Requirements

1 Function: Robustness
Description: Ensure that upon failure, that the time to restart after failure and probability of data corruption on failure is minimized.
Action: Ensure that there is system recovery in place and also that votes cannot be lost if failure occurs.

2 Function: Portability
Description: The generalized abstraction between application logic and the system interfaces.
Action: Make sure that the voting machines can be used on multiple types of votes i.e. Referendum, general Election etc.

3 Function: Accessibility
Description: To make systems and applications accessible to people with disabilities.
Requirement: To adhere to relevant accessibility guidelines in place.
Action: Ensuring all Irish citizens, and in particular disabled citizens, are able to vote.

4 Function: Reusability
Description: Extent to which end products can be used rather than rebuilt
Requirement: Offer flexibility in system design so any future updates can be made with relative ease.
Action: Make sure e-voting system can be used over and won't outdate.

5 Function: Capacity
Description: Number of users, records or data volumes.
Requirement: Consensus of population.
Action: To allow for varying amounts of voters as that can vary pending on Population growth, unregistered voters, registered voters who do not vote etc.

6 Function: Traceability
Description: Property of an element of documentation or code that indicates the degree to which it can be traced to its origin.
Requirement: All votes can be traced, all voting officials are accountable, and all voters can be accounted for.
Action: A database where all embedded software code, documentation can be accounted for. Also all voters can be traced to validate them along with their votes.

7 Function: Interoperability
Description: The ability for the system to exchange and make use of information.
Requirement: For all votes to be sent to server along with vote count.
Action: All voters are accounted for, all votes are kept in a secure database and also that vote count is updated continuously without security risk.

8. Function: Reliability
Description: The system should not fail when voting is taking place. If it does a backup of votes cast should be made available.
Requirement: Votes should be sent to a server as soon as vote is cast to avoid loss of votes. System should be optimised to run at optimal levels
Action: Extensive testing of system should be carried out before deployment.

9. Function: Usability
Description: The system should be simple to use for all users. With intuitive design without complicated features.
Requirement: Interface is easy to use with few buttons and controls as possible.
Action: Any type of voter can use the system

10. Function: Performance
Description: A processor which can handle multiple choices of votes being cast and to restart for a new vote to be cast.
Requirement: System performance should be able to handle multiple votes being cast and handle a new voter almost immediately.
Action: Fast performing system with minimal delay when a new voter would like to use system.

11. Function: Maintainability
Description: The ease with which a system can be modified to correct Faults, improve performance or other attributes, or adapt to a changed Environment.
Requirement: System should be able to be updated or improved without causing disruption to the system.
Action: Easily deploy updates remotely to system.

12. Function: Testability
Description: Ease with which a system can be tested.
Requirement: Enough information in the system to enable us to confidently determine whether the system has performed correctly.
Action: Continuously test system throughout system build for correct performance and desired output.

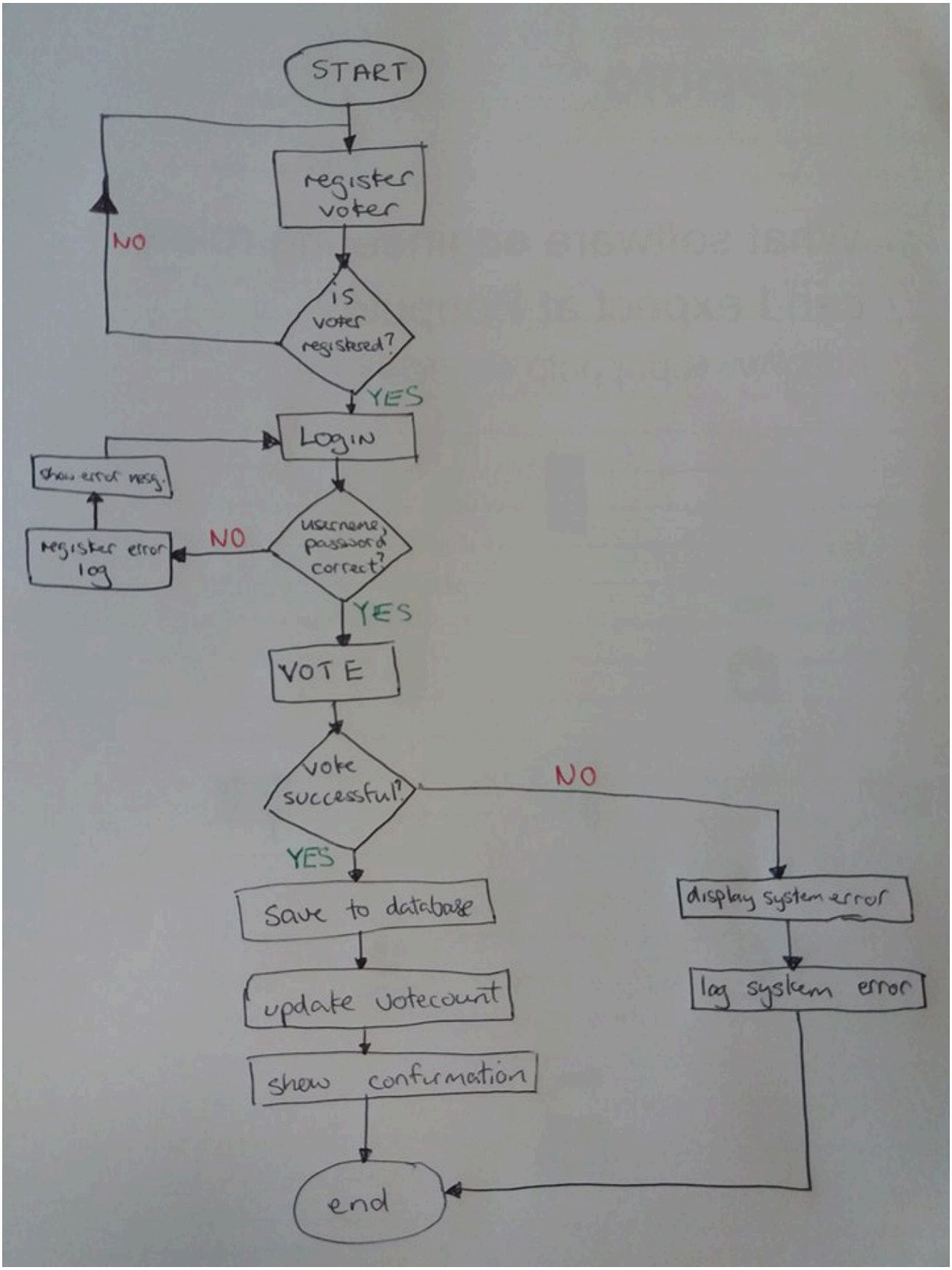
13. Function: Simplicity
Description: System should be easy to use with no complicated features.
Requirement: Easy to use GUI with few controls as possible to make sure
The voter isn't confused using the system.
Action: Design a GUI which is easily understandable and can be used by
All types of voter.

14. Function: Changeability
Description: Ability to update or change features of the e-voting without affecting the components of the e-voting machine.
Requirement: Make a change to the e-voting machine without
Action: Make incremental changes testing at each step to make sure the e-voting machine is working correctly.

Requirement Prioritization

The requirements were ranked based on MoSCoW technique. We gave top priority to everything we required to ensure the success of the project. This means that all functional requirements are ranked ahead of all non-functional requirements. We then sub ranked both types of requirements using a Bubble sort technique, first listing them all and then comparing each requirement with the next and swapping them if we felt that had a higher priority.

Flowchart of System



Scenario for and e-voting system

Initial Assumption: Voter goes to the polling station and hands a form of identification to the polling clerk, so that they can use the e-voting machine to cast their ballot.
Normal: Voter uses the e-voting machine to cast their vote.
Exception: If the voter hasn't used the e-voting machine before then a person is on hand to show the voter how to use machine and make sure a correct vote is cast.
Other Activities: Vote should be able to confirm which vote is going to be cast before finishing.
System State: Voter receives confirmation of their vote being cast correctly.

User Stories

As a voter, I want to cast my e-vote, so that my vote is securely and is efficiently counted.
As a polling clerk/presiding officer, I want to view a count of the e-votes which are cast, so that I can announce the results of the efficiently and correctly.
As an e-voting machine technician, I want to be able to add candidates in different constituencies, so that each candidate is correctly inserted.

Conclusion

Our proposed Electronic Voting system looks to improve upon existing legacy Systems in order to provide a method of voting that improves upon the current System in areas like speed and ease of use but does not compromise on security, our Goal is to create a safer E-voting system.
Due to our research on legacy systems we have come to the realisation that security Was the major downfall of the last attempt and therefore must be a priority in any Proposed new system.
We have outlined scenarios and User stories to ensure we understand the user Needs and can create the best possible user experience.
We have identified our stakeholders in the interest of encapsulating all necessary Requirements for our system.
All our outlined requirements fulfil the SMART criteria to ensure the best possible System design, they are Smart, Measurable, Attainable, Realistic and Traceable.
We have detailed both our functional requirement detailing what our system must Do and non-functional requirements which entail all other constraints.
We hope that our new system design solves the problems of the legacy systems and Provides a safer more efficient voting system.

Team member Contributions

Luke:	Functional requiremaents1-5 and domain analysis
Sile:	Functional requirements 6-11 and Conclusion
Fantan:	Non-functional requirements 1-7, History of E-voting system and Flowchart
Tomas:	Non-functional requirements 8-14, Scenario and use Stories

Brief

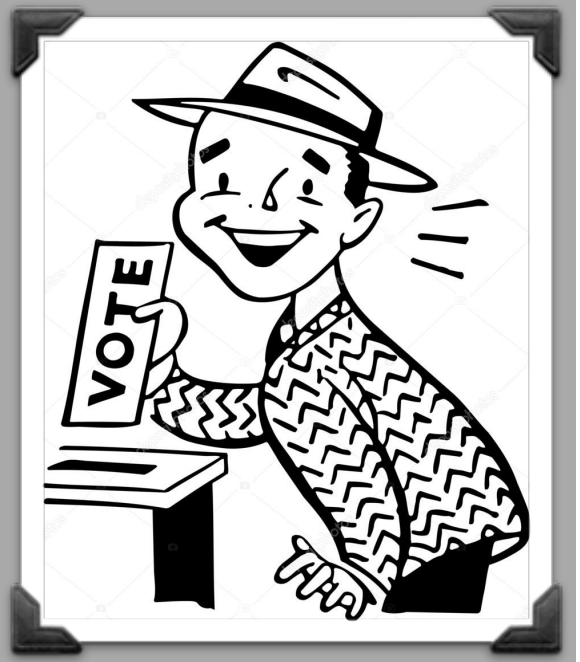
Our implementation of and E-voting system is a simple but sleek modern system that incorporates modern and retro aspects of voting.
Our physical machine is designed to be elegant and extremely user friendly encompassing interactive features while there are features of our system such as checking voter identity that we decided not to change as implementing a machine that uses facial recognition would be too expensive and unnecessary when the system we have now is functions flawlessly

