TALLINN UNIVERSITY OF TECHNOLOGY

Faculty of Information Technology

Department of Computer Science

TUT Centre for Digital Forensics and Cyber Security

ITC70L

Nisham Kizhakkedathil 132113IVCMM

A STUDY INTO THE PROSPECTS OF IMPLEMENTING END-TO-END VERIFIABILITY IN ESTONIAN i-VOTING

Master's Thesis

Supervisors: Dr. Tanel Tammet

Dr. Vadims Zuravljovs

Tallinn 2016

Declaration

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been acknowledged in this thesis. This thesis has not been presented for any degree or diploma at any other university.

Author: Nisham Kizhakkedathil

Signature: …..........................

Date: …..........................

Abstract

Internet has become an ubiquitous infrastructure that provides the foundation on which various physical services are designed. Smooth and efficient elections being the prerequisite of functioning democracies, the internet based voting platforms become pinnacle of attention in rapidly transforming nations. Undoubtedly internet voting is a medium where voters can cast their votes easily and effectively. I-voting being a pioneering and not time tested voting methods, naturally comes with a cloud of doubt on its efficiency and credibility. Estonia is one of the few countries in the world that relies its elections on I-voting. During the elections in 2015, more than 30% of the votes were cast online [1]. This research paper attempts to analyse the Estonian model of internet voting and security risks associated with it. Already there have been several discussions about the security of Estonian internet voting and its lapses, which have been ensued with great acumen. The most profound of which is the absence of provisions for end-to-end verifiability. In the current model, voters can verify only the casting and registration of the ballot ex-post facto. Mainly with the intention to tally the total recorded votes. The thesis explores the prospects of implementing end-to-end verifiability features supplementing the current Estonian internet voting model, with the intention to ensure comprehensive and universal verifiability, additionally the author also discuss in brief the about the social factors influencing internet voting.

Keywords

Internet Voting Security, Estonian i-Voting, Verifiable voting, End-to-End verifiability, Vulnerabilities, Mix-net Voting, Crypto, Homomorphic encryption, Digital Divide, OWASP, BON, Zero Knowledge Protocol.

Acknowledgements

I would like to express my sincere gratitude to my supervisor Dr. Tanel Tammet for his supervision and guidance for preparing this thesis and also giving me knowledge and feedback on my work.

I would also like to thank my co- supervisor Dr.Vadims Zuravljovs for the valuable feedback and motivation which helped me to finish this paper.

Nisham Kizhakkedathil

List of Abbreviations

ATM	Automated Teller Machine
DOS	Denial of Service
E2E	End to End
HSM	Hardware Security Module
HTTPS	Hypertext Transfer protocol Secure
PIN	Personal Identification Number
PKI	Public Key Infrastructure
SMS	Short Message Service
SSL	Secure Sockets Layer
VC	Visual Cryptography
VPN	Virtual Private Network
TPM	Trusted Platform Module
ZKP	Zero Knowledge Proof
BON	Business Object Notation
EBON	Extended Business Object Notation
UML	Unified Modelling Language
DFD	Data Flow Diagram
OWASP	Open Web Application Security Project

Table of Contents

List of Figures

Chapter 1. Introduction

i-Voting – Can be defined as an election system that use electronic ballots that would allow the voters to transmit their votes to the officials over the internet. With the advancement in internet, countries started to experiment their elections over the internet making it easier for the citizens to cast the vote online. More than 14 countries have used remote internet voting for its political elections till now. Estonia is only country in the world that offers internet voting to its entire constituency. Other countries have either piloting internet voting or have piloted it or might have discontinued it [2]. Only two countries in the world, Estonia and Switzerland have successfully implemented and still continuing internet voting for their national elections to cast ballots.

When it comes to internet voting there are standards to be followed. These standards can be the need for securing online voter authentication, secrecy of the vote to be protected and also the entire elections should be transparent. Out of these, the most difficult standard to follow would be the secure online voter authentication. Most of the democratic countries do not have ID card system with secure authentication feature, so it turn out to be a challenge in implementing internet voting. In order to make a successful democracy, trust in the electoral process is essential. As trust is a complex concept where the voters make rational decisions based on accepting the integrity of the voting. In a democracy, only a few percentage of the population will have technical knowledge to understand the internet voting, thus making them to trust in it. Enabling confidence among the population to popularise i-Voting is major issue, this can be done only by enabling trust among the population. With proper auditing and testing integrity of the voting system can be ensured.

