Digital Voter List

Bachelor project
May 22, 2013

Author

Morten Hyllekilde Andersen

IT University of Copenhagen

Supervisor

Professor Joseph Kiniry
Professor Carsten Schürmann

Abstract

The Digital Voter List is a software to register voters at the polling places on the Election Day. The development of such a software requires that it complies with the current legislation and the features needed at the polling places in order for the system to be used in the Danish electoral process.

This thesis contains an analysis of the Danish electoral law concerning the registration of voters and an assessment of whether it meets the necessary requirements defined by the electoral process. The Aegis DVL [1] is a prototype of a Digital Voter List made as a bachelor project with the goal of being used in the Danish electoral process. An analysis of the system is made in order to compare it with the analysis of the Danish electoral law. Based on this comparison the necessary changes for the system to be used in the process of registering voters in the Danish electoral process are assessed.

The assessment concludes that changes have to be made in the Aegis DVL in order for it to comply with the current legislation and be used in the Danish electoral process. Also, additional features must be implemented for the system to comply with the needs defined by the procedures contained in the process of registering voters at the polling places.

Preface

This thesis constitutes a bachelor project at the IT University of Copenhagen developed in the period of February 4th to May 22nd with Professor Joseph Kiniry and Professor Carsten Schürmann as supervisors. The content and goal is part of a DemTech (Democratic Technologies) project and will thus be used for further development of the Digital Voter Lit in order to improve the electoral process in Denmark.

Acknowledgement

Several people's effort are to be acknowledged for the development of this project. My supervisors; Professor Joseph Kiniry and Professor Carsten Schürmann, who have helped with guidance regarding the critical technical parts in the electoral processes needed in the system. Anne Kathrine Nielsen (Ph.D Student connected to the DemTech Research Project) has assisted with knowledge of the Danish electoral. A special acknowledgement goes to Nikolaj Aaes and Nicolai Skovvart who have developed the prototype of a Digital Voter List used in this thesis, and Kåre Sylow Pedersen who has developed the voter card and voter list printer software.

Contents

1 Introduction

This thesis gives an analysis of the legal requirements to the Danish election regarding the Digital Voter List (DVL) and the registration of voters. These requirements will be compared with an analysis of the Aegis DVL system to assess the changes required for the system to be used in the Danish electoral process.

1.1 Background

In autumn 2009, the company KMD A/S published a DVL [2] for the municipalities to use. This system was immediately criticized by professionals from the electronic voting environment. It contained significant flaws and especially the security of the system was pointed out to have shortcomings. It was not certain how many shortcomings it contained as nobody was allowed access to the source code increasing the doubts of the correctness of the system.

The DemTech research project was initiated July 1st 2011. The objective of the project was to improve the Danish electoral process by researching in the area of secure, user-friendly and popularly verifiable e-voting technologies. One of the subprojects was the development of a DVL for a more effective, secure and reliable registration of voters. This system should compete with the KMD system both in security and economic aspects and be developed as an Open Source software.

The work on the DVL within DemTech started in autumn 2011 where Professor Joseph Kiniry (part of the DemTech project) taught an Analysis, Design and Software Architecture course at the IT University of Copenhagen. As a course project, four groups chose to develop their individual interpretation of a DVL [3] [4] [5] [6]. The following spring, a bachelor project [1] were made in the supervision of Joseph. The intention of the project was to develop a secure DVL usable in the Danish electoral process.

1.2 Problem field

Over the last four decades [7] research has been made to improve the election process using information technology. The goal has been to increase safety, anonymity, effectiveness and to reduce the cost of the election. A DVL system has been made by KMD, but due to a lack of transparency, security measures and public access to the code, DemTech has chosen to make an improved DVL as an Open Source software.

1.3 Problem definition

The intention of the Aegis DVL is to improve the process of registering voters in the electoral process. However, the system must comply with the requirements and restrictions stated in the Danish electoral law in order for it to be used in the Danish electoral process. Considering these requirements the following problem is given:

> *Is the Aegis DVL ready to be used in the Danish electoral process, and if not, which changes are necessary to make?*

The intention of this thesis is to benefit the further development of the DVL as an Open Source software. This is obtained by analyzing and assessing the requirements and opportunities of the DVL.

1.4 Scope

This thesis only considers information regarding the process of registering voters on the polling places. However, it does not cover the following topics:

- The specific requirements for generating legal documents and protocols used during the election. This also includes the process of delivering election material to the Ministry of Economics and the Interior and Statistics Denmark.
- The legal restrictions to the election staff required by the Personal Data Act when handling personal data.
- Analysis of all the detailed requirements for the additional processes able to be implemented in the DVL (e.g. the processes, other than registering voters, contained by the DVL developed by KMD).
- Any specific procedures regarding the process of registering voters which are not contained in the Danish electoral law.
- The security aspects of implementing the additional processes in the DVL.
- The detailed requirements for the process of registering letter votes.
- A usability analysis of the DVL to assure that the user interface is created in an intuitive and user-friendly manner.
- The storage and handling of the voter list before and after the election.
- The encryption and decryption of the voter list other than when registering voters.
- The printing of the voter list in the case of any occurring errors, forcing the election to proceed using the paper-based voter list.
- The process of printing and delivering ballots.
- An analysis of the economic aspect of using a DVL compared to the paper-based voter list.
- An assessment of the design, architecture and code specifics of the Aegis DVL.

1.5 Requirements

The goal of the project is to design and develop a replacement for the proprietary, expensive Digital Voter List system developed and supported by KMD. The system will be developed as a FLOSS (Free/Libre/Open Source Software) system with contributions from all developers who find the project interesting.

There have been made several projects on the Digital Voter List that all have ended up with an incomplete system. This project will more or less use all the projects and develop a complete system that can be used in the Danish electoral process. In order to pursue this, the following requirements has been made:

Mandatory Requirements:

- Must be able to generate voter cards from a given set of eligible voters
- Must be able to authenticate a voter based on a voter card number and a CPR number
- Must be able to register when a voter has been handed a ballot and store this information
- Must prevent that a voter can be handed more than one ballot
- Must be able to authenticate and register voters at multiple machines in various polling places
- Must have an interactive user interface for the authentication and registration
- Must be able to print the current voter list at any point during the election

Secondary Goals (optional):

Usability:

- Make the user interface easy to use for non-technical users (election representatives)
- The voter should be able to register at any polling table at the polling place

Persistence:

- Not lose data in the event of a typical system failure (eg. a computer crashes)
- Not lose data in the event of a network failure

Scalability:

- The system should be able to handle a large number of voters

Security:

- The system should use proper security measures and crypto-technology to establish confidence that the system is secure
- Filter the citizens based on multiple lists and criterion to determine the eligibility of the voters
- Analyze the resulting data to detect suspicious voters and fraud

Analysis:

- Analysis of the turnout, both nationally and for specific turnout results
- A public API for the media or any citizen to access (after the election)
- Visualize the turnout results
- Print the list of eligible voters

1.6 Glossary

Table 1 contains a description of the terms and concepts used in this thesis.