Functional & NFR Requirements

- **Physical Machine/System(Functional)**
- **Voter Verifies Identity(Functional)**
- **One Person, One Vote(Non - Functional)**
- **User Interface (Functional)**
- **Showing Relevant Data on Screen (Functional)**
- **Take vote(Functional)**
- **Process vote(Functional)**
- **Store vote(Functional)**
- **Calculate vote(Functional)**
- **Be 99.9% secure (Non-Functional)**
- **User-friendly / Ease of use(Non-Functional)**
- **Store votes (Functional)**
- **System ensures anonymity(Non-Functional)**
- **Undo/submit (pop ups)(Non-Functional)**
- **Safety(Non-Functional)**
- **Statistics / Metadata(Non-Functional)**
- **Cost Effective(Non-Functional)**
- **Transparency(Non-Functional)**
- **Time Constraint(Non-Functional)**
- **The System must allow for voters who cannot reach the polling stations(Functional).**
- **Proprietary open source (Functional)**

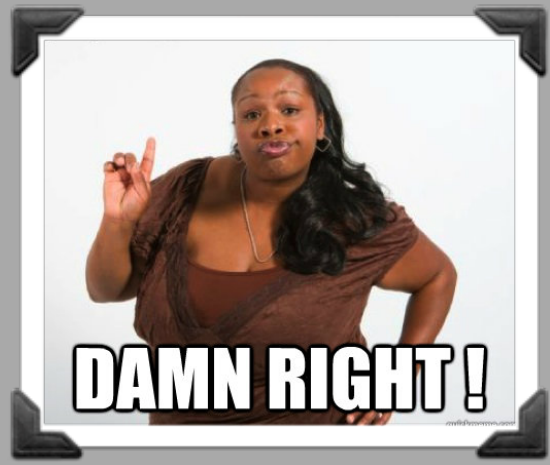
Physical Machine/System (Functional)

What we want from the physical system is simple we want an elegantly designed Machine with a main interactive touch screen that displays the candidates/criteria being voted upon in the election.
The screen will be of 14 inches with sleek edges and will have the most up to date technology to allow ease of use.
The system will be robust, portable and reliable to allowing ease of movement when being removed from location and it will be durable made of a light but strong material such as Aluminium as not to damage in transit .



Sowing Relevant Data on Screen (Functional)

As a requirement we don't want our screen to be cluttered. We will only show relevant data on screen.
There will be no small hard to view text or complicated prompts, only what is necessary to vote will appear on screen. To begin with we will have 2 text fields that will allow the voter to login and verify identity. Next we will have the question being voted on displayed in bold text so that the question is clearly visible as well as the pictures and names of the candidates running for election. When you chose your preference a pop up will appear to prompt you verify and make sure you have selected correctly. The final step is hitting the large submit button which will immediately process and store your vote.
On the screen a message will appear saying thanks for voting. Adding to users satisfaction.



Voters Identity (Functional)

In all voting systems, voters must register to be able to vote in their constituency. On the day of the election/vote they must also prove their identity to the polling station clerks. This is a requirement in order to ensure everyone can only vote once in one constituency. This requirement remains the same whether the voting system is paper based or automatic/ computer based. Traditionally, in the Irish system at least, this is done by the voter producing some form of photo ID, ideally a passport, at the polling station and the clerk first verifying the identity and then checking it against the list of eligible voters. Whether this requirement is met through the use of a computerised or physical solution might simply come down to cost. There are machines currently in use in airport security to scan a passport and a person's face and using face recognition technology it can verify whether it is in fact the person the passport belongs to. It might be cheaper however employ human officials as before rather than invest in these machines.

User Interface(Functional)

The purpose of the large screen is to be able to clearly and concisely read and submit your vote.

The election in action will be clearly displayed on the screen in bold writing and and just beneath the question there will be two large tabs that read YES/NO and when pressed will have a large pop-up to confirm you have correctly enter your appropriate choice.

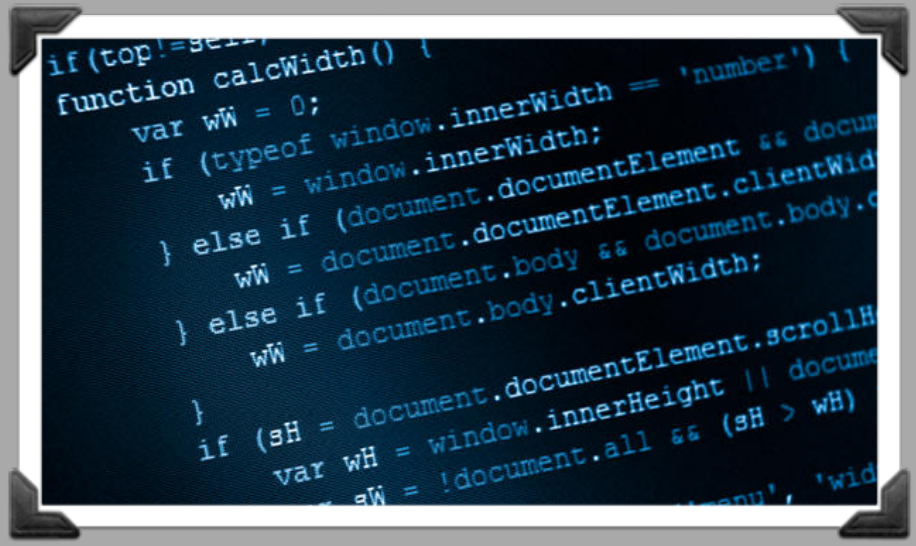
When it comes to multiple choice referendums such as a general election all the candidates that are running will appear on the screen and you will be instructed to touch each candidate you wish vote for.

When you have selected your candidate a keypad will appear on the right of the screen prompting you to enter your preference ie. 1,2,3,4…etc.

After clarifying each vote the user will be prompted to hit the submit button located on the bottom right of the screen this will lead to the votes being processed by a program being run in the background

Casting Vote (Functional)

Casting a vote is simple. All the options appear on the screen the voter selects their preference, they will be prompted by pop-ups that help them select and submit vote. Once vote is submitted the background program takes control and processes vote



Processing Vote (Functional)

When it comes to processing the vote the information will be encrypted and a sorting algorithm eg. timsort is run to efficiently sort the votes. The voters preferences are saved to a database that exists on the portable hard drive disk attached to each individual machine.

Storing Vote (Functional)

As we propose to use a physical machine throughout the E-voting process, this machine will have to have some way of storing each vote at every stage of the voting process, so when the time comes to finally process and calculate the results, it can be done in a timely and efficient manner through the use of software. The advantage of this is that it will eliminate the need to manually count each ballot by hand, thus ensuring that the result of the election/referendum can be delivered to the public without delay.

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. The database on each machine will be maintained and tested by a team of administrators prior to the election to ensure that it will run smoothly when the time comes, and if any problems were to arise on the day(s) of voting, they would be on hand to alleviate the situation. As we are trying to make an improvement to the current system of voting, I believe this is a requirement that our E-voting system must have in order to offer a comprehensive improvement to the way voting is carried out in our country.

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. Our current way of tallying up the votes of an election or referendum lies with a select team of highly vetted election officials, whose responsibility is to painstakingly sift through each piece of ballot paper and count each vote for each candidate. Unfortunately this can take quite a bit of time, and often recounts are inevitable due to human error. 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.

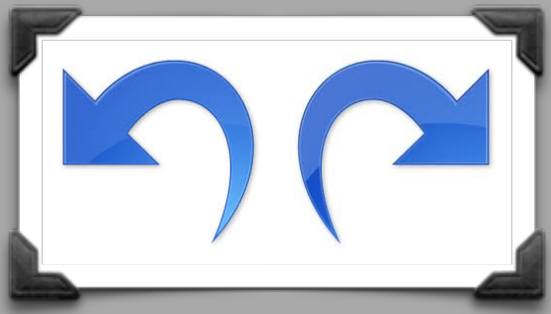
Since we have proposed to use MySQL to store the votes, it seems only logical to use the built-in mathematical functions in order to process the huge volumes of data stored in each database. This would also afford substantial statistical information to be made available to the election officials for. This can be performed by fewer trained and vetted staff in order to provide the results of the election in a timely fashion.

System must be 99.9% secure(Non-Functional).

One aspect of any election which is of paramount importance is the secure manner in which the voting process is carried out, and how the integrity of the election is upheld by not allowing any outside factors influence the vote, be it through intimidation or bribery etc. However, since we are promoting the use of an E-voting system, the importance of securing the vote and upholding the integrity of the election process doesn't hold the same importance in a functional regard, as the votes will still be stored and so on. On the other hand it is fairly significant in terms of it being a non-functional requirement. When people vote, they like to think that they are having their voice heard and we certainly think this is incredibly important while living in a modern democracy. The general public certainly deserve to be safe in the knowledge that their vote isn't being tampered with, and that their vote represents their preference.

Since the voting system is done with the help of physical machines, on site security will come in the form of administrators and/or general security staff, to ensure that none of the machines have been tampered with. It will get slightly more tricky when it comes to voters who cannot attend the polling stations (see related requirement.). This will require some solid encryption of the voters data to make it as secure as possible, and avoid any malicious users looking to tamper with votes.

Undo and Submit (Non-Functional)



As was the case with votes being spoiled due to mistakes being made with ballot paper, I certainly cannot see why it would be any different with the use of an E-voting system. As we are proposing to use a machine with a touch screen interface, I believe it's pertinent to provide the users with the option to undo their selections in the case of a mistake being made. This point becomes even more valid when it comes to more traditional voters using the system for the first time, as they may not have much experience with touch screen technology. It also allows users who have simply pressed the wrong option by accident, to undo and change their selections. Upon submission of the vote by the user, a pop up should come up prompting said user to review their selections before offering their final submission. This could certainly be an important requirement for the system as it has the potential to significantly lower the amount of spoiled votes.

Proprietary open source(Functional)

With the general scale of the elections undertaken in Ireland, using bespoke software created by a big company could incur huge costs for those who are running the election. To eliminate this we would use open source software developed for the sole purpose of running election. This would also give us the benefit of having a team of highly skilled developers working on the project, which would ultimately give us a comprehensive system on which an election could be run smoothly.

The System must allow for voters who cannot reach the polling stations(Functional).

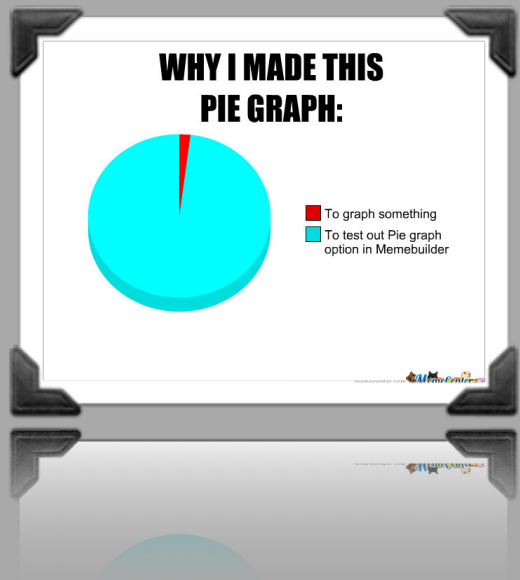
Unfortunately there may be certain voters in each constituency who will not have the ability to reach polling stations on the day of an election, so we believe there must be certain efforts made in order for these people to be able to provide their votes and have their voices heard. What we propose is that these voters will have special unique identifiers sent to their homes, along with a URL to the website which will take their votes. They will use the unique identifier to log in and then will be able to cast their votes. Allowing voters to vote online will require the securing and encryption of the data as it comes from voters home PC's and out into the network, so it will more than likely have to use https. We feel strongly that this is a really important functional requirement as it includes voters who may not have had a chance to cast a vote with the installation of Physical machines at polling stations.