1.1 Motivation

Associated with the dawn of the internet age, i-Voting have emerged as a trending topic prompting people to think in a way that if they can conduct financial transactions online and even avail most other public services, why they can’t they cast their ballot online too. In 2005, Estonia became the first country in the world to offer internet voting to its citizens for the national elections. Latest statistics shows more than 80% of the Estonia’s population uses internet for their day-to-day activities. This exemplifies the level of internet penetration within the nation. During the national elections in 2015, more than 30% of the total votes were cast online showcasing how significant internet voting is in Estonia [1]. The national ID card of Estonia which acts as a smart card is the backbone of the internet voting in Estonia. As of now, out of 1.3 million population, more than 90% of the population have an active ID card. Estonian ID card can be used for secure authentication and access in to Estonia's various e-services databases for both public and private sector utilities [3]. Estonian ID card also can be used for digital signature and document encryption.

1.2 Scope

This thesis intended to provide an analysis of current Estonian i-Voting model, to ascertain the possible security weakness and flaws, and in effect suggesting a better framework for making the i-Voting infrastructure design more secure and transparent. The scope of making this system secure involves protocols that meet specific security requirements which protect voter privacy and authenticity evidently making the election transparent. Transparency can be achieved by providing verifiability features within the i-Voting system whereby voters can audit their votes. Aim of this thesis is to provide a feasibility study on applying end-to-end verifiability for Estonian i-Voting, a feature which it is currently lacking but has potential implications on overall transparency.

1.3 The Problem Statement and Research Questions

Can there be a trusted i-Voting system, at all if there is one, that is secure, and more specifically can we rely on the system as opposed to setting trust on the infrastructure or its administration in itself. In lieu of this, how good does the implementation of current i-Voting system in Estonia fairs. The core issue of this research can be identified as:

"Can End-to-End voting system provide a panacea to the current transparency issues facing internet voting system of Estonia."

Establishing veracity of the ballot is intrinsic to the confidence of citizens in their country's elections. The research question explores the possibilities of implementing verification mechanisms for the votes cast, so the end user does not have to solely rely on the robustness of the technical implementation of the system. Also an analysis is being carried about the existing End-to-End voting systems and their vulnerabilities.

1.4 Research Methodology

The research is done based on a combination of qualitative and quantitative approaches where rigorous quantitative methods have been applied to unravel the current security lacunae faced by the Estonian i-Voting system particularly citing the previous researches on duplicating the model; and statistical reports and surveys in media publications that have attempted to gauge the trust of the people within this infrastructure. The quantitative approaches utilized have enabled to identify the present threats prevalent at the various stages of the internet based voting infrastructure and also propose possible solutions to them and vote cast verification in detail.

1.5 Thesis Outline

A brief summary of the thesis is as follows:

The introduction part which provides the brief outline of the research and thesis paper is followed by Chapter 2, Internet Voting: Significance & Concerns that is a brief discussion of general internet voting significance and concerns. This chapter also examines the Switzerland i-Voting experience. The chapter explores the major debates that arose in Switzerland about i-Voting putting down both for and counter arguments.

Chapter 3 and Chapter 4 discuss in detail about the Estonian i-Voting model, procedures, and security aspects presenting proposals for improvement of i-Voting process stressing on the transparency aspect. Chapter 5 and 6 discuss about End-to-End verifiability in detail along with the requirements, crypto foundations for an ideal End-to-End system, existing models, their draw backs and security challenges possessed by these models. Here, the paper offers insights into the technological aspects of i-Voting system in Estonia in order to provide technologically viable solutions to the problems of transparency in elections, the prime issue raised in the research.

The research found these measures as of utmost relevance to increase voting acceptance and citizens' trust in the system. This aspect is discussed in chapter 7, which is a study of internet voting acceptance bringing up proposal to build trust in it. The chapter stresses trust as a major prerequisite of democratic political structures and thus demanding measures from the part of respective governments and other concerned bodies to ensure citizens' high level of trust in the i-Voting system.

Chapter 2. Internet Voting: Significance & Concerns

Experiments towards implementation of internet voting has yielded diverse results, owing to the disparities in the existing electoral and democratic systems, demography, political culture and technological contexts of different nations. This, at the same time complicating any analysis on internet voting, opens chances for a broader perspective to think about the significance of internet voting and related concerns. While there is mounting technological and sociological global interest in i-Voting system, and a much wider realization of its possibilities, it is important to look into the general concerns expressed before going into specific case studies [4].