Term/Concept	Danish translation	Description
Ballot	Stemmeseddel	The ballot is used to cast the vote
Danish electoral process	Den danske valgprocecss	All of the procedures concerning the Danish election
Danish electoral law	Den danske valglov	The law defining the rules of the Danish election
Digital Voter List	Digital Valgliste	The system used to register voters electronically
Election book	Valgbog	The book containing documentation of essential information about the election in a specific polling district
Election official	Valgtilforordnede	The personnel at the polling place who registers voters
Election secretary	Valgsekretær	The person responsible for a specific polling place
Election Day	Valgdag	The day of the election
Election board	Valgbestyrelse	The board in charge of the election in each municipality
Letter vote	Brevstemme	The vote cast in the Population Register, if a person is unable to attend the polling place on the Election Day
Letter voting protocol	Brevstemmeprotokol	The protocol containing documentation of all the letter votes
Machine	Maskine	The computer used in the electoral process at the polling place
Manager machine	Managermaskine	The computer used by the election secretary to manage the Digital Voter List
Manager	Manager	The election secretary managing the Digital Voter List
Polling booth	Stemmeboks	The booth where the voters cast their vote

Polling district	Valgdistrikt	Each municipality is divided into one or more polling districts
Population Register	Folkeregisteret	The register in charge of the Central Person Register
Polling place	Valgsted	Each polling district contains one or more polling places where the voters can cast their vote at the Election Day
Polling table	Valgbord	The tables where the election officials register voters
Polling table number	Valgbordsnummer	The number of the polling table
Poll book	Afstemningsbog	The book containing documentation of essential information about the election in a specific polling place
Station	Station	The computer used by the election officials to run the Digital Voter List
The Ministry of Economic Affairs and the Interior	Økonomi- og Indenrigsministeriet	The Ministry in charge of the election
Voter	Vælger	A Danish citizen older than 18 and complying with the restrictions in the Danish electoral law
Voter list	Valgliste	The list containing information of each citizen's eligibility to vote
Voter data	Vælgerdata	The information about the voters
Voter card	Valgkort	The card sent to the voters with information about the election

Table 1: Glossary of terms and concepts used in this thesis

2 The Danish Electoral Law

The Danish law includes an electoral law describing the restrictions and requirements concerning the Danish electoral process. In some aspects, the law is old and could benefit from a reevaluation of the procedures performed in the Danish electoral process. In this section the procedures defined by the law are described, an assessment of the law is given, and some beneficial changes are suggested.

2.1 Statutory Procedures

The procedures regarding the electoral process are defined in the Danish electoral law [8] (DEL). In the following, the procedures in the DEL concerning the registration of voters are described together with the procedures in the DEL possible to be implemented in the DVL for increased simplicity, effectiveness or security.

To give an overview of the election process, a flow chart is given in appendix 9.2 Flow Chart of the Election Process.

Lost voter card

In the case that a voter has misplaced, forgotten or in other ways lost her voter card, she is entitled and required to have a new one printed at the polling place[1]. Afterwards, she is to go to a polling table and register as any other voter.

Exercise the right to vote

The voters must personally appear at the polling place in order to submit their votes[2]. This can only be done by handing over their voter card in exchange for a ballot.

Identify the voter

In the process of registering the voters, the voters are required to state their name, residence and date of birth upon request from the election official[3]. This is done to verify the identity of the voters. If any doubt of the identity, the voters are required to provide supporting documentation as evidence.

Letter voting is binding

The voters who choose to vote by letter voting are excluded from voting at the Election Day[4]. This also means that they are not allowed to have a new voter card printed or in any way change their vote after casting the letter vote.

Keeping the election book

The election board of a municipality is required to keep an election book containing information about the vote and the result. This requires the election board to keep note of the unused, the exchanged, and the invalidated ballots[5]. The book is then signed by the entire election board and stored together with the unused material as documentation for the election until the end of the complaint period[6]. After the election has ended, the book must be sent to the Ministry of Economic Affairs and the Interior and Statistics Denmark[7].

---

[1] DEL §47
[2] DEL §47
[3] DEL §47
[4] DEL §67
[5] DEL §74, §52 and §73 pc 6
[6] DEL §74 pc 5
[7] DEL §74 pc 3

Replacement of a ballot

The voters can have their ballot replaced if necessary[8]. The ballot is handed to the election officials and they are given a new one. It is important to keep count of the invalidated ballots and the ballots handed to the voters as the count must match the amount of registered voters at the end of the election.

Letter voting

Voters, who are not able to personally attend the polling place on the Election Day, are entitled to letter vote at any Population Register in Denmark[9]. This increases the amount of letter votes as all voters, who are not satisfied with the place or day of the election, can use their right to letter vote. The letter votes are sent to the municipal council in which the voters are registered on the voter list[10]. The letter vote is received upon request of the voter and requires the voter to show the necessary evidence of identification.

Registration of letter votes

The letter votes are registered at the polling place in which the voters are registered in the voter list. The letter votes are examined[11] at the Election Day or the day before in order to check the eligibility of the voters and register them before the beginning of the election. This makes it possible for the election official to identify if a voter has already voted by letter vote and reject their attempt to vote again.

Printing and distribution of voter cards

The voter list is created by the Population Register[12] with data from the Central Person Register (CPR)[13]. A voter card is printed for each voter contained in the voter list and sent to the specific voter[14]. This procedure ensures that all eligible voters receives a voter card.

Keeping the letter voting protocol

The letter voting protocol is initiated when receiving and forwarding the letter votes. The amount of letter votes and the date for casting the vote is noted[15]. It is used as documentation and stored if any errors occur later in the election process.

Keeping a poll book

The election secretary is required to keep a book in which the essential information about the vote at the specific polling place is documented[16]. This includes the results of the vote and the notation of invalidated votes.

2.2 Assessment of the Current Law

The description of laws are often generic as they must apply to all situations. The DEL is no different and is therefore analyzed by the Ministry of Economic Affairs and the Interior who has made a folder [9] with guidelines to the electoral process for the municipalities to use. This folder helps the personnel in the municipalities to read and understand the DEL.

---

[8] DEL §48 pc 2
[9] DEL §53
[10] DEL §61 pc 7
[11] DEL §66
[12] DEL §18 pc 1
[13] DEL §19
[14] DEL §20
[15] DEL §64
[16] DEL §29 pc 5

In many ways, the current DEL is characterized by the absence of digital tools at its creation. It was redesigned in 2005 [10] where a series of rules were redefined in order to allow the use of specific digital tools in the Danish electoral process. This covers the use of a DVL, a digital letter voting protocol and the ability to submit the election records digitally to the Ministry of Economic Affairs and the Interior and Statistics Denmark after the vote has ended.

The law changes concerning digital tools accompanies a need for definition of the security aspects of such tools. If an unauthorized access to a DVL is made, it can cause severe consequences. This is especially harmful if a malicious entry is not detected, potentially leaving the voter list incorrect and exposed to greater abuse.

The correctness of the information about each voter who have letter voted are currently verified at the Election Day or the day before. The invalidated letter votes does not count, which means the voters will not have their say in the outcome of the election. If the verification was done earlier, a procedure could be performed, informing the voters of the invalidated letter votes in order to give them a chance to recast their vote. This could be a procedure performed continuously by the Population Register, who already administrates the casting of letter votes.