System Ensures Anonymity((Non-Functional)

The secret ballot is a voting method in which the voters in an election or a referendum is anonymous. It preventing attempts to influence a voter by intimidation blackmailing and potential vote buying. It is essential that the system ensure anonymity. We need a unique identifier to show that person a registered voter and to prevent people casting more than one. However, it is important that a vote cannot be traced back to the individual. All personal identity markers of the voter must be machine encrypted, unreadable to humans in order to attain this requirement in the e voting machine. Proxy voting will not be permitted in this system as it infringes on the privacy of the secret ballot

Statistics-Metadata(Non-Functional)

By metadata I am referring is the retrieval of information about the votes outside the calculating of votes. Which is used as the statistics relating to the election, but not focusing on the result itself. For example, voter turnout, voting rush hours and regional trends. The retrieval of such information would be relatively simple to attain. If we store additional information with the vote such as polling station and time that vote was cast. All this data as well as the vote itself should be stored with the anonymous user. Ideally, we would like to claim as much information about the voter as possible, but this might not be entirely feasible without encroaching upon the users privacy and anonymity. Also restrictions on the systems memory size may also prevent this from happening. Voting statistics are essential for the voting process. Information such as voter turnout gives legitimacy to the current voting system. This requirement is vital for a democratic election.



Ease of Use (Functional)

Ease of use The voting machines are being deployed to the general public. When dealing with the general public we must consider that the various ranges of technical ability in the population. With this in mind, the voting machines will have to be made as simple as possible. The voter should be able to interact with the machine, and cast their vote in a manner which does not require to much effort or focus. The general public are likely to get distracted by external stimulus e.g. phone, so the machine must not require too much focus to return to after the voter turns their attention elsewhere. To ensure we make the machines as undemanding as possible we will have to run tests to see if it is suitable to be deployed. For example, timed speed of learning, number of help frames. The test should be conducted on all groups (age, tech ability) of people within the population to get most accurate results. Although we cant ensure every voter will be perfectly satisfied with the unadorned format, we expect the voting machine to be suitable for all voters to manage, given adequate learning time.

Safety (Non-Functional)

Safety is the process of protecting against external or internal dangers. It is of utmost importance that we try eliminate all potential risk for any person interacting with the system. We need to ensure that the system does not breach the voters safe space. If we don't, it may discourage potential voters from voting, giving a result which is not representative of the population. Calling into question the legitimacy of the result entirely. For the safety requirement to be implemented we need to recognise the potential hazards in the system and prevent them before deployment. This might include manually checking machines to ensure no loose wiring or working closely with specialists in the U.I. design to minimise chances of a trigger for seizures. Testing would be essential for this stage. No E-voting machine can be dispatched without a safety guarantee. However, attaining this level of safety for the device should not be too hard or expensive as potential hazards in such a device are so few.

One Person, One Vote(Functional)

Each person in Ireland over the age of 18 is entitled to one vote. Every voter should have a unique identifier to indicate you are an Irish citizen, over the age of 18 and a registered voter. This identifier should be viewed and checked for legitimacy, before voter may cast their vote. After the vote is cast, voter may no longer cast another vote again. This ensures integrity in the voting process, as all people in Ireland above the age of 18 are equal. A database containing all registered voters information will be constructed. This database will be asked to check each voter in accordance with their identifier, before the voter is given permission to vote. This methodology is used to protect against voters voting more than once. Once user has voted the database will note that under his/her information. This requirement must be 100% reliable, otherwise the entire voting process will be spoiled. This is one of the most important requirements so a great deal of effort and time must be dedicated to this area. To make certain it is dependable, numerous testing under every circumstance will have to take place, to safeguard against malicious voter interaction.

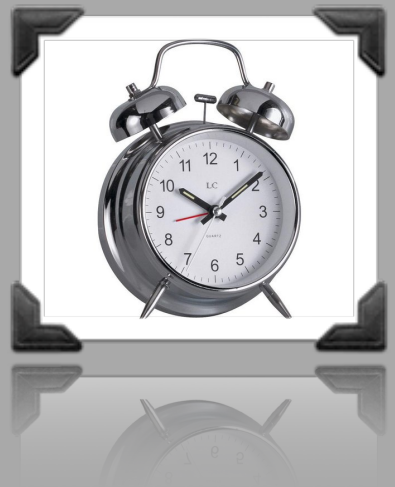
Transparency(Non-Functional)

Elections are hugely important events which affect every citizen of a country. Thus, fairness and transparency are absolutely crucial to any election system. In a traditional paper-based voting system multiple officials supervise each step of the process to ensure fairness. In an e-voting system, it is not as easy to supervise each process as the voting machines could be considered to be black boxes. It must be a requirement for officials to be able to 'view' the voting and counting processes. In an e-voting system, this would involve knowing the inner workings of all and any machines used, including the physical architecture and the software running on the machine. Officials would be needed to review all the code and to ensure that that is the exact code loaded onto every machine. This requirement holds for all polling machines, counting machines, and servers holding records of the results.

Avoid Tampering(Non-Functional)

As voters will be left alone in the polling booth with the polling machines, it is required that a number of security measures be put in place to prevent anyone tampering with the machines during that time. If left unchecked, someone with malicious intent could tamper with a polling machine, possibly disabling the machine without anyone knowing, which would make all votes cast at the same machine null and void. This requirement is very important as if not properly protected against a relatively small group of determined people could completely change the result of an important election.

Time Constraint(Non-Functional)



When it comes to the system as a whole we need to think about the election process, and the parts that actually allow the election to happen. For instance, the stakeholders in an election, such as the voters, election candidates, election staff (People who work at the polling station

Cost Effective(Non-Functional)

Any system should be developed to be as cost effective as possible. This is especially true for a large scale system such as an e-voting system. Although , since the system would be publicly funded there would not be a focus on profit, it is still an important requirement to keep costs down. The best way to achieve this would be through more time spent during the planning and early development of the system. Developing cheap prototypes would be a very cost effective way to avoid possible large scale errors later down the development line.

System Description

The system will be a touch screen machine similar in shape and size to an atm. Within this will be the underlying hardware of the machine, it's process, memory, storage etc which will receive data from the connected touchscreen. These machines will fit inside voting booths for privacy. Users will enter in a code and then be presented with their voting options. The user will then cast their vote and the machine will be locked until the next user enters the booth and their unique code. Machines will be connected on a local area network and all votes will be sent to a central machine and a backup. The votes will then be taken from this machine at the end of the day and sent onto the central authorities.

Functional Requirements

Requirement 1a: User Interface

The system should provide a friendly graphical user interface to ensure ease of use when voters cast their votes. The system must be fair in its representation of all voting options/candidates. In the case of choosing between different candidates, all choices should be displayed on one screen. The user should not have to scroll up and down to view the complete list as this would give an unfair advantage to those displayed at the top of the screen.

Requirement 2a: Simplicity

The system shall be simple and user-friendly. Voting should be quick and intuitive with no special skills required. Entering voter details should be straightforward and the process should not require extra skills or mental effort from voters.. The likelihood of making mistakes should be minimised. Complexity should also be kept to a minimum for election officials.

Requirement 3a: Flexibility

The system should have the ability to adapt to possible or future changes in its requirements. Different interfaces should be created for different ballots, e.g. referendums only have a yes/no option while general and local elections have to implement a numbered selection. The system should allow for multiple voting scenarios in the same session, e.g. referendums are occasionally voted on the same day as the general election.

Requirement 4a: Accessibility

The system shall cater to the needs of physically challenged voters. The system must be accessible for illiterate and sensory deprived people. A separate custom station must be created to accommodate those with disabilities. The system must implement braille screen readers and voice recognition to support the needs of blind people. Voting devices should have audio capability, which can operate in multiple languages. Workstation must provide a wheelchair friendly zone. An option should be given to change the colours for the colourblind. Disabled will be allowed to bring a partner to assist with their votes.

Requirement 5a: Eligibility

Can they vote? One vote only. Each voter on entrance will receive a unique code after authenticating their registration. The code is required to access the candidate selection screen. Once the unique code has been used for the vote it cannot be used again. This ensures each voter only gets one vote. Once the vote has been cast, the machine will be locked until the next code is entered.

Requirement 6a: Auditability

The system shall have reliable and authentic election records. The system should log activities and provide a way to analyse the logs, to facilitate accurate reconstruction and analysis of events that occur during the voting process. The audit service should have various means for searching and examining the logs associated with the voting process. The logs must be tamperproof and secure from interference by unauthorised individuals. Counting tallies will meet 100% accuracy to ensure the vote is fair, a minimum of 10 recounts of tallies will be executed to ensure the accuracy rate. Tally counting system will be implemented efficiently. Tallies will be updated automatically as each vote is cast. Tallies in the database will not contain voters' names for privacy reasons.

Requirement 7a: Vote Confirmation

After the voter presses the submit button, the system will output a confirmation of candidates the voter has voted. On the output, there will be the list of candidates the voter has voted on and the candidates that the voter did not vote for. This ensures the voters have casted the votes that they intended initially. There will be a back button and a confirm button. The back button allows the voter to make changes to their votes. Confirm button will submit their vote, after pressing the confirmation button, the voter will not be able to change his/her vote.

Requirement 8a: Correct Input

Can't vote for too many options or too few, must enter the correct input. Ballot information must be displayed in colour and must incorporate pictures of the candidates. When voters make their selection on the touchscreen, the selected candidate or issue must be highlighted. There must be a final vote or finished, button or screen for the voter to cast their vote. This must display a prompt when pressed, asking the user if they are sure they are satisfied.

Requirement 9a: Cost

Has to be affordable but maintain efficiency. System should offer efficiencies over paper alternatives. Internal components must only provide the resources needed, high end technology should not be needed for such a simplistic system. Likewise the code running within the machine should be lightweight and efficient so that the system isn't overburdened.

Requirement 10a: Closure Deadline

When the voting deadline has ended the system must not allow anyone else to cast a vote. The system must automatically lock at the deadline, even if someone is in the process of voting. There must be zero tolerance. Users should be warned at decreasing time intervals before the deadline to have prior notice of this happening.

Requirement 11a: Government Approval

The system must adhere to government requirements. It must comply with all legal, statutory and regulatory requirements. It should also comply with any international electoral standards with respect to electronic voting. The system must follow the edicts of any and all legal instruments that provide the framework for the security and protection of personal data stored within the electoral register and other relevant government data repositories.

Requirement 12a: Fault Report

The system must send a notification to administrators if an onsite workstation is classified as faulty or inoperable. Void machines will have to be replaced by another. Back up machines should have been tested previously and tested again after replacement, to ensure the

machine is not faulty. Machines that are reported faulty will not be used again until repaired, tested and certified.

Non Functional Requirements

Requirement 1b: Voter Anonymity

Once a vote has been entered, it must be impossible to check the identity of who cast that vote, thus ensuring that votes cannot be associated with voter identity. This is to protect the security of those voting. There must be no way of verifying exactly how an individual voted. It also stops voters being able to prove to others how they voted, which would decrease the amount of vote selling, vote rigging and coercion.