The potentials of i-Voting in enhancing the democratic system with increased people's participation and thus widening the political spectrum is now more than less widely accepted. The current rise of internet as a strong sphere of democratic participation had all the more provided new impetus for the discussion on i-Voting. At a time when internet has established for itself a significant role in modern democracies, the proponents of i-Voting considers itself as a logical outcome of the increased reliance on internet for democratic opinion making and participation both by individual citizens, and by official and non-official institutions. Most discussed is the possibilities it holds for increasing voter turn-outs, and extending easy access to democratic electoral process to various disenfranchised groups like citizens living overseas, military personnel and disabled citizens [5]. The experiments in i-Voting in most places has proved this point especially among the youth who is more accustomed to internet democracy [6].

Administrative efficiency along with a reduction in overall monetary cost of elections is as well, one of the foremost reasons that encourage democratic nations to take on to i-Voting. Proponents of i-Voting has continuously stressed this, pointing towards the labour saving options that would reduce the overall cost of elections at the same time increasing the efficiency of the system thus leading to a productive output. "The common errors and mistakes that recurred in manual voting systems, from the part of both voters and electoral administrators can be made more error free when a computer is used this it also making it easier to develop a unified standards in the ballot format" [7]. Apart from the practical possibilities of i-Voting the proponents of internet voting considers it as a logical outcome of an increasingly digitised era. The initial discussion on i-Voting that took stronghold in Europe in the 1990's, happened as part of a broader step towards modernizing elections. However, if we examine the current status of various nations vis-a-vis internet voting what we get is a mixed report, with few nations successfully implementing while many had postponed or simply gave up the whole idea. This calls for an analysis of the challenges and concerns, both technological and sociological, which would then allow us to propose different means to deal with these.

One of the major concern raised against i-Voting, which is also the central issue that the paper is engaging with, is its insecurity, potential for violating voter privacy and lack of transparency. Rachel Gibson in her work ‘Elections Online: Assessing Internet Voting in Light of the Arizona Democratic Primary’ divides the security concerns of an internet voting system can be mainly divided into three broad categories [8]. The first which is termed ‘authentication’, points towards the difficulty in ensuring the claimed identity of the voters. Some critics are of the opinion that even with a more rigorous authentication procedures, the i-Voting system provides more space for bribery and voter coercion than possible in traditional voting practices.

The second concern is about ensuring voter privacy which is in a direct oppositional relationship with higher authentication measures. The stronger authentication procedures are the more vulnerable is the anonymity of the voters. Use of PINS and digital signatures can possibly work as link between the voters and their ballots. The third category which is termed ‘integrity’, points towards the possibilities of technological interference, like Trojan-horse viruses and “site-jacking” that could have an adverse effect on the election results. With the increasing instances of online attacks targeting higher echelons of power had forced democratic sympathizers and technicians to think about more secure i-Voting systems.

A much more major issue from a sociological perspective is the question of “digital divide” that makes the already underprivileged more so. The concern over “digital divide”, recently have taken a lead pointing towards the extreme disparities in the digital literacy of various sections of citizens of different countries. The arguments that expresses the possibilities for an increasing voter turn outs are often received with the parallel possibility for an increasing digitised divide in the election procedures. A fundamentally unequal situation will be created in the citizen’s engagement with the most important foundation of democratic politics. Similarly important is the concern about the effects increasing virtual relations could have on the quality of democratic participation. It is widely opined that virtual i-Voting could be pernicious for it reduces every risks associated with casting votes, confining a voter to his own PC, providing a possible ground for an elimination or bringing down of face-to-face democratic engagements, which is already on a decrease with the increasing reliance on mass communication medias for various democratic procedures and participation [9].

Ever since, i-Voting, gained a central stage in the discussions on electoral procedures, political scientists and technocrats had expressed their various concerns, among which the above discussed ones have had a space in the debates across nations. The net result is not a devaluation or a naive dismissal of i-Voting, instead it has triggered a more positive approach leading into researches and scholarly studies intending to present proposals for a better i-Voting system. Chuan-Kun Wu and Ramesh Sankaranarayana in their work 'Internet Voting: Concerns and Solutions' dealing with technological security concerns associated with i-Voting and presenting their solutions argues 'technically those concerns can be eliminated with current technologies' [4]. We also have experiences of successful experimentation and subsequent implementation of i-Voting in countries like that of Estonia and Switzerland. The following chapter will elaborate the points raised through a brief analysis of i-Voting experience of Switzerland.

2.1 Case Study: Switzerland Model of i-Voting

Switzerland is one of the few among the world countries that had successfully implemented electronic voting system. A close study of the process of its implementation, the discussions and concerns expressed, its current status and future prospects and challenges would enable us to look into the various facets of digitised voting system. Initially looking into the peculiarities of Switzerland's voting system and democratic model, and trying to trace the history of i-Voting, this chapter focus on the issues of security and transparency that reflect on the debates and discussions that stemmed around i-Voting in Switzerland.