The restrictions of the voters entitled to letter vote was changed in 2013 [11], allowing all voters to letter vote in any municipality in Denmark. This increased the voters' chances to vote, as they are not required to vote in the municipality in which they are registered. Also, the timespan in which they can cast their vote is increased to the timespan of casting letter votes. This change is likely to increase the amount of letter votes, increasing the workload in registering letter votes before the Election Day. If so, the incentive of using a DVL at the polling places to ease this workload is enhanced.

The law states that the election officials are not required to ask for identification or personal information in order to verify the identity of the voters[17]. If no further verification is made, it will increase the risk of abuse of the electoral system, as it will depend on the capability of the election officials' personal assessment.

The electoral process is not only fragile in the polling booth, by the ballot box and in the counting process. If a voter, who is incorrectly handed a ballot after an inadequate verification, she will be able to cast an illegal vote.

2.3 Beneficial Law Changes
The security measures should not only be at a level adequate to avoid the currently known ways of abusing the system. Therefore, the highest level of security must be achieved in order to ensure that future or unknown abuse attempts are thwarted.

2.3.1 Security
The voter data in the current voter list comprise of residence, name and date of birth. The date of birth states the age of the voter and the name gives an indication of the gender. This information helps the election official to assess if the identity of the voter corresponds to the rightfull owner of the voter card. However, the assessment performed from this information is vague. The age is often hard to tell from people's appearance and names can be unisex.

---

[17] DEL §47

The security in the process of verifying voters can be increased by adding CPR numbers to the voter list. This will give an unambiguous information of the gender and serve as a (more or less) secret key only known by the voter and the election official. Additionally, the security of the verification can be increased, if the election official is allowed to ask the voter to state their CPR number for identification purposes. Furthermore, the election official should be obligated to ask the voter a question about a personal information, so the election official can verify their identity by looking up the correct answer in the voter list. This will decrease the abuse of voter cards and remove some of the assessment responsibility from the election officials.

With the incorporation of the DVL in the DEL follows the necessity to define security measures for the system and its physical setup at the polling places. This must be done in order to avoid unauthorized intrusion, malicious attacks and other abuse of the system. The only existing security measure required for the system figures in the Personal Data Act, stating that *the system must have the appropriate technical and organizational security measures*[18]. The additional requirements could contain the following restrictions:

1. The system must not have access to the internet at any time before or during the vote, since this will open the opportunity for people all around the world to hack the system.
2. Precautions must be made to ensure that the computers using the DVL have not been tampered before the installation.
3. Unauthorized access to the physical setup at the polling place must be prevented during the Election Day.
4. A statistics analysis of the actions made by the personnel using the DVL must be available in order to avoid excessive abuse. It will make it possible to identify if the registration of voters made by a specific member of the personnel has exceeded the usual amount.

It is stated in the DEL that all the documents used and generated at the polling places are to be destroyed after the Election Day[19]. The requirements of how the procedure of deleting the documents must be stated more clearly, when the documents are stored electronically. Furthermore, to avoid abuse, it must not be possible to recreate the documents after the election. This will increase the security of the voter data and other secret documents generated during the election.

2.3.2 Efficiency

The letter voting material consist of a ballot, an envelope, a cover letter and an outer envelope[20]. Filling the cover letter is done by the voter, and the filling of the outer envelope is done by the personnel at the Population Register. These procedures could be performed digitally by using the DVL. This change would decrease the amount of invalidated letter votes, and increase the efficiency of the procedure. It would also increase the efficiency of validating the letter votes before the Election Day, as they would be put into the voter list automatically. The change could be scaled down to the use of a digital form in the letter voting procedure. The form would contain the fields to be filled in, verify the entered data, and allowing physical printing. This would exclude the critical aspects of e-voting regarding the anonymity of the voter, transparency of the voting process and the security of the system.

The DEL states that *the voters are required to have a new voter card printed, if they have lost the one they were sent*. The procedure is performed by the election secretary who finds the voter in the voter list, prints a

---

[18] [23] §41 pc 3
[19] DEL §104 pc 3
[20] DEL §60 pc 1

new voter card, and hands it to the voter who is to go to the polling table to get registered. This procedure could be shortened, if the election secretary registered the voter right away instead of printing a new voter card. It would be more efficient and eliminates the possibility of any occurring errors after printing the voter card. Additionally, this would simplify the procedures performed at the polling place since the printing of voter cards would not be necessary.

3 The Digital Voter List

The DVL is a system used to register voters electronically at the polling places. It verifies their eligibility to vote and issues a ballot. It can print a voter card if a voter has lost it and needs a replacement in order to get registered.

The DVL is a vital part of the election process as it hands out ballots, giving eligibility to cast a vote. This means that if anyone is unrightfully handed a ballot, they will be able to cast an illegal vote without any obstructions.

3.1 Open Source Development

The development process is essential for a system of this type, as it will reflect on the quality, security and the correctness of the resulting software. This specific system will benefit significantly from being developed as a FLOSS (Free/Libre/Open Source Software) system.

An argument for implementing the DVL as an Open Source software can be found in the article "Transparency and Accountability Don't Hurt Security – They're Crucial to It" [12] by Bruce Schneider. In this he describes how the lack of transparency and accountability in a society will result in specific people having too much power which is a danger to the society. Similar, an election system like the DVL must be transparent to the society and the developer must be accountable for the system. This results in increased trust from the society as they know who is responsible and they can verify the correctness of the system.

In the development of a FLOSS system it is necessary to choose the license most suitable for the purpose of the software in order to restrict its use rights for others. When choosing an appropriate license a number of aspects are to be considered. First, if it should be allowed to reuse the code within a software using a different license, and secondly, if it should be allowed to make releases under a different license when having implemented the code.

The intention of this FLOSS system is to make the software available for public view and use, to secure transparency, public verification of the security, and to ensure that all municipalities have the opportunity to use it.

This requires the license not to allow others to distribute the code under a different license that makes it inaccessible. The most commonly used license, covering the requirements stated, is the GNU General Public License [13] (GPL). GPL is a viral license, meaning that it requires the software, which reuses the GPL licensed code, to use a GPL (or GPL-approved) license. This means that the use of a GPL license opens the opportunity for reusing code that is licensed with GPL. This makes the development easier and cheaper while increasing the quality of the code.

3.1.1 Advantages

- In an Open Source project the design and the code of the software is publicly accessible and thus all the parts regarding security are available for the public to see. This requires that the design of the security does not rely on any secret code (also called security through obscurity). Consequently, security methods tolerating public availability, without reducing the security, must be used.
- Public accessibility will increase the correctness of the software[21], as it becomes possible for other contributors to review and comment the code. However, it is not certain that all code will be

---

[21] [22] p. 20

reviewed or that the reviewer will leave it correct. This means that the possibility of the code being correct is improved, but not necessarily to the state it should be in.