Requirement 2b: Result Integrity

Results can't be tampered with or changed, no modification of results. Results should be stored locally and the machine should be non networked to avoid outside interference with the results. Results should only be accessible by administrators in each centre who in turn will pass them on to the relevant authorities.

Requirement 3b: Reliability

During voting period, the e-voting system must work 99.99% peak efficiency. Backup generators must be at every voting station to ensure unforeseen circumstances like power failures. The votes will not be stored on a single database to avoid a single point of failure. Votes will be stored at a minimum of 2 other databases to ensure votes are not lost due to any unforeseen events.

Requirement 4b: Testing

The system should be tested by prescreened security experts to an extent where there is no known way to exploit the e-voting machines. This ensures the system is at the required security level, so that election officials have confidence that the system meets all necessary criteria to allow a fair vote. The security team must ensure that the system provides standard error checking to prevent errors occurring once the system is online. When checking the database for errors, a 100% scan of the data is required, rather than selecting a sample set. The sensors in the touch screen devices should be tested prior to the election in case any have been knocked out of alignment by shock and vibration that may occur during

transport and any damaged ones should be realigned at the polling station before the start of voting.

Requirement 5b: Development Team

Before beginning development of the e-voting system, there must be checks on the personal integrity of those developing and operating the voting system. To accomplish this, those individuals should have unquestionable records, both in their previous employment and with regards to their Garda security clearance. This is done to help prevent bias and malice in the development and operation of the system, which could alter results.

Requirement 6b: System Control

More than one qualified individual should have full administrative control over the system, the administrative authority should be spread out over a group of people. Within this group of administrators there must be checks to ensure there is no chance of collusion among members. For instance in the case of an election, the administrators must not all be part of one political party or the other, as this would increase the chance of collusion and potential tampering of results. There must be no question of vested interests.

Requirement 7b: Instructions

User manuals should be provided for voters several days before election by post and online. These should be short simple leaflets with bright diagrams, using simple language, so that voters can easily follow and understand how the use the system on the day. They should be in both English and Irish to account for the two different languages used in Ireland.

Requirement 8b: Error Response

Due to the brief voting timeframe, the system should support response time for addressing severe issues of less than 5 minutes . Intensive testing should be done at the development stage to find all issues and work them out before launch. Any possible issues that could arise should be identified and all administrators should be made aware of them and how to fix them quickly on the day.

Electronic Voting System.

Used for casting and counting votes. E-voting can speed the counting of ballots, reduce the cost of paying staff to count and improve accessibility of disabled voters. A good system must perform most of these tasks while dealing with the following requirements.

E-voting which is physically supervised by a government rep located at polling stations.

Remote E-voting via the internet gives accessibility to remote/disabled voters however there are major issues regarding the integrity and security of having general/local elections.

Insecurities to avoid:
default admin password.
unpredictable machines.
inconsistent errors.

We have decided to focus on an e voting system situated in polling stations. Online voting poses too many threats as it is inherently vulnerable to outside attacks. Online e-voting might encourage the buying and selling of votes. It also opens up the issue of voting under duress as there is no guaranteed privacy. It is susceptible to DDoS, hacking (social engineering) and high congestion rates.

Requirements.

1.**User should be allowed to confirm the votes being sent into the system is what they intended.**The window should show all of the candidates voted for by the individual. The user should be given the option of going back and changing any of their votes. Once they are satisfied, they can officially submit their ballot by clicking the finish button. The only room for user input on this page will be two buttons on the bottom of the page.One button lets the user go back and change their vote,and the other button submits the vote.By clicking the “Go Back” button, the user will be brought back to the voting page and allowed to change any vote they wish to. Clicking the “Submit” button confirms the votes on a hard drive and brings the user to the “Receipt” page. After the ballot has been officially submitted, the user can no longer change their vote.(Functional).

2.**Each voting system should be easily configurable for each constituency.**
From the main menu of administrator functions,there must be a way to setup a new election each year. New elections require both a fresh database to store votes,and a new interface as viewed by the user. For inputting new candidates,there needs to be a simple GUI that will accept new names under their respective categories. For each system to be specific to their location it must be easy to setup a specific location area for each voting systems. People in Dublin should only be able to vote for candidates in the Dublin area. To reduce errors each voting box should be able to use geo-location to find out their location and set the required constituency with the required candidates to vote for in that area. System design should handle matching candidates to the database with no need for the administrator to ever look at the code.(Functional)

3.**The system should not allow a person to vote more than once.**
Each person will have to input there PPSN to verify they can vote and are of age when first entering the voting system.The user must also enter a registration number which will be sent out to each person who can vote by email.The user must also bring two forms of id to confirm that their PPSN number is valid and not someone else's.we want to have greater emphasis on vote authentication to avoid impersonation. Staff will be present to confirm each ID given by the user.
Each person who is sent a registration number will be stored on a server situated in that constituency once the person has voted this will be updated to show that they have already voted and they will be denied to vote again. A page should show up explaining to the user that they have already voted and show them how they can track their vote using a paper trail method.(Non Functional).

4.**The system software package will perform all functions with minimal delay from the time of the initial request.** The system requires a high level of performance from each component. Specifically, there must

be a guarantee that the vote information that users are confirming from the application is quickly and reliably reaching the main terminal to be counted and printed. Votes cannot be lost in the transmission of the data. This includes making sure that the main terminal can be run confidently, without fear of a crash. The hard drive holding the data in the voting machine should have some form of security and redundancy using a form of RAID configuration. When voting is finished this hard drive should be safely delivered by a member of staff to the local counting area within that constituency.(Non Functional)

5.**A simple tutorial of the system should available to the user on request by pressing a button called "help".** This tutorial should not be forced on the user or hinder their progress in casting their votes.The tutorial should be written plainly and very clearly. A button will be by each candidate's name with a number from 1 to however many people the user wants to vote. An option to not put down a candidate as an option should be given as well. All buttons will be default to None at first meaning no votes cast for anyone. If the user wants to put someone as their first choice they will put a number one in the button input. The system must be able to verify which number is associated for each candidate that the user has entered. The tutorial should be supplied in more than one language including Polish, Irish, English and Mandarin.(functional).

6.**Two Step Authentication** – For logging into vote a user is asked for their PPSN but this is insecure as the sole method of authentication. The user could be sent an authentication token through text or email which they could provide when they register to vote. This prevents vulnerabilities in the system as voters' PPSNs could be leaked or obtained by other means. Drawbacks to this feature could be that older generations may not use or not have availability of a mobile phone or email. Alternative means of communicating details for two step authentication would need to be set up for these situations.(functional)

7. **Selection of Multiple Candidates** – In many elections voters are asked for their choices ranked from first to third. Each time a voter selects a candidate the UI would have to be updated to ask for their next choice. The voter should also have the choice to submit their votes without using all their choices, this could be implemented through a “Submit” button which appears on each screen after the first choice has been made. If the user clicks submit before using all their choices it’s important that they are asked if they are sure if they want to proceed, this just safeguards against any issues with premature submissions.(Non Functional)

8. **Can only vote for a person once** – Carrying on from the previous point it’s important that each vote the voter makes is for a separate candidate, i.e. if a person votes for a certain candidate they will not be available to vote for that candidate a second time. This allows for a more even distribution of votes among parties/candidates.(Functional)

9. **Limited time to complete voting** – To prevent voters wasting time, a timer could be implemented to limit the time to complete voting. The timer interval would have to allow for decision making while voting but also not rush the voter. The only drawback of this time limit could be with people with disabilities or people unfamiliar with the interface, the interface would therefore have to be made as accessible and user-friendly as possible but extra time could be allocated to voters in such situations. This could be done by staff at the polling station or if the voter has a disability they have registered with the state, the timer could be set when verifying the PPSN against the records.(Non Functional)

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. 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)

11.**The user interface should accommodate the needs of all people including: deaf/blind/colour-blind/bilingual.**
For deaf individuals there should be clear and concise instructions (help frames) with every stage of the voting process. An option for sign language representation should be implemented in the process. Navigation of a UI is tedious for blind people as it can be unreliable and clunky. A braille option should be provided (like ATM transactions) on the side of the screens along with the option of a headset explaining the steps of voting. Colour changes to UI should be accessible to colour blind individuals. Voting process should also be included in Irish/Polish (other languages). For individuals with manual dexterity disabilities large navigation buttons will implemented. The number of help frames should be of a reasonable degree. Over use of these leads to user frustration, but after every candidate selection a box should ask the user "Are you sure?" with a "Yes/No" response. There should also be the ability to undo a step if a mistake is made.
The use of an pen should be available to older individuals to be reminiscent of older voting systems. The voter uses a pen or pencil to mark his choices (arrows/circle) on a ballot, the ballot is machine friendly and readable, allowing the vote to be stored electronically.(NON FUNCTIONAL)

12.**Provisions should be made to allow a supervisor/guardian to accompany voters who cannot operate the UI alone.**
The opportunity for a step-in appointed guardian/supervisor for the voting of individuals unable to operate the UI (illiteracy) will be allowed, given the permissions of the government reps/admins and the individual making this decision. This person must be appointed beforehand and will require the same proof of identification before operating the machine.

13.**We will be employing a Direct Recording System for voting with the inclusion of a Voter Verified Paper Audit Trail to ensure there is a record/receipt of voter's actions.**
The use of a paper trail allows transparency and it engenders trust within the stakeholders and voters.
The receipt of vote will be emailed to the voter to further ensure privacy.
We want to avoid black box voting as much as possible as we wish to ensure the confidence of the voters and stakeholders in representing their choices with accuracy. Direct Record System voting improves the speed of counting greatly. It also provides immediate feedback with issues regarding under-voting/over-voting. Voting should be saved on on a hard disk and on a smartcard issued to the voter which is then placed in a ballot box as a backup should there be a failure / data auditing on the hard disk. No voter can replace votes. Party in charge of tabulation cannot change the outcome.(FUNCTIONAL)

14.**In order to minimise the possibility of a break in voter privacy and maximise the confidentiality & integrity, we will employ data level encryption of votes using an election public key.**
In the Public-Key Algorithm there is a pair of keys. One is known to the public and the other is used to encrypt the data to be sent to another party who holds the corresponding decryption key (private key).
This methods allows the vote and the voter to remain protected from eavesdropping. It is both secure and practical
Identification and authentication:
In a multi-user system the user must identify themselves, the system will then authenticate the identity before allowing access to the system.
We'll also be implementing SSL encryption for data traffic to be sent to a database as an extra layer of security.(FUNCTIONAL)

15.**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.
By having a (set) combination of these profiles it reduces the possibility of identical matches eg.(fingerprints are not entirely unique).
Every stage should take several images to begin with to form a template of both Fingerprints, Retina and Face.
Fingerprint scan returns a map of that person's fingerprint ridges.