Discussions around internet voting took stronghold in Switzerland in the 1980's, when internet voting occupied a central stage in the European discussions about, modernizing elections. Today, Switzerland is way ahead of other European countries in actualizing this goal. The Swiss democratic system is unique among the modern democratic nations for its insistence on direct democratic participation parallel to representative democratic system, thus regarded by political scientists as a 'semi-direct democracy'. The Swiss political system is divided into three levels, federal (national), cantonal and communal, organized in a sophisticated federal structure granting communes and cantons power of self-determination with minimum interference of the federation [10]. Being a multi-lingual and multi-religious society the Swiss political system is organized as a responsive and inclusive polity which is most reflected in its electoral practices. Any innovations and policy changes in this arena necessarily happens within an already existing system shaping itself in accordance to that system [10].

In February 1998, the Swiss Federal Council adopted "Strategy for an information society in Switzerland" laying the foundation for its journey towards e-governance, "aiming to make Switzerland one of the leading countries in this realm". From then on, a number of loosely connected specific projects are undertaken and carried on by various governmental segments, on local and national levels [11]. The “information society", the inter-ministerial coordination group assigned by the Federal Council to study the possibilities towards e-governance, proposed an action plan including two major projects. While the electronic desk is suggested exploiting online channels for general administrative procedures like tax paying and military services the second project, "e-voting" projects, presented a more direct e- intervention into the democratic system of an already well developed democratic model [12].

In the Swiss case, a number of characteristics of the electoral system and some specific concerns widened the possibilities for adopting e-voting opening up a space for creative discussions and engagements in the peculiar federal and democratic system of Switzerland with large number of polling procedures, both electoral and issue voting, the prospects of technology in minimising the organizational and economic burdens was strongly stressed. Also important is Switzerland’s experience in successfully implementing and organizing distant votes through postal service helped to increase voter turnout over the course of time. It is as well argued that different from other western countries, in Switzerland, with long tradition of public voting, the fears and norms concerning secrecy in voting is much less. The most pronounced argument expressed by political scientist and politicians supporting the adoption of internet voting is the prospects it holds for a shrinking voter turnout, especially among the youth [13].

Backed by its 'postal' experience in virtual voting, the Swiss confederation, in 2001 decided to support and work towards implementing "internet voting", inviting interested cantons to come forward to initiate the project in their respective cantons. In its initial report to the parliament the Swiss government employs the French term "vote electronique", which instead of simply denoting casting of votes via internet, refers to a much broader democratic concept, where the facility will be widened encompassing other unique civic political rights of Swiss citizens like signing of initiatives and referenda [14].

The pilot projects in the experimental phase was volunteered by three cantons, Geneva, Neuchâtel and Zürich, and was restricted to some municipalities of these cantons, owing to peculiar federal character of Switzerland where a nation-wide single system was not in par with structural organization of the country's democratic participatory system, in general, and election process, in particular. Thus a general national analysis of Swiss e-voting system is impossible. For any scholarly approach it is binding to look into the diverse experiments of the different cantons and the diverse results it had yielded which would then allow us to develop a general analysis of the prospects and challenges of e-voting.

Fernando Mendez and Uwe Serdult, in their work 'From Initial idea to piecemeal implementation: Switzerland's first decade of internet voting reviewed' compiled in the edited volume Design, Development, and Use of Secure Electronic Voting Systems, understands the Swiss path to e-voting as the 'Helvetic route', which allows a comparative analysis of three competing experiments [15]. They argue that Switzerland unlike Estonia, who implemented e-voting as generalised system of electoral participation on a full scale, adopted e-voting through a piecemeal approach. Of the three cantons Geneva with an already existing centralised voter registry and a more centralised canton system attracted attention for the wide success it had achieved in its path towards e-voting.

In the 2009 referendum voting the voters of Geneva overwhelmingly welcomed e-voting system adding to the authorities' strive to establish itself as the 'E-capital' of Europe. Zurich presents a different example wanting to prove the feasibility of e-voting even with a decentralised voter registry, based on a system, virtually centralised and a sharing of data between the municipalities and canton. Unlike Geneva, the electoral process was maintained by a private company. However, owing to the technical and economic setbacks, and inability to meet the expected voter turn- outs Zurich dropped the plan in 2010, only to re-join in 2014. The Neuchatel, presents yet another model, different from both the others since, from its initial stage it is subsidized by Federal Chancellery and is completely integrated into E-government portal that allows the citizens a direct interaction with the government. Despite the initial failures in realizing increased voter turn outs the Neuchatel model is a success with no major impediments. However, the financial issue remains as an important question in continuing and furthering the system [14].