- The voluntary contributors are usually passionate about the software[22] and some are even end-users. Collaboration with end-users as contributors in the development process helps improving the quality of the software more quickly as they will provide ongoing feedback and stress testing[23].
- The quality of Open Source software is often said to be lower than the commercially produced software. However, a report by Coverity [14] shows that Open Source code is of equal or better quality than the proprietary code.
- The possibility for code review and the interaction between the developers increase the quality of the software[24].

3.1.2 Disadvantages[25]

- The quality of each contributor vary, and if the code is not reviewed, it can cause errors making the software crash.
- Poor code quality or malicious contributors can make the software vulnerable to attacks.
- Contributors can reuse code fragments of licensed software, which are illegal to use, and thereby cause infringement of intellectual property.

Most of the disadvantages are unlikely to happen because of code reviews and the fact that contributors are helping due to their own interest in the topic. The list of advantages and disadvantages shows that there are several benefits to choose Open Source as the development process of a software project.

3.2 Assessment of the Digital Voter List

The DVL has a series of advantages but also some disadvantages. Below is listed the essential aspects of the DVL, giving an idea of the considerations to be made before its implementation in the Danish electoral process.

3.2.1 Advantages

The main advantage of the DVL is the increased effectiveness of the registration of voters. Using the DVL, the information required to identify a specific voter is typed or scanned into the system, and thus, the election official does not have to manually search through the voter list. The increased efficiency reduces the number of personnel necessary for registering voters, ultimately reducing the cost of the election.

The manual procedures of registering voters using the paper-based voter list can be carried out differently in each polling place, making the possibility for errors to occur. In the DVL, the personnel are forced to follow the procedures the way they were designed by the system. This will reduce the risk of errors and makes it harder to abuse the system, and thereby, the election process becomes more secure.

The act of accessing the election data illegally is more difficult in the DVL than in the paper-based voter list. It requires more specific skills, which are not commonly possessed, to perform such an action. In comparison, the paper-based voter list is accessed without any skills necessary.

---

[22] [22] p. 19
[23] [22] p. 20
[24] [22] p. 22
[25] [22] p.49-51

The DVL does not only speed up the procedure of registering voters but also several other procedures later in the election process. The poll book and the election book can be made electronically, introducing the advantage of an automatic retrieval of the necessary information from the voter list. Similarly, the letter voting protocol can be made by retrieving information about the letter votes from the voter list. The reporting of the turnout can be made by calculating the amount of voters who have been registered in the voter list. Finally, the election book can be sent electronically to the Ministry of Economic Affairs and the Interior and Statistics Denmark.

All these procedures can be more effectively carried out and simpler to perform by integrating them in the DVL. This will reduce the possibility of errors while performing the procedures, as the system secures correct execution by having the features customized to comply with the legal requirements.

3.2.2 Disadvantages

The main disadvantage of the DVL is the risk associated with the case of an illegal intrusion in the voter list. Because of the centralized data, this could damage the election more severely than it would have by using the paper-based voter list. A malicious intrusion into the system could tamper, retrieve or even destroy the data in the voter list, and thus force the election at the specific polling place to be shut down. If the attack is detected before any damage is made, the polling place would have to either restart the DVL system or print the voter list and carry on using the paper-based voter list.

The paper-based voter list does not set high demands to the election staff as no specific knowledge is needed to carry out the procedure. On the contrary, the use of the DVL requires that the election personnel have experience in using a computer and knowledge about the use of software systems. These skills are common, but if the personnel do not possess them, they are to be educated before the Election Day, resulting in an additional expense in the election process. The necessity of education could be reduced by designing the DVL as user-friendly and intuitive as possible.

3.3 Analysis of Aegis DVL

For a system of this type, it is essential to maintain a high level of security and ensure its correctness. It can have fatal consequences if an error occurs and changes the system or the data to a state, which it is not able to recover from. Therefore, this aspect must be considered thoroughly during the development of a DVL.

The Aegis DVL software is a prototype of a DVL system developed as a bachelor project by two students from the IT University of Copenhagen. In the following section, an analysis of the system is given in order to identify and assess the necessary changes to be made in order to use it in the Danish electoral process.

3.3.1 Functionalities

The system consists of a manager part and a station part. The manager part is for the election secretary to use and concerns the functionalities to manage the election. The station part is for the election officials to use when registering voters. On the first screen of the system, the user is forced to choose the part to use which then determines the functionalities available.

Manager

Before entering the manager part of the system, the manager is obligated to upload the encrypted voter list used in the DVL at the Election Day. This ensures that the data is available to be shared to all stations that connects to the manager. Simultaneously, the manager has to upload the public encryption key in order to translate the data in the voter list by decrypting it.

Before the manager screen is reached, a master password is shown. This password is used in all authentication processes in the system during the election, involving the initiation of the election, registering of voters by the manager, and ending the election.

The manager is responsible for connecting and disconnecting the stations from a list of IP addresses of the stations accessible at the polling place. This can be done both before and after the manager has started the election, making it possible for additional stations to be added during the election. When a station is connected to the manager, it is synchronized by retrieving the current voter list in order for it to participate in the registering of voters.

The process of connecting a station requires that two different private keys are physically exchanged between the manager and the station. This exchange of keys prevents stations to gain unauthorized access to the functionalities, if they are not known by the manager.

The manager is responsible for starting and ending the election and thus the registration of voters. The start of the election enables the manager and all connected stations to register voters. The end of the election stops the registering of voters for all instances of the DVL and exports the current encrypted voter list. In this way, the voter list is available after the election to document the registrations made. It is also possible for the manager to export the current encrypted voter list during the election for any reason that may occur.

Registering of voters by entering their CPR number is only available for the manager as a security measure. This makes it possible for the voter to be registered, when they have lost their voter card, since their voter card number, which is normally used as a unique identification, is not available for retrieval.

Station

Functionalities are only available on the station, if it is connected to a manager, and the election is running. The only functionality of the station is to register a voter by entering (or scanning) a voter card number. This limitation of functionality is done as a security measure to reduce the need of individual assessment by the users and thus to avoid any errors in the process.

Table 2 contains a complete list of the functionalities available for the manager and the station.