Retina scanning provides an analysis of the blood vessels in the back of the eye. It will use a low-intensity light to capture the image.
Face Recognition uses relative distances between facial characteristics on the face to generate a distinctive facial map.
The user will create a template for themselves to be stored on a civil database. The systems need to have a low False Match Rate to reduce the probability that the system will incorrectly match inputs. It should also record a percentage of invalid inputs. Since it is possible to have small changes to fingerprints/retinas/faces due to age/injury. There should be a threshold of correctness. The algorithm needs to determine how close to the original template the incoming input needs to be so that it can be considered a match.(FUTURE FUNCTIONAL)

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)

17. **Database records should include all pertinent information to facilitate error handling.**
Each recorded vote should include information which will allow each vote to be traced back to its point of origin, in case of inconsistencies between national and local tallies or suspected attempts to tamper with votes. The database record should include the identity of the person who cast the vote, as well as the time and location at which the vote was cast. While errors should be prevented wherever possible, this would preserve the integrity of the voter records in the event that insecurities within the system are found and exploited.

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.

19.**Voter records should be maintained independent of each individual election/referendum.**
All votes should be cross referenced with a database maintaining up to date information on all eligible voters. This would facilitate the verification of data, and would prevent less easily identifiable attempts to manipulate the voting system, such as people using the identities of the recently deceased or people who have multiple PPSN / fake identities. This should be maintained at the national level and not be in any way accessible or modifiable at the polling stations.

20. **Scalability**
Each polling station should have a central server which records and verifies all votes coming in from each individual machine. For votes encompassing a larger region (e.g. national elections), additional servers should be allocated at the regional level, such as each county having its own server to tally and verify records, and another server at the national level for final tallying and verification. As previously discussed, it's important that the data is verified at each of these levels by comparing the records with the the data stored at the polling stations' servers, preventing inconsistencies.

Functional Requirements

1) Help for blind/colour blind

Help for **colour blind or otherwise visually impaired** individuals shall be implemented in the system. In the case of colour blind people, there shall be a setting for the interface to have a colour scheme that would make the colours of the background and buttons heavily contrast each other. The system would also have a braille terminal installed below the screen display to allow individuals who are blind to navigate the interface. There shall also be the option of using a pair of headphones that would help the user to navigate the interface if they are unable to read braille. The system's screen reader shall be able to inform the user of all the options available to them on the screen within 30 seconds with the use of headphones. This system will be available to at least 99.9% of the e-voting machines that will be available around the country. This requirement would be realistic, reliable and sensible as it would allow all users of the e-voting system a chance to make their opinion heard.

2) Use PPSN to identify Voters

While anonymity is important, in order to make sure that each person registered to vote can only cast their vote once, the system will implement a machine outside of the voting booths that will be solely be used for identifying the individual who is about to enter the voting area to cast their vote. This machine will run software that will prompt the user to input their PPS Number. Once they have entered the number, they would then need to then scan an official document that states their pps number, such as a driver's license or a health insurance/medical card. The system would then update a database containing information on everyone who is registered to vote and mark this user off, so they may not vote again on any other machine. This system and database would be separate to the actual voting software. This system shall be very efficient and the user should be able to complete the identification process in the space of 1-2 minutes. This system will be available to over 99.9% of polling stations.

3) Photo identification software

The system shall support facial recognition software before entering the booth as well to add another layer of security. This will work in tandem with the verification by means of the PPS number. The process of facial recognition process shall take a maximum of 5 seconds upon scanning the user's face. This process will be virtually identical to the system that is in place in airports around the world where the user scans their passport into the system and then positions themselves in front of a camera that scans their face and matches it to the picture on their passport. This system shall be 99% accurate and available to at least 99% of the voting locations. The system shall not store the user's facial scan, merely use it to cross reference with the scanned passport picture and then be discarded. The only information that will be stored is that this user has now voted.

4) Touch Screen Interface

The system shall implement the use of a touch screen system, for user interaction. The user shall be able to select the candidate they wish to vote for by simply by selecting their name on the touch screen display. However, their vote will not be cast upon a single touch of a candidate's name. To avoid mistakes, there will be a total 3 times that the user will select the candidate's name before the vote is cast. Upon the first selection of a candidate's name, the screen shall display the candidate's party and the core values, promises of the candidate. The user will then be prompted to either cancel this selection and return to the main selection screen or to confirm that this is the candidate they would like to vote for. If the user chooses to confirm their selection, a third and final window shall pop up, asking if the user is sure that this is their final decision. If the user once again confirms, their vote shall be registered and they shall be prompted to proceed to the exit. This touch screen system shall be available for at least 99.9% of machines in the country.

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.

6) Store Results

Votes need to be stored in order to have them on record and to count them later. Each county would have both the main database to store the results and a backup database in case some fault was to occur, which can only be accessed via official eVoting machines. The backup database would only be connected to the main database for security reasons, and the main one would be connected to the national database, held in a secure government building. When a registered voter casts their vote, it is sent to both the main and backup database of its respective county and nowhere else. Only when voting has concluded will the stored voting information be passed to the national database. If a fault occurs, either in transition to or at the national database, such as votes being corrupted or only a portion of the votes being safely transferred, all votes stored in the national database for that ongoing election are discarded and each county must send their stored votes again, regardless of whether that county was part of the fault. After the results have been validated and counted, and after the election has officially ended, the results will be archived and cleared from each database, both county and national.

7) Validate Results

The validation of results system will prevent any false votes, be they intended maliciously or otherwise. To combat a false vote, say if someone votes incorrectly or puts down a candidate not up for election, a simple algorithm will run as a validation scheme, checking against all possible failures such as a fault in the system while voting, or the inclusion of an outside candidate. Another issue that would need to be addressed would be a single voter casting multiple votes. This could be a fault in the system, a mistake made by the voter, or a third party trying to secure more votes for a single candidate. In an effort to combat this, the system could query a

database which holds the “state of voting” of a registered voter, which basically indicates whether a person has voted in the ongoing election or not. If they haven’t voted, after the database has been queried, their state is changed to “voted”. If the database is queried again for the same person, it signifies that the system is trying to count multiple votes from that one person. To deal with this, the system would have to discard both votes, updating the vote count, and throw away any subsequent attempts to register a vote to that individual, as there would be no way to identify the official vote.

8) Calculate Results

The calculation of results would be done on three separate machines running three separate counting algorithms. These machines would not be connected in any way physically, preventing an attack on one machine affecting all three. The three separate algorithms would be for detecting a fault in the software, as different results would be obtained. If the result from two of the machines is different than that of the third, then all three machines are inspected and fixes are applied where necessary. After the machines are thoroughly inspected, the count is redone. The validation of the votes will already have been done prior to vote counting, so there would be no need for extra validation at this point. The counting of the votes would be done three separate times on each machine, and the result is only accepted as final when all three machines give the same result all three times. After an official result has been accepted, that result is stored in the national database until an announcement has been made, after which the result is archived along with the votes.

9) Voters can review their vote at the end

This requirement allows voters to see what they have chosen when they are about to finish voting. The voters can see the candidates that they have picked and the number choice they have given to each candidate. As well as this, voters will also be allowed to confirm their email address/phone number or a receipt to guarantee the vote has gone through. This will reduce the errors a voter may cause and allows them to rectify any mistakes easily. The

main reason for this requirement is to reduce errors. Sadly, this requirement is not exactly measurable we can if the voters made a mistake or not but this is ok as this requirement does not need to be measured. The goal of reducing errors is attainable as we supply voters to change their minds if needs be. Allowing voters to see what they have chosen and make sure all contact details are correct will almost insure no errors. Sadly, reducing errors to zero is not realistic as human error is a factor. We cannot completely reduce the possibility of an error for them but we can make it as little as possible and help correct their mistakes. The voters need this requirement as they are prone to make mistakes and need a way to rectify them. Our assumption is that errors will be made but we cannot completely cut out errors. I would count this as high priority especially for as something serious as someone's right to vote, they should not be locked into a vote they do not want to cast.

10)

The voter will receive an email/text/paper receipt confirmation of their vote

We want to make sure the voter knows that their vote has gone through and there were no errors in the sending of the vote to the server. We will provide this service by email preferably if not we will take a phone number. If the voter has neither of these, for example the elderly, a paper receipt will be issued. Of course, the voter can choose to have all three options if they desire. We could almost certainly measure the amount of confirmations sent. The server would be able to be able to keep track of the emails, mobile numbers and receipts sent or printed. This can be done using a simple counter and a method that adds all the counters together. Is it achievable that these methods of confirmation will work? It is achievable that at least one of these methods will work. Realistically there is a possibility that they may all fail at once but the probability of the is significantly low. All we can do is offer the others as backups and try to make the server as stable as possible. The users require this as they will appreciate and need a confirmation so they know the system is working. Assumptions will be made that at least one of these will suit the voters. This requirement is important as it will place confidence in the system and allow users to know their vote counts!

11)

A Description of The politicians who are up for election in that constituency

This is a functional requirement for the E-Voting system .This is a characteristic which is necessary for the system as it informs the voters of the main policies of the politicians who are located in this particular constituency and their main objectives which they want to achieve and implement before the end of their term .These features will allow and educate the voters on who they should vote for as they will be well informed on what party and politician they feel they should vote for .This feature will also enable the politicians to communicate and interact with the people the hope will elect them as they will be able to inform the voters on how they expect their changes and new introductions should impact them for the better . This feature of the system will be available to the voters as a drop down menu underneath where they can pick their preference for who the wish to vote for . This makes the system more user friendly as it allows the voter to easily learn the policies of the politician without having to navigate through difficult interfaces to observe the policies. This requirement also coincides with the requirement to aid the deaf as they will be able to listen to the policies when they click on the menu.This in my opinion is a SMART requirement as it is both attainable and realistic.

12)

Rectifying wrong candidate choice

Stated before people are bound to make mistakes. This requirement allows the voter to change their choice of candidate while looking at the ballot sheet or when they are looking at their review and confirming contact details. The voters can mend any wrong placed number on any candidate allowing them to change their mind. We cannot measure this as we do not know when a mistake has been made! We do not need to necessarily measure this just give the voter the opportunity to correct their mistake or change their mind! Reducing the errors is possible with this requirement as it easily allows voters to change their minds. There is a lower chance of mistakes being

made because of it. Realistically we cannot completely cut out errors as we are dealing with humans who are prone to errors. We can only give them the tools to correct their mistakes and to make sure they are making the right choice. Voters will require this as they are prone to making mistakes and need a way to rectify them. The assumption is that mistakes will be made we cannot reduce them to zero just make them harder to make and easier to correct. There is a relationship here between this and them being able to review their vote. Both requirements are there to help reduce errors that can occur in an easy and user-friendly way.

Non-Functional Requirements

1) Making the system more reliable so it does not crash

This E-voting system should be able to deal with the millions of packets of data being submitted by the voters around the country without crashing. For this to happen the system would have to be thoroughly tested prior to being made available for the election. The system should also be efficient for the voters despite the number of people trying to use it. The system should not slow down with the sheer amount traffic passing through it. On the off chance that the system should crash a back-up should be made available so the voters who have been affected will not have to begin the process again and they can just recommence from the point they had reached prior to the system crashing. The system should guarantee 99.99% that the system will not crash. I believe this is a SMART requirement for this E-voting system as it is an attainable and reliable requirement.