Despite the initial success and plans for further enhancement of e-voting in Switzerland a number of concerns are still strongly pronounced. Arguments for e-voting stressing on the possibilities it offers for augmentation of voter turn outs and voter quality that would in turn enhance the quality of the democratic process is more or less challenged by a set of counter arguments, among which security concerns take the lead. The Swiss federal system ensures the voters secrecy and confidentiality. However the e-voting system would need identity verification of the voters to log in so as to ensure 'one man, one vote' principle. A strict separation of voter's identity and ballot could only ensure the confidentiality of the citizens' ballots. Moreover, e-voting also increases the risks of manipulation of votes and other technical security threats. Increasing incidents of web spoofing, hacking and system failures demands a more cautious approach towards digitising elections [16].

Lack of transparency also remains as a central issue of concern as "all processes of data generation, transformation, and storage occur in black boxes that are often not fully transparent even for technical experts" [17]. The highly technical system open only to the experts would lead to a decrease in the role of 'average' citizens in vote counting and other related processes [11].

Other concerns like that of 'digital divide' and lack of a comprehensive framework for a digitised democratic system has attracted much attention. The negative impacts of digitised elections in maintaining a creative democratic environment, both in democratic participation and opinion making is much discussed. The term "fast-democracy" is coined by Engi and Hungerbühler to describe the tendency, where an e-voter sitting at the comforts of his home would no longer feel the need to step out to participate in public conversations on individual opinions and decisions [18]. The easy voting facilities offered by e-voting is as well feared for encouraging voters to cast their ballot with little thought and reflection.

The results of the pilot experiments in the three cantons more clearly reflects this ambiguous position of Switzerland vis-a-vis internet voting. We see huge difference in the experiments of different cantons, also, within the different cantons in different time period. A much noticed trend was the novelty effect, where the voters experimenting with the new system once or twice revert back either to postal or ballot systems. This was observed in both Geneva and Zurich systems. Even in Geneva system, which is considered as the most fruitful experiment, the internet voting system had to be halted for two years in 2006 and 2007 that adversely affected the voters' confidence. However, a closer study of the diverse reactions and systematic planning had helped Switzerland to overcome the challenges and move towards an extension of the e-voting services to other cantons and fields [9].

What is interesting in the Switzerland case is the diversity of its experiments and the analytic possibilities it offers for a study on e-voting that would help to generally reflect, on a comparative scale, about the experience of other countries with e-voting system. Along with concerns and discussions relating to peculiar features of Swiss electoral procedures, e-voting experiments in Switzerland had also opened up larger debates and discussions on the very idea of digitised democratic system and the ‘technological shift’ in the modern democracies. The crux of these discussions remains the prospects and challenges it offers for a better democratic polity and social system.

Chapter 3. Estonian i-Voting Model

The i-Voting experience of Estonia is noted by scholars as giving fresh insights into the future and prospects of digitising democratic politics in general and internet voting in particular. The intentions to implement i-Voting in Estonia was announced as early as 2001 which was realized in 2005 for local elections as an additional voting channel thus establishing itself as the first country to use Internet voting for political elections. Today, over 30% of Estonian votes are now casted online [1].

Internet voting is a revolutionary process which redefines the democracy. It ensures the magical rights to a person to cast vote from anywhere, the only thing required is an internet connection on a smart phone or a computer. The process is really strengthening democracy by ensuring the participation of technophile youths. Recent studies conducted in several parts across the globe points out the positive role of internet voting in increasing the voting rates [19].

France, Switzerland, Netherlands, United Kingdom and USA are some of the major countries who experimented i-Voting. However, Estonia is the country which use internet voting as the best alternate. Since 2000, 8 elections in Estonia used the system of i-Voting. The local election in October 2005 was marked in golden font in the history of democracy due to the introduction of internet voting. The parliamentary elections in 2007, 2011 and 2015 also used the option of internet voting [1].

Internet voting is a national pride for many Estonians. But, Central Party, a major political party in Estonia, demands i-Voting should be abandoned [20]. Estonian internet committee have announced that the system “is as reliable and secure as voting in the traditional way” [21]. Several critics in and out questioned its credibility [21] [22]. Absence of end–to-end verifiability, complicated set of procedural controls which are inadequate to achieve security or transparency and cyber-attacks are the main argument putting forward by the critics. These details will be discussed in the chapter four.