Manager functionalities	Station functionalities
• Upload encrypted voter list and public encryption key • Connect to station from list of reachable stations • Disconnect a connected station • Update the list of reachable stations • Assign manager role to station • Start the election • Register voter by voter card number and CPR number • Register voter by CPR number • Export the current voter list • End the election	• Register voter by voter card number

Table 2: A complete list of the functionalities available for the manager and the station

3.3.2 Network Architecture

The system requires that several computers run the Aegis DVL system in order to initiate the election. The computers must be connected through a local network without access to the internet. These restrictions, set by the developers of Aegis DVL, must be followed in order to obtain the security needed for this kind of

system. It would still be able to run the system without complying with the restrictions, but it would reduce the security significantly. The manger and all the station running the DVL have a local database of both the voter list and the logging data. The voter list is continuously synchronized with the manager's voter list as a security measure to preserve the data in the case that any of the connected machines crash. Figure 1 shows an example of the network diagram used.
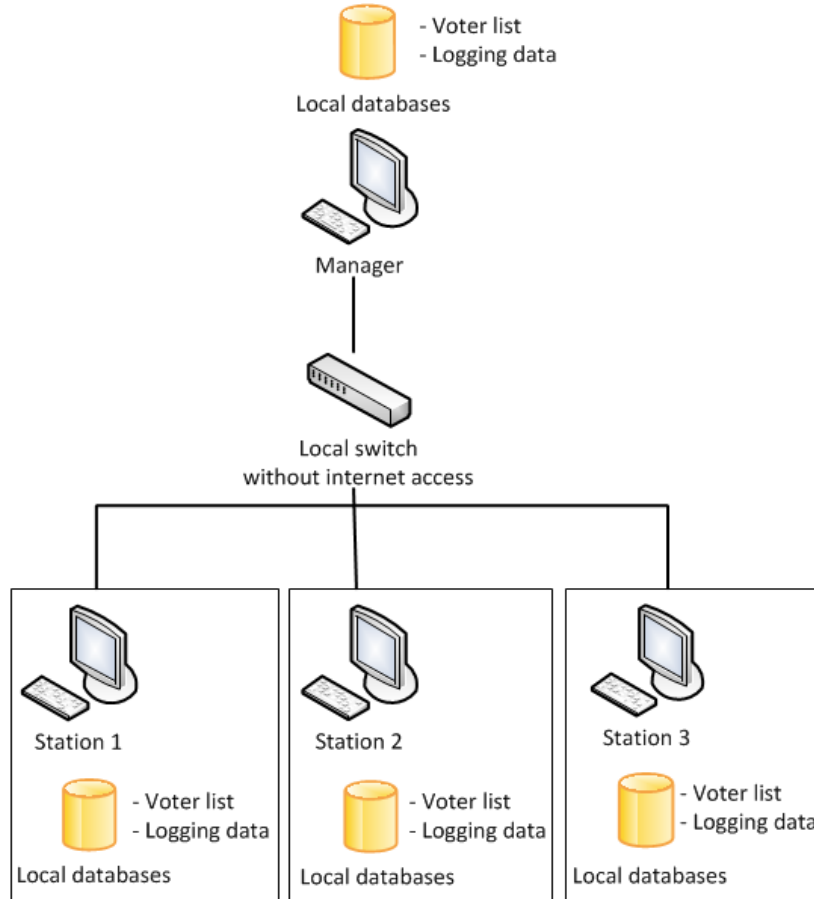

Figure 1: An example of the network diagram used at the polling places.

3.3.3 System Development

The system was developed using the Business Object Notation (BON) [15] in the analysis and design process. BON is a notation to analyze and design object-oriented software in a simple way without using regular code. It was used to analyze and design the classes needed in the system and the different types of methods they should contain. Furthermore, it was used to set the preconditions, postconditions, and the invariants of every method.

The BON specification was used to generate artifacts such as the domain analysis, design and architecture of the system. This was done by using the BONc tool suite [16] to parse and typecheck the informal and formal specifications of the system ensuring soundness and completeness. Additionally, the tool suite generate XHTML documents used as documentation of the system with its benefit of a graphical presentation. The BONc tool suite is also used to perform a static analysis

The conditions from the BON specification was used to develop the system with the Design by Contract [17] approach using the Code Contracts [18] framework. The compiler for Code Contracts was used to ensure that

the software behaves as expected by making sure the contracts, made of the BON specification, was not violated at any time.

3.3.4 Technologies

The development of everything concerning cryptography is done using the Bouncy Castle framework [19], which is developed as an Open Source project without any restrictions in the license and thus free to use. It consists of an API (Application Programming Interface) used in the process of sending and receiving symmetric and asymmetric keys, when the computers need to identify one another before communicating through the local network.

The databases in the system are managed with the SQLite Database Management System (DBMS). The DBMS consists of an API used to handle all the manipulation of the databases in a secure way. This saves the programmers from developing the procedures on their own and thereby reduces the risk of making errors.

The database is synchronized using a customized method made of a combination between the *Request synchronize* method and the *On action* method described further in the Aegis DVL report[26]. The voter list database uses this method to synchronize the voter list of each machine every time an action is made. This is done by broadcasting the information of the changes. This method is also used to communicate between the machines in the process of managing the connected machines.

3.4 Changes and Additional Features

The intention of the system is to be used in the Danish electoral process. This demands that it contains specific required features for the process of registering voters to be successful. Many of the procedures performed at the Election Day would be easier to perform if implemented in the DVL. However, they are optional as they are still able to be performed manually independent to the DVL.

The changes chosen to be performed should be incorporated in the existing BON specification of the system. The specification can then be used to develop requirements to the code with the Design by Contract approach using Code Contracts.

3.4.1 Requirements

The changes in Table 3 are required for the Aegis DVL to function successfully in the Danish electoral process. This has been developed by doing a line-by-line analysis of the DEL and the guidelines made by the Ministry of Economic Affairs and the Interior. Furthermore, election professionals have been consulted which, amongst others, include Anna Kathrine Nielsen from DemTech and personnel in the municipalities. It was considered to consult an end-user, but the changes must be based on the requirements from the law and not the actual procedures performed at the polling places.

In addition to the changes in Table 3, a list of bugs and errors in the current version of the Aegis DVL is given in the bachelor report of the Aegis DVL[27].

#	Description of change/additional feature
1	The current system requires four machines to be connected in order to start an election. This restriction must be changed to allow one machine to run the system as some polling places will not use more than one machine to register voters at the polling place.

---

[26] [1] p. 17
[27] [1] p. 39

#	
2	The Population Register does not provide the CPR number of the voter in the voter list and thus it is not possible to use it to validate and register voters.
3	The functionality to print voter cards must be available for the manager in order to print a replacement voter card if a voter requests it.
4	The manager must be able to browse and search the voter list in order to find a specific voter and print a replacement voter card. This is necessary as there is no unique identification of the specific voters other than the voter card number, which can only be retrieved from the voter card.
5	The logging data must be synchronized continuously, similar to the data in the voter list, in order to secure its preservation in the case that a computer crashes. This is especially necessary when the logging data is used as a security measure to avoid abuse.
6	The manager must be able to monitor the logging data of all the connected stations in order to detect abuse or suspicious use of the system.
7	The system must show personal information about the voters in order for the election officials to assess and verify their identity during the registration process.
8	The voter card number should be hashed before printing it on the voter card to avoid abuse by replicating voter cards.
9	The functionality to decrypt the voter list must be available for the manager. This will be used when printing the voter list in the event of a network failure causing the election to proceed using a paper-based voter list.
10	Both the manager and the election officials must be able to see the reason for a voter's eligibility status. This will show if a voter has already voted by letter vote or is registered in another polling place.
11	The manager must be able to mark a specific voter in the voter list as having letter voted during – and before – the election. This will prevent voters who have already voted by letter vote from voting twice.
12	The manager must be able to edit the voter list during the election. This is necessary as it is stated in the DEL[28] that voters can be obtained on the voter list during the Election Day.