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. If not, we can identify if there is a fault or problem easily as there will be a timeout. This will allow us to resend the packet or deal with it if the problem is bigger such as a server crash. We can measure this requirement quite easily as we

can monitor the number of packets being sent to the server. We could also estimate the amount of people voting at one time using the measured packets. It is attainable that most packets will make it to the server but realistically we are limited. Such limitations are bandwidths, congestion and timeouts could mean lose in packets. We cannot control realistically but it is attainable to minimise the possibility of these happening. As in using multiple servers, minimising packet sizes and offering the best possible bandwidth. Designers need this as it assures a QoS. We have the assumptions that connections are bound to fail but we have measures in place that can rectify any mishaps. There is a relation here between this requirement and the requirement of no central server. Both deal with the possibility high volumes of traffic as well as the making sure the vote makes it to the server. This is a critical requirement as it insures QoS for the voters (even if they don't know it's happening) and the designers as it helps identify problems.

3) A Signature file for decrypting the results submitted from the e-voting stations

The signature file would be used for accessing the data from the individual databases containing the voting results from each constituency. The signature file will provide security for the data as any entity who would try to obtain the data illegally would be unable to do so as they would also need the signature file to be able to enter the file containing the voting results of the election. The signature file will also enable the entity who own the data to analyse the voting results which will allow them to determine the popularity of individual politicians and parties in the different constituencies and evaluate the voting patterns throughout the country. The signature file will also redundancy for processing and determining the eventual results of the election as it will allow for the manual counting of the poll results if the program for the calculation of the was to have a bug which had not been realised while testing the system. This signature file is also related to the calculation of results which is a functional requirement for this system as it is a mechanism which provides the ability to double check the results of voting from the polling stations. Due to these characteristics I believe that this is a SMART requirement for this E-voting system.

4) No central server (core of network). Voting machines at the edge

The server will be placed offsite of the voting centre. The voting machines will contact the server via protocols as they will be placed at the edge of the network. This will provide security as hackers will find it hard to gain access to the server. The TCP connection as stated in another requirement will stop the hackers from flooding the server. The voting machines being at the edge and not near the core will stop any access that should not be allowed. This will help guarantee a secure election. We can measure how long it takes to connect to the server and any attacks that may occur. It is attainable to get the servers offsite but realistically they will not be completely secure and may fail. Causing traffic issues a backup would be needed to help stop this problem from occurring. We can only minimise this problem not guarantee it won't happen as that would be unrealistic. Designers need this requirement to help with security and to help with traffic control. We assume people will try to hack and make it harder for them to do so. We also assume that there will be a high volume of traffic and put measures in to make sure there is a backup to help. As stated there is a relationship between this requirement and the TCP connection as both help with security and flow of traffic. I would count this a very high priority as for this kind of system you can never be too careful especially where security is concerned.

5) Problems with Identification of Disfigured People

A problem with the facial recognition software is that people who have been in a severe incident or who have a disfigured face may not be recognisable by the software. To combat this, such an individual would have to officially register to obtain a special identification card that, when used in an eVoting station, would bypass the facial recognition step in the other implementation. To get around anybody simply stealing one of these identification cards, the owner of the card, when registering for it, would have to scan in their fingerprint. After they use the card in the eVoting station, instead of being prompted with the facial recognition software, they are presented with a fingerprint scanner as the next level of security. This fingerprint scanner would be connected to a separate database which holds the information about the fingerprint and who it belongs to, so a simple

query would allow or deny access to the machine. This implementation would be available in 50% of the voting stations in every county.

6) A separate voting machine for the physically disabled

A number of additional machines would be made available at the polling stations throughout the country to aid the physically disabled to vote in a way that suits and is comfortable for them. For a blind person the system should be made available to be comprehended with both a screen reader or an optacon. These two options would allow a blind person to complete their voting in a way that is easy for them and will allow their opinion be valued. This in my opinion is a SMART requirement for the system as it is specific, maintainable and reliable. This feature is also linked to a functional requirement of this E-voting system to provide help for the blind/colour-blind who wish to take part in the voting.

7) Separate Machine for People with No Hands

To accommodate registered voters who have either lost their hands or lost use of their hands, a separate machine would be provided for them. The screen which holds all the information about voting for candidates, information on those candidates, and the actual voting itself will be at face level for ease of viewing. The controls for navigating the screen will be at ground level, so the voter can use their feet. The controls to vote will not be a touch screen system – like the other implementation – as it would be easier for the voter to make mistakes if they are using their feet as opposed to their hands. On the control board there will be the usual buttons for direction, a back button, and an enter button when choosing options. Just like the touch screen implementation, however, the voter will be prompted three times to confirm their choice, to avoid any error. This implementation will be used in 50% of voting stations in every county.

8) A Mobile Voting Station For people in Rural areas

A mobile voting station would provide both easy access for older people who cannot drive to vote and also cut down the cost of transporting and

setting up more polling stations throughout the country. The mobile voting stations would be utilised in rural areas across the country. The mobile stations would be available between certain hours during the day on which the voting is to take place. The station would then move to the next area to enable to vote. This would severely reduce the cost of setting up more polling stations in certain areas around the country. Rather than setting up several stations in close proximity to each other the mobile voting station would travel between these areas throughout the day of the voting to allow these people to participate in the voting and make their preference be counted. This requirement is in my opinion measurable, attainable and realistic which therefore makes this a smart requirement which is a reasonable requirement for an E-voting system.

All work was shared equally among the group. Each member got 5 requirements each and each member helped to put all requirements into one file.

Outline of system:

This is specifications requirements for a national e-voting system for Ireland. The registration process will be carried out with databases to record eligible voters allow people to register online. There will be lightweight devices set up in the place of polling stations that can store encrypted voting information which will all be connected via ethernet to a storage device. The system will be able to manage both elections and referenda. To keep track of who has voted we will use a combination of 2 tables. The device can scan passports, faces and fingerprints to verify the identity of candidates to ensure they are entitled to vote. The device should be as user-friendly and intuitive as possible to avoid complications for people casting their votes. Once the votes are cast, the system shall count and store the votes for 6 months, for the possibility of a recount etc.

Requirements:

Functional

1. Encryption
2. Storage of Votes
3. Registration
4. Local Network
5. Voting Formats
6. Vote Counting
7. Identification
8. Blank Vote
9. Creation of Database and Tables
10. Querying Database
11. Removing Voters
12. Backups

Non-Functional

13. Online Registration
14. Candidate Description
15. Simple GUI
16. Text-to-Speech
17. Clarity
18. Search Bar
19. Multiple Languages
20. Colour Coding
21. Device Design
22. Guided Tips
23. Double Confirmation

1) Encryption

The system shall support the encryption of votes. The implementation would be easy as there are readily available encryption services available. The system will have to encrypt all votes in order to keep anonymity. The encryption would take place in the voting hall. The function could be measured in how secure it is by how the type of encryption it uses. The system shall implement Advanced Encryption Standard as it could take up to years to decrypt. This is a must have function of the system as it would pose a major security risk if there is a breach. Unencrypted votes could lead to an undemocratic voting process as users would not have the anonymity that a current voting system provides

2) Storage of Votes

The system shall use a local network to connect the voting stations in a polling station to the database.
The system shall support the storage of votes. This is an achievable function as the votes would be stored on a storage device. The system shall implement of the storage of the votes using the vote database. The system would then store this database on a storage device. 100% of the votes must be stored with no corruption. The state is required to store the votes for a period of six months after the election. This is a must have function for the system as it is required for a democratic election. Without this service the system could to lead to unfair voting processes.

3) Registration

The system shall support user registration. This is an achievable service as an implementation could be easily made using a database of registered users and a database of eligible users. This is needed by the requirement of the need for a database of registered users. When a user registers the system will check if they are in the eligible users who can register and if the user is already in the registered users database. The user's basic details and PPS number will be on the eligible users database. Without this function users who cannot legally vote could vote.

4) Local Network

As we are using a local ethernet connection, the difficulty of this being implemented depends on the amount of voting stations in a venue. 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. However, this method is more secure than transmitting the information packets through wi-fi to the database where they can be more easily intercepted.

This part of the architecture is an absolute must to be implemented, as we need a secure way of transferring information from voting machines to our database. Without it information could be lost, corrupted or tampered with.

5) Voting Formats

The system shall support different voting formats. This is an achievable function as the system could change the input using software. The system shall implement a digital user interface which will allow the voting system to be changed. The system shall implement the three voting systems currently that take place in Ireland. This is a should have function as it would make the system more reusable but could be implemented later if there is a time constraint. This function could be measured in the ease of implementation of new formats. This function would allow the reuse of the machine for other voting processes which would allow the machine to be used more effectively

6) Vote Counting

This would be very easy to implement as our database has been set up, connected to the voting machines and secured. All we would have to do is when a vote is cast, we would update the total votes column for the selected candidate that has been voted for in the SQL table.

This is a must for the system as without it working properly we will not be able to get the total votes cast for each candidate. The system must be ready to receive these updates consistently from up to 30 voting machines.

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 (almost) every citizen in the country will readily have a passport available. Missing or stolen passports are also cancelled once the owner has realised it is missing, rendering it useless for voting. To combat the possibility of people stealing passports in order to forge a vote, a face and/or fingerprint scanner will also be implemented. In the case of somebody not being able to scan their face/finger (e.g. in the case of disfigurement), an attendee can verify the person's identity prior to the vote. These softwares should also easily be available COTS. The success of this system can be measured by the rate of failure in facial/finger print recognition. This function is required to maintain the integrity of the voting system. The system must not allow people to vote for anyone but themselves.

8) Blank Vote

The system shall provide a blank vote/none of the above option. It is important to allow candidates to cast a "none of the above" vote as it is an option in the current system to scratch your vote. This is a very basic feature to implement but it's important that it's not overlooked as there is a big

difference between people not casting a vote and people casting a blank vote. For this reason, it is vital for the system to provide a “blank vote” or “no vote” option.

9) Creation of Databases and Tables

The system shall create a database with 2 tables upon starting up. One will be a new empty table that will hold a record of which candidate/option was voted. The other will be a table that holds the details of all the people that can vote at that particular polling station. This database will take information from the database of people registered to vote. It should be able to store up to 10000 records while maintaining a reasonable efficiency. Both tables should set up without failure 100% of the time. There should be no major difficulties in setting up a database and filling in a table. This is a high priority specification as it is required by many other function of the system. This is required by the organizers of the vote as they will need a way of recording everyone’s votes and who has voted.

10) Querying Database

The system must query the table in the database that holds a record of people that are registered to vote at that particular polling station. This is done after the system identifies the voter. If they are in the table then the voter continues with the voting process. If the query fails then they are either notified that they are not registered to vote at this station or they have voted already. This is a high priority function as it prevents voters from submitting votes multiple times or voting at multiple stations. This would be simple to implement as it would only require a simple table query. The system should be able to support multiple queries as there will be up to 20 voting devices connected to the main database simultaneously. It is the people running each polling station that require this to help deal with any mistakes on their part.

11) Removing Users

The system should remove the information of a voter from the local database table of registered voters upon the completion of the voting process. The system should be able to handle up to 10 voting devices to alter the table simultaneously. This should be simple to implement as the system will already know the identity of the user and location in the table at this stage. This is a high priority feature as it is the only way to record a voter has voted without tying the data to their vote in some way for example an entry into a who has voted table and an entry into the votes table having the same timestamp. This is needed by the organizers of the vote to prevent people voting multiple times in a single election.