The working of Estonian voting system can be summed up as follows: A voter who identifies himself with his identity card logs in to the voter server. The server checks the voter's identity card and provides him with the ballot paper on which he signs his encrypted vote which is verified by the voting server. Further, at the time of tallying, the encrypted votes are scrambled, which is finally decrypted by the HSM and counted.

3.1 Voting Process

Unlike other countries, there are mainly four features which makes Internet voting a best alternative in Estonia: the widespread internet usage, effective legal structure to address the internet voting issues, digital authentication of voters through the identification system and a healthy political consciousness [23]. The Digital Signature Act (DSA) of 2000 provides individual a right to use digital signatures in online transactions including voting. Apart from USA which also has a DSA, the key feature in Estonian DSA is the digital certificate embedded in the card which can be used for individual authentication when combined with the unique personal identification number (PIN). The smart card reader inside the user’s computer port reads the digital signature on the identity card. The user can connect to the government register and authenticate the unique PIN and card. The ID card can be used for all government transactions including i-Voting [24].

Normally, the duration of Estonian Internet voting is seven days. Estonian ID card and the Pin associated with it is essential to cast vote. Those who wanted to vote online should login in to ‘www.valimised.ee’ and authenticates the ID and cast the vote, after that the process is as follows, the ID card is inserted to the smart reader and the first PIN is typed [25]. In this stage, the voting server queries a server with the voter registration database; the voter would be then sent to a page which shows the candidate list. A candidate can be selected from the list and voter can confirm the selection by entering the second PIN. At this stage, the voted ballot’s encryption take place. Upon entering the second PIN, the voter would effectively sign something like a digital version of absentee ballot “envelope”. This “envelope” would later be removed from the actual ballot if he had not cast a paper ballot. One of the voting server will verify if the server is undoubtedly correct. If yes, the encrypted ballot will be transferred to another server and is stored till tabulation. The voter would finally receive a confirmation message on the browser [23].