Table 3: The required changes to be made in order to use the Aegis DVL in the Danish electoral process

3.4.2 Optional

The changes in the following tables are optional, since the DVL can fulfill its main purpose without them. Many of the changes are procedures done manually in the current electoral process, which could be more efficiently and securely performed if implemented in the DVL.

#	Description of change/additional feature
13	The manager should be able to retrieve statistics of the actions made at the Election Day in order to identify any abuse during the Election Day.
14	The manager should be able to calculate the current turnout during the Election Day. This is especially useful when reporting to the media.

Table 4: Optional changes

Letter voting

The changes in Table 5 are all features to support the process of letter voting done at the Population Register in the municipalities. The features listed are not to replace it completely as this is not possible without a change in the DEL. These changes would improve the efficiency of validating the letter votes on the Election Day, which could be useful since the amount of letter votes increases as written in 2.2 Assessment of the Current Law.

---

[28] DEL §22

#	Description of change/additional feature
15	The personnel at the Population Register should be able to print a cover letter for the voter to attach to their letter vote. This will reduce the errors made by the voter when filling in the information.
16	The personnel at the Population Register should be able to register information of the casted letter votes in order to make lists of the letter votes casted and proceed with change 17.
17	The personnel at the Population Register should be able to sort and distribute letter votes depending on which polling place and municipality the voters are registered. This will reduce errors during the sending of the letter votes and improve the efficiency of marking the voters, who have letter voted in change 18.
18	The personnel at the polling places should be able to register lists of letter votes in the DVL at the polling places in order to mark the specific voters, who have letter voted. This is meant to be used with the list generated by the Population Register explained in change 16.

Table 5: Changes regarding the process of letter voting

Management of the election book

The changes in Table 6 comprise the features required if it should be possible to manage the election book using the DVL. This would make the procedures regarding the election book easier and more efficient, as some of the information needed to fill in is already in the system. Furthermore, the election board would avoid having to print the election book and sending it manually, which is rather cumbersome and time consuming.

#	Description of change/additional features
17	The election board should be able to report the result of the vote from the specific polling place in the election book.
18	The election board should be able to report the counting of ballots of the polling place in the election book.
19	The election board should be able to print the election book both digitally and on paper in order to proceed with change 20.
20	The election board should be able to send the election book to The Ministry of Economics and the Interior and Statistics Denmark after the result of the vote is calculated at the specific polling place.
21	The election board should be able to present the result of the vote on the internet for everyone to see.

Table 6: Changes regarding managing the election book

3.5 Evaluation

The Aegis DVL is a DVL with a great potential to be used in the Danish electoral process. However, there are parts of the system that need to be reevaluated and changed in order for it to fulfill the needs of the process of registering voters.

The user interface requires more attention and will benefit from performing a usability test. It also needs an excessive functionality test, which is often done during the Open Source development process, where the functionalities will be stressed to avoid future errors during the Election Day.

The registration of a voter by CPR number is not possible as the voter list received from the Population Register does not contain this information[29]. This is a problem for the Aegis DVL as the function is used to register the voters, who have lost their voter card, since it gives a unique identification of the voter similar to the voter card number. Instead, the system must be able to search the voters by name and address in order to be uniquely identified. This is an inefficient and weak solution as manual procedures tend to increase the amount of errors made, however, it is currently the only possibility available.

---

[29] See Appendix 9.1 Voter list

The procedure of registering voters, who have lost their voter card is done by entering their CPR number. The problem with this procedure, other than the issues mentioned above, is that the DEL requires the print of a replacement voter card in order to register the voter[30].

The way of registering voters in the system is exposed to errors because of a lack of control. The procedure only requires a voter card number, and the election personnel does not have the possibility to verify that the voter is in fact the rightful owner of the voter card. The procedure must be extended with a verification step, in which information of the voter is displayed to further assess or question the voter. This will prevent people from utilizing false or stolen voter cards and is a requirement stated in the DEL[31].

The master password is only shown once when the manager starts the manager part of the DVL. If the password is forgotten, the manager would not be able to register voters, who have lost their voter card, or to start or end the election. In this event, precautions are necessary to reacquire the password or end the election. Biometric authentication would be a solution as it prevents the manager from forgetting the password.

In the procedure of ending the election, the system exports the encrypted voter list, which is also possible during the election. The function to export the voter list during the election is not secure, as it could be done by anyone illegally acquiring access to the manager machine. This is solved by restricting the function with an authorization precaution, requiring the master password.

The current logging data is only possible to use for post-election evaluation and error correction. It should also be available during the election to avoid unhandled known errors from damaging the election process and work against any abuse of the system. This requires that the logging database of each instance of the DVL is synchronized and contains the logs made at all the machines. This also helps to preserve the data in the case of a computer crashing.

The DVL system is responsible for securing the continuation of the election even though errors or unforeseen events occur and cause the DVL system to stop. It requires a set of predefined fallback procedures, describing when to take action and what to do. In the event of a station crashing, the election will continue using the DVL system and reconnect the station if possible. In the event of a network failure causing the stations not to synchronize with each other, it is required that a polling table number is attached to each voter in the voter list. The election will then continue by using a local DVL system on each station only able to register voters with its own polling table number attached. In the event that the system is exposed to intrusion, the DVL system must be stopped, the voter list printed, and the election process must continue with the paper-based voter list. The same procedure applies in the event of a power failure.

The Open Source development process will benefit the development and the end product of the DVL system. The security measures available in the development of an Open Source software corresponds to the needs of the DVL and will require the critical parts concerning security not to rely on any confidential information in order to be secure.

The procedure of using BON and Design by Contract is a simple and effective method to achieve a documented and correct system. The use of BON is beneficial as it does not set many rules to the specification, and thus it will be faster and easier to make the analysis and the design. Furthermore, it will

---

[30] See 2.1 Statutory Procedures
[31] DEL §47

secure seamlessness and reversibility, making it is easier to change the design continuously and reflect back to earlier changes.

The changes stated in 3.4 Changes and Additional Features are described as abstract user requirements. In order for them to be implemented, they need to be changed to specific system requirements, which in detail describe the exact changes necessary to implement[32]. This will decrease the risk that they will be understood ambiguously by the developers and thus prevent them from implementing the changes in an unintended way. In order for the requirements to be able to be tested during and after the development, they must be described in a qualitative and measurable way[33] improving the correctness of the implementation of the requirements. Before developing the requirements, they must be validated[34] to ensure they actually cover the final intention of the system. This can be done by having the requirements reviewed, experiment with a prototype or generating test-cases[35].

---

[32] [24] p. 84
[33] [24] p. 89
[34] [24] p. 110
[35] [24] p. 111

4 Reflection

The DVL software is dependent on the security of its procedures. When designing such procedures it must be acknowledged that it will never be completely secure. The system will always have personnel responsible for certain procedures making them able to take advantage of the system.

The IT competences of the personnel at the polling places varies increasing the requirements to the system. For this reason, the procedures of the DVL must be thoroughly identified in order to implement the necessary security precautions in the system. These precautions must be implemented to prevent the personnel from making errors. Furthermore, the varying IT competences of the personnel increase the importance of fully testing the procedures contained in the system.