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. This is not a necessary function as the system can run fine without it but it is something that should be implemented. Local hosts of polling stations would benefit from this features the most as it prevents any unnecessary hassle from trying to get people to come back and resubmit their votes.

13) Online Registration

They system should allow people to register online to vote. The system should allow for people to apply for registration online. Online applications can be reviewed before approval so it should be very easy to prevent accidental/unauthorised applications. This should ease the process of becoming eligible to vote and could lower the number of citizens who don't vote because they are not registered, in particular people coming of age to vote who are yet to register. This is not a mandatory requirement but could improve the voting system in the future by reducing abstentions.

14) Candidate Description

The system could have a candidate choice description.

Upon a voter selecting a candidate, their initial details box could expand to show some of their policies and past accomplishments in politics. This would help voters who are still undecided or on the fence between multiple candidates to find the candidate that is suitable to their own voting interests.

The drawback however is this would take a considerable amount of time to implement, as we would have to have a description for hundreds of candidates across the country. Listing individual policies and goals is very time consuming, and so while this could be implemented, it is not a major concern and would be left till later when major functions are completed.

15) Simple GUI

The system shall support a simple GUI. This is an achievable function as a simple GUI design could be implemented using programming libraries readily available. This is a requirement for the user as it makes their experience much easier. This function should be measured by getting test users to test the system and fill out a survey. Large buttons for user input would allow visually impaired users to use the system. This is a should have as it would make the process easier for users but

could be changed at a later time as the system would function without a simple GUI. This would allow users who are not used to using technology to use the system easily.

16) Text-to-Speech

Text to speech to dictate what is on the screen/Braille buttons.

The voting machine should have speech to text recognition and Braille buttons included next to the regular user interface.

This could prove a challenge to implement as we would have to create specially tailored software and hardware for the inclusion of this requirement. While it is not a must to have, we should still implement it for usability standards.

Some users will have disabilities that require them to use these, and we must accommodate their needs.

17) Clarity

Only show what is needed to vote, no unnecessary options.

The voting machine's interface must be clear and concise, and must not show too many details and options that may confuse users.

As we have many features on our system, we must use UI usability standards to allow users to easily navigate our system and know where they are on the system.

18) Search Bar

The system could provide a search bar for candidates.

The voting machine could have a search bar at the top of the screen to allow voters to search by candidate name, or by party.

This would not be too difficult to implement as we would only need a simple search method in the voting machine's software to complete the searches.

This allows users to quickly search and select candidates that they already know they want to vote for, rather than scrolling through the full list of candidates. It is not a necessity though, and is something the system could have if we have extra time to implement it.

19) Multiple Languages

The system should support multiple languages. It is required that public services are provided through at least both English and Irish, therefore the system must cater to both languages. In the interest of usability, the service could be provided through several world languages. However, this is not a necessity and would require a lot of time to error-check and validate, so it could be left for future implementations.

20) Colour Coding

The system could have colour coding for each party.

The voting machine could display different background colours around the box for each candidate, signifying the colour of their party. This would not be too difficult to implement as we will already display which party the candidate stands for, and so we could implement the distinct colours using ID's for each party, which the candidate will have.

This will help usability as voters are already familiar with party colours. For example, red for Labour or white for Independents. However, since we will already be displaying the candidate's party next to their name, this feature is not too important to implement, and so is something the system could have if there is extra time to implement it.

21) Device Design

The system shall support a small device. This is a realistic goal as small devices are already available which can be designed to implement the system. The system shall implement the system a small device with a touch screen. The touch screen would take the user's input. This is a could have as the machines physical design will only affect small differences and overhead cost for the system. This is a requirement for the state as it makes overhead costs lower. A small design would make storage and transport costs cheaper.

22) Guided Tips

The system could provide guided tips for the voters to help them get through the voting process. These would just be a short set of instruction shown on the screen as the voter progresses through the process. These tips should be objective and contain no influence towards a voting option. Providing accurate and concise tips could be difficult to implement and require a lot of testing to make sure there is no confusion created. This feature is not important to the complete system but it would be a useful to have implemented. Both voters and local polling station organizers would benefit from this as it would greatly reduce the number of people seeking the help of the organizers and reduce pressure during rushes of voters.

23) Double Confirmation

The system should have double confirmation for all choices made by the voter. When the voter selects the option they would like to vote for, a message box should show up asking to confirm the choice. When the voter goes to finish their vote, a final confirmation box should show up letting them know that there is no changing it after this, and showing them what option(s) they have selected. This should be an easy implementation as it shouldn't affect or rely on any other functions. This is not a feature that is required by the system to function but is a should have. This is to prevent people from making any mistakes in selecting the wrong option or finishing too early. This benefits both the voters and the local polling station organizers as it prevents a lot of complaints that the organizers would have to deal with.

The work was divided equally

between all members of the team.

Voting is one of the primary foundations of democracy. Previous legislation and non-electronic voting systems have been developed over the years to ensure that the requirements required for democratic elections are met. There are a number of technological products and programs already available on the market. Technology usually moves at a pace faster than the legal system does. However, technological evolution should always be pursued as a means to improve human life. In this respect, all technological development, should be carefully reviewed with an eye towards determining their contribution to the improvement of society. Any attempt to introduce e-voting will have to address a series of complex constitutional and legal issues.
We have attempted to address some of the key issues through this set of requirements. If implemented into any Voting system used should protect the integrity of the democratic process and ensure the wider trust in the system.

Functional Requirements

1: Voters Log in
The system must provide an interface that can be accessed from any Web Browser. The interface must content a “Login” button that if it's clicked on would display a log in form which will ask the voter to enter their address, username, password and election code given by the government previously. After accessing the interface, the voter should pass the iris lector implemented by showing the eyes to the camera of their computer. If the iris lector cannot recognize the voter, the police will be sent an immediate message.

2: Multiple Vote Restriction
The system should send the information for the login attempt over the server where it can check whether the user has voted or not. When the system receives an attempt to log into the system with a username that has already voted, it should direct the user to a page indicating this and deny their login attempt.

3: Voters help
The system must provide a “help” button that once clicked on it displays a list of most common questions and some contact information in case the user needs personalized assistance. This contact information must contain desk assistants phone numbers and their skype usernames which clicked on will immediately realize the call.

4: Candidates visualization
Voter must be able to select a candidate from candidate list by mouse clicking. When the voter clicks on the candidate's profile link his profile page will be displayed. In this page by clicking the "CV" link the voter can reach the general information about the candidate and by clicking the "promises" link voter can view the candidate´s election Campaign.

5: Election results
Once the voter has voted should be able to see how the election is going. He clicks on the "show election results" button and the system displays the required information according the actual content of the election database.

6: Mobility: The voter should not be restricted to cast his ballot at a single poll-site at his home precinct. They shall be able to vote from any poll-site within the nation.

Non-Functional

1:Voters must be able to prove their identity. Voters must do this before they cast their vote. Voters must bring photo ID and their proof of their registration to vote. A fully qualified member of election staff must identify a voter from photo ID and check their proof of registration to vote against the Registrar of Voters. Voters must not be allowed cast their vote until their proof of identity and registration to vote is verified.

2:Voters should not be identifiable from their votes. All identification of voter should be carried out before they use the e-voting system. The voter should not be asked for any unique identifier when casting their vote. Once a vote is cast it should not contain any information relating back to the individual Voter.

3:Voters should not be physically visible to any other voters when they are casting their vote. A voter should not be monitored when casting their vote. A voter's vote should not be viewable to any other party when casting their Vote.

4:The e-voting system should be tested by security experts to ensure it is secure from denial of service attacks and malicious code. These security experts must not be a part of any government organisation. The security experts must not be a member of any political party. The e-voting system should be tested for malicious code at 2 hour intervals throughout the election day. If malicious code is found voting should be suspended and all votes from the previous 2-hours should be rechecked for validity. Administrators operating the system should be thoroughly vetted. Administrators should not have any criminal background or previous Conviction.

5:Administrators must not be part of any government organisation. Administrators must not be a member of any political party.All administrative operations must be carried out by an authorised administrator. When operating the e-voting system administrators must be asked for proof of authorisation. Administrators must each have their own unique proof of authorisation. Administrators must log every operation they carry out on the e-voting system.

6:The e-voting system must be operational by people who are differently abled. For example, a blind person must be able to operate the system using audio queues (earcons, spearcons, guided walk through). For the sake of anonymity, the user must be able to connect headphones.

7:The operation of the e-voting system should not be time based. A user should have all the time they need to decide on who they vote. This improves usability for those with issues reading the text and also for allows the user to make up their mind without feeling rushed.

8:The e-voting system must prevent user errors. A user should be alerted with a dialogue box if they are about to make an irreversible decision such as confirming their vote for a certain party.

9:The system should reduce short-term memory load. Displays must be kept consistent as a user moves through the system. If a user can select multiple candidates to vote for (like in the Irish voting system), a list of the user's already selected candidates should be viewable.

10:The voting system should be easy to understand for a new user. Options should be easily understood and in no way confusing to the user. The system should have a ~0% error rate.

11:The e-voting system should be operational 99.9% of the time. In the event of the e-voting system being non-operational voting should be suspended and voters should be informed of when voting will recommence. If the e-voting system is non-operational for an extended period of time the election day should be re-scheduled and all previous votes should be Disqualified.

12:Votes should not be able to be tampered with after they are cast. Counting of votes should be carried out by qualified staff. Qualified staff must not be a member of any political party. Qualified staff must not be a member of any government organisation. Qualified staff must be observed by a third party when counted the votes. The e-voting machines should be tested for tampering and malicious code before votes are counted. All votes should be checked at least three times.

13:The e-voting system should not be able to be tampered with during operation. Voters should not be able to access any non-voting operations when casting their vote. Any non-voting operations should be require a proof of authorisation.

16:The design implementation and testing processes implemented in the system must be well documented and easily accessed when required so that voter confidence in the system can be ensured.

17: Any implementation of the system must be affordable and efficient.

18: The core of the system, especially the vote-casting equipment, shall be open source, so that it can allow external inspection and auditing.

19: The administrative authority shall not rest with a single entity. The authority shall be distributed among multiple administrators, who are known not to collude among themselves (e.g., different political parties).

20: The system must not be a barrier to voters i.e it must but simple enough that anyone can operate it irrespective of the experience and comfort levels with technology.

Contributions
Everyone worked together as a group.

Requirements for an Irish E-Voting system

R0: A database containing the personal information of all those registered to vote needs to be created. The E-Mail addresses of the person should be included in this database.

R1: Where E-Mail addresses have been supplied, the system should be able to read E-Mail addresses from the database, and E-Mail them a key to use with the system. This will ensure only those registered can take part in voting.

R2: Each key that is E-Mailed should be unique for each person registered, ensuring the integrity of the vote is not compromised. The key should also be rendered useless once entered so that no one can vote more than once.

R3: The system should have a way of being time activated, for example it should open for voting at 12AM and close at 11:59PM. It should also have a way of counting votes once the voting has closed, and vote counters should be able to access this figure and add it to non-online votes

R4: There should be a web-page for choosing the candidates you want to vote for. This web-page should be as accessible as possible, following principles from Usability Engineering such as Fitt's Law. This web-page should display each candidate with a drop down menu to choose which preference the candidate is.