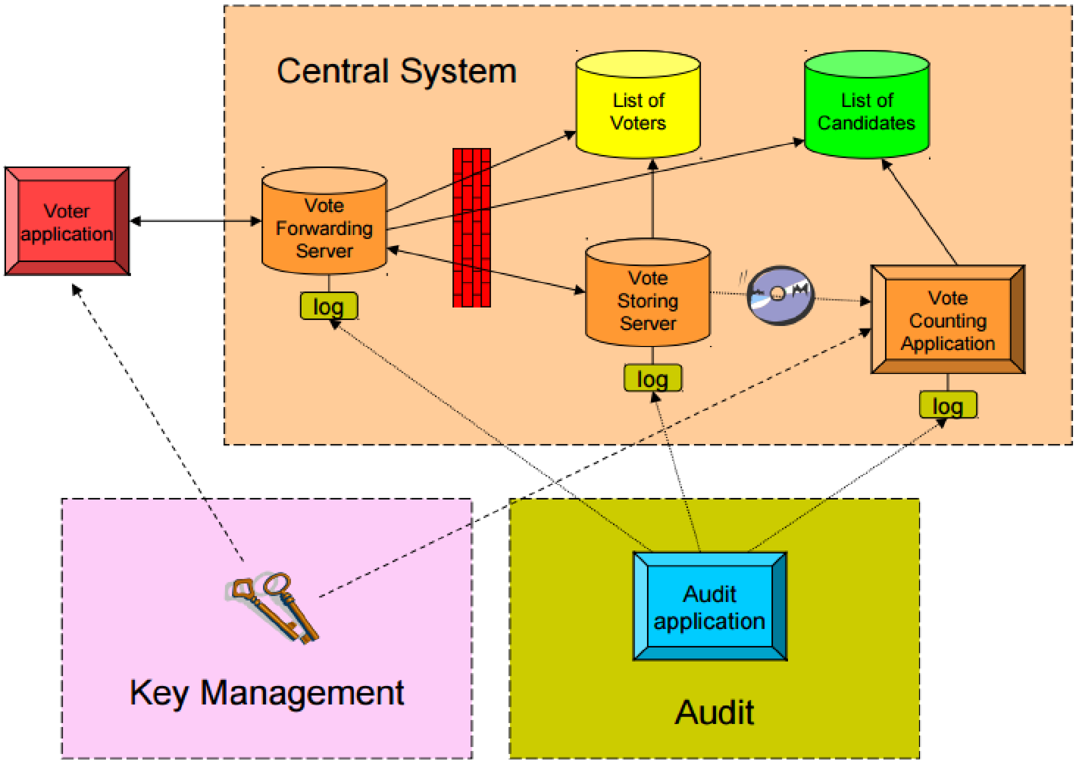


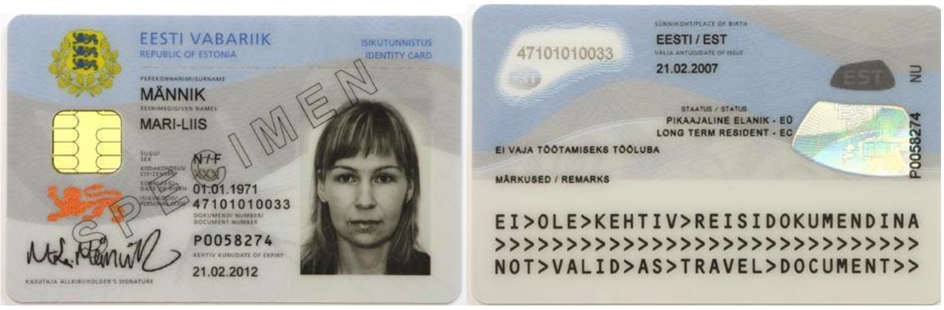
Figure 1. Architecture of Estonian i-Voting Model [26]

If a voter also had voted a paper ballot, the voter's internet ballot would be tagged making it unable to be counted on the election. Internet votes are counted, within the last hour of Election Day, in the Estonian Parliament building. To ensure privacy, all communication devices of observers are confiscated and the doors are sealed and strict security measures are taken. A Secure hardware module is used to decrypt the votes. The decrypted votes, which is transferred into a CD-ROM will then be tabulated by the election committee in front of the observers, including auditors from KPMG Baltics (a professional services firm providing audit, tax and advisory services) [23].

3.2 Estonian National Identity Card

The national ID card is the backbone of internet voting in Estonia. More than 90% of Estonian populations have an active ID card. The idea of a digital ID card was emerged in 1994 in the institute of Cybernetics. Estonia begun the initiative to develop the ID card in the year 1997. Tarvi Martens, Ahto Buldas and Jaan Priisalu presented a draft in front of the Citizen and Migration board and the Informatics centre, specifying a period of at least 15 months for the necessity preparation. On May 1998, several representatives of the private sector met under the initiative of Tonu Liik, Advisor of the Ministry of Internal Affairs. A “committee for development of the Identification Certificate and its technical specification” was created based on the directive of the Ministry of Internal Affairs. On March 1999, Estonian Informatics Centre created the ID card work group (TK4-ID). Estonia used its first ID card in January 2002 [27].

National ID card is issued by the Estonian Government’s Citizen and Migration Board (CMB). ID card is mandatory for all Estonian citizens above the age of fifteen. The ID card carries out mainly two functions; physical identity and electronic identity. It can be used as a physical ID just like in other countries and also it can be authenticated electronically to website and networks, digitally sign communications and transactions as required. Estonian ID card is used for legal travel, health insurance, banking, digital signatures, i-Voting, access to government databases and e-prescriptions. The front side of the card contains holder’s signature and photo and also the name, national ID code, birth time, sex, Citizenship, card validity and residence details of the card holder (if applicable). The backside contains the birthplace, card issuing date and card and holder data in machine readable (ICAO) format [28].


EESTI VABARIIK
REPUBLIC OF ESTONIA
ISIKUTUNNISTUS
IDENTITY CARD
PEREKONNANIMI/SURNAME
MÄNNIK
EESNIMED/GIVEN NAMES
MARI-LIIS
SUGU/SEX
N/F
KODAKONDSUS/CITIZENSHIP
XXX
SÜNNIAEG/DATE OF BIRTH
01.01.1971
ISIKUKOOD/PERSONAL CODE
47101010033
DOKUMENDI NUMBER/DOCUMENT NUMBER
P0058274
KEHTIV KUNI/DATE OF EXPIRY
21.02.2012
KASUTAJA ALLKIRI/HOLDER'S SIGNATURE
SPECIMEN

47101010033
SÜNNIKOHT/PLACE OF BIRTH
EESTI / EST
VÄLJA ANTUD/DATE OF ISSUE
21.02.2007
EST
NU
STAATUS / STATUS
PIKAAJALINE ELANIK - EÜ
LONG TERM RESIDENT - EC
EI VAJA TÖÖTAMISEKS TÖÖLUBA
MÄRKUSED / REMARKS
P0058274
EI>OLE>KEHTIV>REISIDOKUMENDINA
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
NOT>VALID>AS>TRAVEL>DOCUMENT>>

Figure 2. Front and Backside of Estonian ID Card (Source: https://www.politsei.ee)

Estonian ID card contains two certificates, one for authentication and the other for digital signatures. The two associated private keys in the card are protected by separate PIN codes. The Certificate, which binds the public keys are stored in an LDAP (Lightweight Directory Access Protocol) database and on the card. The nature of the ID card is universal and there is no restriction to it. It can be used in any forms of communication varying from person to person, organizations and government [10]. Mobile phones with special SIM can also be used for digital signing and authentication. A system called mobile ID is developed for this purpose. In the 2015 election around 12.2% of the Estonian i-Voters casted their vote using these facility [1].