It is noteworthy that the introduction of digital technology in the electoral process has not introduced additional security measures in the Danish law. On the other hand, it is difficult to specify security requirements for a system like the DVL, since new ways to abuse the system are continuously developed. This increases the responsibility of the designers of the system, as they must identify all the security threats possible.

While designing the system a problem occurred as the voter list did not contain the CPR number of the voters. The CPR number is the only single information able to uniquely identify a voter, except for the generated voter card numbers. This made it difficult to design procedures for voters who have lost their voter card, since they could not be easily identified. It resulted in a manual procedure requiring the ability to search the voter list increasing the risk of errors significantly.

5 Conclusion

An analysis of the DEL and the Aegis DVL system identified several changes necessary for the system to be used in the Danish electoral process. The following describes the required changes:

The Aegis DVL requires four machines to run the DVL. This requirement must be removed in order for smaller polling places to use it to register voters.

The process of printing voter cards, performed by the manager, must be implemented with a unique way to identify a voter. This must be done by searching the voter list, since it does not contain CPR numbers as a unique identification. Furthermore, the voter card number must be hashed before printing the voter card to reduce the risk of replication.

The logging database of all machines must be synchronized in order to preserve the data in the case of a computer crashing. This will also give the manager the opportunity to monitor all changes performed on the voter list in order to identify possible errors and abuse.

The registration process must be extended with a verification step displaying the personal information of the voters. This will allow the personnel to assess the rightfulness of their identity. The procedure must also show detailed information regarding the eligibility status of the voters. This makes it possible for the personnel to inform the voter of the reason for the rejection to vote.

The manager must be able to mark the voters who have letter voted to ensure that they cannot vote twice, and she must be able to edit the voter list before and during the election. Also, a functionality must be available to decrypt the voter list during the election.

Mandatory Requirements:

All the mandatory requirements were met except the one allowing the election secretary to register voters by their CPR number. This requirement was unable to be fulfilled, as the CPR number was not a part of the voter list received from the Population Register.

Secondary Goals (optional):

Make the user interface easy to use for non-technical users (election representatives)
This requirement was not met, but is advised to do before using the system in the election process. It can be done by performing a usability test with end-users of the system to discover their needs.

The voter should be able to register at any table at the polling place
This requirement was met since the entire voter list is available for all the machines connected to the manager. It must be noted that the requirement only applies when the DVL is running, and not in the case that a fallback procedure has been started.

Not lose data in the event of a typical system failure (eg. a computer crashes)
The synchronization of the voter list makes sure that all voter data is shared and stored on each computer connected to the manager. This ensures that no data is lost in the event of a typical system failure.

Not lose data in the event of a network failure
The event of a network failure would make it impossible to register voters at the stations. This ensures that no additional data can be added to the voter list, and thus the voter list of the manager machine is up-to-date.

The system should be able to handle a large number of voters

This requirement was not tested and therefore cannot be ensured to apply for the system. A large number of voters require an increased number of stations to be used at the polling place. This will increase the amount of network communication and thus the amount of commands to handle. A message queue must be implemented to handle incoming communication in order to ensure all commands to be executed. The queue must take into account that the commands do not have the same importance. For instance, a command to end the election could be sent to the stations. This command must be executed instantly to stop the registration of voters at the station.

The system should use proper security measures and crypto-technology to establish confidence that the system is secure

This requirement cannot be ensured since the security and the cryptography of the system were not assessed.

Filter the citizens based on multiple lists and criterion to determine eligible voters

This requirement was not met, however, it is necessary to be considered, when the registration of letter votes is to be performed.

Analyze the resulting data, to detect suspicious voters and fraud

This requirement was not met. However, it is described as an optional change to the current system. The requirement is necessary to apply in order to ensure the security of the election process. Suspicious voters are not avoided through an analysis of the resulting data but in the process of registering the voters.

Analysis of the turnout, both nationally and for specific turnout results

This requirement was not met. The analysis of the turnout could be an enhancement to the implementation of the election book, since the election book contains the result of the turnout.

A public API for the media or any citizen to access (after the election)

This requirement was not met. The publishing of an API needs access to the internet which is not an option in the DVL due to security reasons.

Visualize the turnout results

This requirement was not met, since it is not considered a valuable feature at the polling places and thus should not be implemented in the DVL.

Print the list of eligible voters

This requirement was not met. It should have been a primary requirement, since it is necessary for the system to be used in the Danish electoral process.

6 Future Work

The future work on developing the Aegis DVL requires collaboration with the necessary authorities in order to gain access to the current voter list. Furthermore, a collaboration with the Ministry of Economic Affairs and the Interior should be established to initiate a discussion about the changes suggested to the DEL and the voter list.

Afterwards, the development should proceed following the requirement engineering process specified by Ian Sommerville in his book Software Engineering[36] and shown in Figure 2[37]. This will ensure the development to identify and fulfill the requirements needed for the system to be used in the Danish electoral process. As an example, the next step is to do the "User Requirements Elicitation" phase. This should be done in collaboration with end-users in order to identify their actual needs.

Furthermore, a cost-benefit analysis of the change from a paper-based voter list to the DVL should be made in order to include the cost aspect in the decision making process of using the DVL.
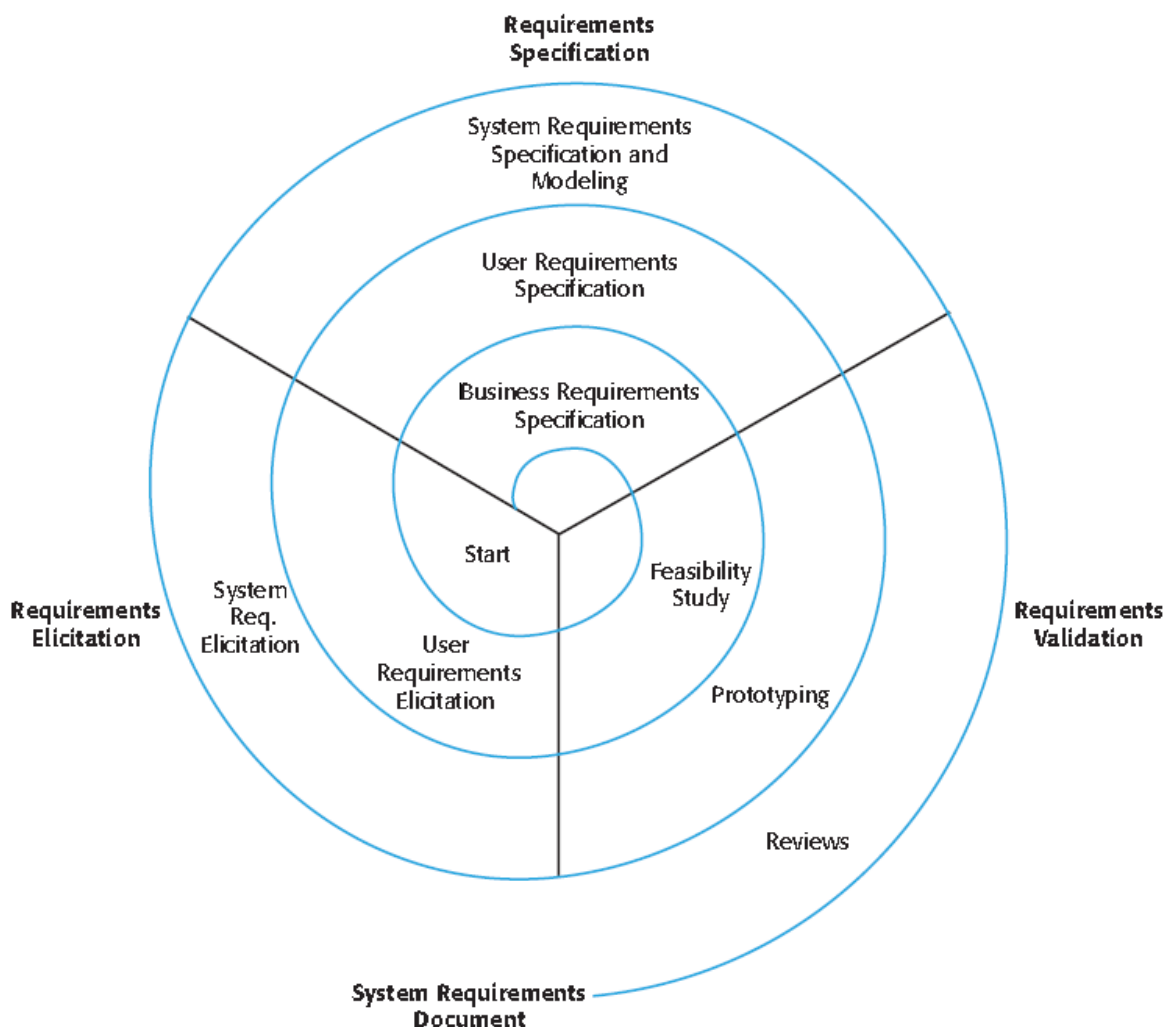