R5: There should be a separate web-page for the end of the vote which will show any interested users the results of the online vote only. The online vote will probably be counted quicker than the non-online vote so the results would be available sooner.

R6: In extension of R1, an algorithm will be needed in order to generate random keys. It could use some form of hashing in order to generate the keys.

R7: There should be immediate feedback for the user when voting. IE, if they try to submit their vote without selecting at least one candidate then it should not advance the web-page and a message should pop-up telling the user why they cannot submit their vote. If the user submits there should be a web-page thanking the user for their vote, so they know it has been counted.

R8: The server should be extensively tested before being made publically available. This will ensure reliability of the system and give everyone a fair chance at voting.

R9: The system should be basic but in-depth so that any person should be able to use it if they wish, IE both a computer scientist and someone who uses the internet once a month should be able to cast their votes.

R10: A database is needed in order to keep track of all the votes cast. Each time a vote is cast the database should be updated to include the new number of votes each candidate has.

R11: There should be a system to back up any data as a fail-safe against system failures. This way if the system goes down votes will still be counted and the vote remains valid.

R12: If someone decides they want to vote via the E-System then the system should support E-Mail addresses being added after voting starts. This means if someone registered is unable to make it to a physical voting station for any reason they still have the opportunity to have their voice heard.

R13: Any updates or changes to the system should be extensively documented and publically released. This ensures transparency and would stop any potential claims of votes being fixed by the system administrators.

R14: As voting is a relatively fast process there should be a large team of administrators so that if there are issues with the server they can be remedied as fast as possible and keeps the voting process going on a near constant basis.

R15: Voter privacy must be assured at all times. This will maintain the integrity of the election and dispel any worries of voter intimidation or bribing, as if the address and names of voters are public then there is no guarantee neither has taken place.

R16: A receipt should be given to the voter, either email or paper with a unique id for their vote but keeping the voters personal data completely anonymous. This would function as a paper trail, allowing to detect possible election fraud and also act as a output to the voter, confirming their vote. Voters should then be able to check if their vote is present in the system in an anonymous way.

R17: When a user votes, a prompt should appear and inform the voter of their current choices and allow the voter to change their vote if needed to prevent voters from accidentally casting a vote that wasn't intended.

R18: The system must prevent auditors from changing any data, or accessing any voter's personal data. System logs should be created that cannot be modified, to track any admin or auditors use of the voting systems data.

R19: There should be accurate data supplied with the system to allow even those who have not looked at the manifestos of parties to make an informed decision when voting. This could be as simple as 4 or 5 bullet points under each candidate outlining the main aims of their political party.

Description of the System

The system is an internet voting system, encompassing voting, vote counting, and voter verification. The system allows users with valid permissions to vote over the internet from their own machines at home and abroad. Those who would be unable to vote that way will be accommodated using machines located at polling stations. The system stores these votes in multiple ways to improve redundancy and reduce the chance of losing votes. The system then counts the votes automatically, but includes tools for manual verification purposes. The system is capable of handling the different voting styles used in general elections, local elections, presidential elections, and referenda.

Components

- Web application
- Native applications (iOS, Android)
- Polling stations
- Machines at polling stations
- Voters' computers
- Voters
- Candidates
- Admin staff

List of Requirements

Functional Requirements

1. It must not be possible to tell what/who any specific voter has voted for.
    - Rationale: The secrecy of the ballot must be maintained, to prevent altering of votes by intimidation, blackmail, or vote buying.
2. Voters may vote from a web browser using the voting web application or from native applications on iOS and Android devices.
    - Rationale: Permitting voting via the web and via mobile devices makes it easy for voters to vote. It also aids accessibility, as voters may use their own devices and accommodations.
3. Voters may also vote from dedicated machines in polling stations, which use the web application.
    - Rationale: Some voters may not have their own devices, and should still be able to vote. Using the web application for these machines makes the system more consistent and easier to deploy.
4. Every vote will be stored in at least 3 locations and 2 different storage media.
    - Rationale: Records at any server may be incorrect due to (for example) data corruption, vote tampering, or power loss. By storing votes redundantly, these errors can be tolerated.
5. Where records from multiple servers disagree, the majority consensus shall be accepted as correct.
    - Rationale: If there is a majority consensus, that is more likely to be correct than incorrect.
6. The voting web application will send votes to one or more verification servers, which will verify that the votes are legitimate and that the voter is entitled to vote.
    - Rationale: Allowing voting via the internet means that all data must be verified on the server side. Having the option of multiple verification servers allows for load balancing and for continued functioning of the system if some servers crash.
7. The system must be able to accept legitimate votes from across the world.
    - Rationale: It should be possible for people who are entitled to vote to vote, even if they are abroad when voting is happening.
8. The internet based system should be capable of sustaining 30% of the voting population voting simultaneously without failure.

    - Rationale: There are likely to be peak voting times during the election, and the system should cope with peak traffic.
9. The system must be capable of fairly calculating which votes, in the case of a General Election style vote, will be redistributed as part of a surplus of an elected choice.
    - Rationale: The voting system should accommodate general elections, as well as other kinds of election.
10. If multiple votes are received for a given voter, only the latest vote will be counted.
    - Rationale: Voters should be allowed to change their minds during the election. This also allow voters to correct mistaken votes or accidentally spoiled votes.
11. For a vote to be considered valid, the voter must demonstrate something they know (e.g. a password), something they have (e.g. a government-issued smart card), and a biometric identifier (e.g. their fingerprint).
    - Rationale: Multi-factor security makes it difficult to steal someone's vote. Prevention of voter fraud is extremely important in a voting system.
12. A voter will be presented with a set of options (e.g. a yes/no question for a referendum, or a specific candidate for a general election) and for each, shall be able to record an answer from a set of available answers ("yes" and "no" in the case of a referendum, or a unique preference number in the case of a general election), or record no answer.
    - Rationale: Voters should be able to submit votes that follow the format for the election at hand. Voters should also be able to record a spoiled ballot (in this case, an empty one), as a protest or for other reasons.
13. The system has a voting register, which identifies who is entitled to vote. The system will consult this register to determine whether a voter is entitled to vote.
    - Rationale: There must be some consultable record of which identities are entitled to vote.
14. Voters may register to vote, and if they are entitled to vote this process will add their identities to the voting register.
    - Rationale: New voters will become eligible over time, and there needs to be a process for them to be added to the voting register.
15. Machines being used to vote via either the web application or the native applications must be able to provide biometric identifiers to the server.
    - Rationale: Verification must take place on the server side, and biometric authentication is required by point 10. Votes from voters' own machines should be as trustworthy as votes from machines at polling stations, and vice-versa.

Non-Functional Requirements

16. Votes should take under 4 minutes to complete assuming all decisions in regard to the vote are decided before beginning.
    - Rationale: Voting should not be too time-consuming, as that may prevent some people from voting and reduce effective turnout.
17. The voting web application and native applications must conform to the Web Content Accessibility Guidelines version 2.1, achieving level AA conformance.
    - Rationale: Voting should be accessible to people with disabilities, to ensure that their needs and rights are respected and upheld by government, and empower them to define how those things are done.
18. The system should be secure enough that the time taken to hack it is greater than the duration of the election.
    - Rationale: It should be difficult to compromise the voting system, as doing so would ruin the integrity of the election.
19. The voting web application must be functional on 95% of the userbase's browsers.
    - Rationale: The web application should be accessible to as many people as possible, but it may not be possible to support all browsers that voters use. Voters with unsupported browsers will still be able to use the machines at polling stations.
20. The system must be available to users for 99.9% of the election time.
    - Rationale: The voting system should be as close to always being accessible as possible, as voters may have only a small window of time in which they are free to vote.
21. The systems must boot and be ready to use in under 3 minutes.
    - Rationale: In case of errors, it may be required to reboot the voting system. To minimise impact on voters, this should take as little time as possible.
22. It should be possible to examine voting records to verify a vote count.
    - Rationale: If there are suspicions that a final vote count is incorrect, it should be possible to verify whether or not it is correct.
23. Newly-registered voters will be added to the voting register within a week of receipt of their registration.
    - Rationale: Voters who have just become eligible to vote should be able to vote as soon as possible, so that they don't miss any opportunities to vote while their details are being processed.

1. User-Interface: The system needs a user-friendly user-interface. It will not disadvantage any candidate while displaying the choices (e.g., having some candidates off screen, and requiring the user voting to scroll down, in order to see and vote for them).

2. Support for Disabled Voters: The system needs to cater for the needs of physically challenged voters (e.g., Blind users should be able to vote, the system should also be colour blind friendly).

3. Eligibility: The system should check the voting eligibility of the voter, and only authorized voters who are registered members with a citizenship, should be able to vote.

4. Confirmation: The voter should be able to confirm how exactly his vote is being cast and will be given a chance to modify his vote before he commits it, in order to prevent wrongful selections.

5. No Under/ Over voting: The votes will be prevented from selecting more than one candidate, and also prevented from selecting no candidates to vote for, resulting in eliminating invalid votes.

6. Convenience: The system will allow the voter to cast their votes without prior knowledge of the voting system. The system should not require any special skills in order for the voter to cast their votes, as the complexity of the system would result in less valid votes.

7. Anonymity: Ensures that the votes must not be connected in any way to the voter identity, and can not be reverse engineered in order to find the identity of the voters choices.

8. One Session Vote: The voter needs to be able to complete the vote in only one session, by logging in, submitting the vote, then logging out, without the need to login multiple times.

9. Accurate Number of Votes: The system must record every vote properly, avoid vote duplication and must not round up the number of votes for towns/counties.

10. Equal Treatment of All Votes: The system must treat every vote as equally important and must not prioritise some votes over the others (eg. a vote from a politician must carry same weight as vote from a factory worker).

11. Support for Different Votings: The system needs to be designed in a way that allows it to be optimised for different ballot types such as voting for the President of ROI, Referendums and Members of the Dáil Éireann.

12. Network Infrastructure: The system requires a robust network to function properly. It needs to be able to support more than one million voters at the same time as well as being resistant to attacks such as flooding.

13. Bilingual: The system needs to support both English and Irish languages, as under the Constitution of Ireland, both are recognised as official languages of the Republic of Ireland.

14. Tutorial/Help: The system needs to possess the ability to educate the voter how to use the voting system and be able to assist them should the user run into some issues while voting.

15. Reliability: No votes should be lost in an election, regardless of any power outages, network outages or computer failures, etc. Failsafes need to be put in place to ensure that the system stays up throughout the day of voting.

16. Certifiability: All systems should be tested so that the public has confidence that they run as they are meant to. Many people think all voting systems should be open source and open architecture. This way anybody can examine the system and find errors.

17. Cost Effective: Whatever system is put in place will need to be cost-effective. Regardless of how well the system performs in other regards, if it is too expensive it will not be used.

18. Vote Selling: There should not be any confirmation of your vote that could help enable selling of votes. Receipts or any proof of your vote that can be given to someone should not be allowed.

19. Maximise Throughput: The amount of time needed on the system to cast your vote should be minimal. To ensure time efficiency and no delays in votes being cast.

20. Auditable: The system should be auditable from a paper trail in order to ensure everything is being done correctly and in the case of a recount. This will be important in the event of any discrepancies and will help discover the voters intent.