Figure 2: A spiral view of the requirement engineering process

---

[36] [24] Chapter 4 p. 82-117
[37] [24] Figure 4.12 p. 99

7 Other Work

A lot of work is worth looking into when further developing the Aegis DVL. This especially includes research made on the digitalization of the voting process, since other digital technologies used within the election process considers similar critical problems as the ones identified in the DVL.

Additionally, it is worth looking into any Open Source software able to improve aspects of the DVL. For instance, the CryptDB project [20] concerning the crypto-commands necessary to ensure the security of processing information in a database. It is important that the software used is Open Source, as it must be available for verification.

8 References

[1]   N. Aaes and N. Skovvart, "Aegis DVL," 2012.

[2]   KMD A/S, "KMD Digital Valgliste," KMD A/S, 2009.

[3]   M. H. Andersen, J. D. Møllerhøj and M. Valentin, "PX3 - Digital Voter List," 2011.

[4]   C. Martinsen, N. M. Søholm and J. A. Meier, "Group CJN - Digital Voter List," 2011.

[5]   E. B. Nygaard, M. O. U. Mortensen and R. Greve, "Group EMR - Digital Voter List System," 2011.

[6]   C. Olsson, K. S. Pedersen and H. Haugbølle, "Dirty Lion - Digital Voter Registration System," 2011.

[7]   DemTech, 29 04 2013. [Online]. Available: http://www.demtech.dk/wiki/DemTech.

[8]   Ministry of Economic Affairs and the Interior, "www.retsinformation.dk," 11 02 2013. [Online]. Available: https://www.retsinformation.dk/Forms/r0710.aspx?id=144959. [Accessed 08 05 2013].

[9]   Ministry of Economic Affairs and the Interior, "Vejledning om afholdelse af folketingsvalg," Rosendahls-Schultz Grafisk, 2010.

[10] L. L. Rasmussen, "www.retsinformation.dk," Civilstyrelsen, [Online]. Available: https://www.retsinformation.dk/Forms/R0710.aspx?id=10039. [Accessed 2 5 2013].

[11] M. Vestager, "www.retsinformation.dk," Civilstyrelsen, [Online]. Available: https://www.retsinformation.dk/Forms/R0710.aspx?id=144580. [Accessed 02 05 2013].

[12] B. Schneider, "www.theatlantic.com," [Online]. Available: http://www.theatlantic.com/politics/archive/2013/05/transparency-and-accountability-dont-hurt-security-theyre-crucial-to-it/275662/. [Accessed 21 05 2013].

[13] GNU, "www.gnu.org," [Online]. Available: https://www.gnu.org/licenses/gpl.html. [Accessed 05 09 2013].

[14] Coverity, "Coverity Scan: 2011 Open Source Integrity Report," Converity, 2012.

[15] Waldén, Kim;, "Business Object Notation (BON)," in *Handbook of Object Technology*, CRC Press, 1998.

[16] ETH Zurich, "tools.ethz.ch," 2007/2008. [Online]. Available: http://tools.ethz.ch/tools2008/tutorials.html. [Accessed 17 05 2013].

[17] B. Meyer, "Applying "Design by Contract"," 1992, pp. 40-51.

[18] Microsoft, "www.microsoft.com," [Online]. Available: http://research.microsoft.com/en-us/projects/contracts/. [Accessed 16 05 2013].

[19] The Legions of the Bouncy Castle, "www.bouncycastle.org," [Online]. Available: http://www.bouncycastle.org/csharp/. [Accessed 17 05 2013].

[20] R. A. Popa, C. Redfield, S. Tu, H. Balakrishnan, F. Kaashoek, S. Madden and N. Zeldovich, "CryptDB," [Online]. Available: http://css.csail.mit.edu/cryptdb/. [Accessed 05 20 2013].

[21] Albrecht, Anne-Marie; Vice Office-Manager, Copenhagen Population Register, *Anonymized Voter List.*

[22] B. Golden, Succeeding with Open Source, Addison-Wesley, 2005.

[23] F. Jensen, "www.retsinformation.dk," 31 05 2000. [Online]. Available: https://www.retsinformation.dk/Forms/r0710.aspx?id=828. [Accessed 17 05 2013].

[24] I. Sommerville, Software Engineering, 9th ed., Addison-Wesley, 2011.

9 Appendix

9.1 Voter list

This voter list is received from the Population Register in Copenhagen [21].

VALGLISTE
Europa-Parlamentsvalg den 07.06.2009

Side: 335

Kom. nr.	Distrikt	Bord	Vejnavn
0101	11	04	

Husnr.	etage	side/dør	Navn	Fødselsdato	Anmærkning	Valgnr.	Anmærkning
005	03	tv	Hr. Karsten Mosholt	08-06-53		11-06046	
005	03	tv	Fr. Eva	09-11-44		11-06047	
005	04	th	Hr. Antony	07-03-74		11-06048	
009	03	th	Hr. Torben	04-01-45		11-06049	
009	03	th	Fr. Anette Riis	05-09-43		11-06050	
009	03	tv	Fr. Birthe Hagedorn	25-01-36		11-06051	
009	05	th	Fr. Ane Solvejg Gosvig	13-02-31		11-06052	

9.2 Flow Chart of the Election Process