3.3 Verifiable i-Voting in Estonia

Comparing to the traditional paper based voting, lack of physical evidence makes e-voting risky. The electronic ballot can be easily tampered with a bug. The connecting of voting devices and digital ballot box in the Internet makes it attack prone from the network. Estonian i-Voting system have been in attention as many critics pointing out the security features main among it is in its original form, the voting system gave no reliable feedback concerning whether or how the vote was actually received by the server. During the 2011 elections, a student developed several versions of malware which is capable of blocking or changing the vote. The basic protocol's simplest nature makes the manipulation unnoticed by the voter [29].

After the 2011 elections, the OSCE/ODIHR report addresses these problems. The report states: *The OSCE/ODIHR recommends that the NEC forms an inclusive working group to consider the use of a verifiable internet voting scheme or an equally reliable mechanism for the voter to check whether or not his/her vote was changed by malicious software* [30].

After this, a verification system was proposed and implemented. The verification was first implemented in the 2013 local municipal elections. At the initial stage, only Android OS 2.2 and higher were supported as the mobile application platform. 136,853 e-votes were given and 133,622 counted. Verification was utilized by 3.4% of internet voters. In the latest 2015 Parliamentary Elections, around 4.3% i-Votes were verified [1]. This shows there is a steady increase of interest in the voters about verifying their votes.

Chapter 4. Security Analysis of Estonian i-Voting System

Empirically there is enough evidence to undermine the use of Internet for any reliable system. Perhaps the most fitting example for the point made, is Stuxnet. If a system can be brought down when it is off line it does not take great feats of engineering to do the same on a system which is online and ready to be abused [31]. Confusing the user with innumerable protocols and layers of encryption is defeated of its efficacy, when an endpoint after all has to decrypt and make sense of the information being sent. That being said it does not mean that they are meaningless. It simply implies that when deciding upon a system that has any binding implications such as a political election, which elects a government into power there has to be strict insight into the same.

Convenience has serious drawbacks in terms of security. And in this case the convenience is analogous to the comfort of being at home for a national election. The idea of a digitally controlled election does not make sense if there are for instance innocently infected client computers that cast a vote, or can even change a vote at a later instance for that matter. The idea behind effecting a change of vote is justified and quite eloquently made, as to where a vote caster could be coerced into making a vote not true to his actual intentions owing to a third party. Thus the implication of making the vote process coercion resistant introduces a few lose ends. Procedural controls also is a concern for systems such as these, as alterations could lead to serious flaws in the entire system.

The idea that an infiltrated voting administration would render both physical and cyber voting system unusable, is the main contention of currently employed Internet voting system. The need to build a better voting system with current technology eludes us still, but not a far-fetched idea given the sense of End-to-End verifiability and protocols such as Zero knowledge protocol.

Analysis Method

For our primary analysis and towards reasoning into the negative causal defects of the Estonian voting system let us look into the work done by Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. Alex Halderman in "Security Analysis of the Estonian Internet Voting System" [21]. There is every reason for the authors to push a sense of caution to their readers so as to why internet voting is not at all a good idea for a National Election. Structurally we can layout our analysis into a series of small steps.

Background

The Estonian I- voting systems uses the National ID card infrastructure, which is already in use in the country for a plethora of services ranging from bank transactions to various governmental transactions. The card is loaded with the ability to digitally sign and authenticate documents. It contains two sets of RSA key pairs, one of which would authenticate and the other which would give or provide digital signatures. The private keys in the card cannot be exported and thus all the required operations are done on the chip embedded in the card. The public keys are also shared on a public LDAP database, which is use with the former helps establish the identity of the owner.

4.1. Voting Infrastructure and Protocol

The Internet voting process is based on various stages. Primarily it is uses what is known as the double envelope system so as to provide both security and anonymity. The traditional approach for the double envelope system was developed in order to make a smooth process for absentee voting. So in short, the double envelope system is a system designed to protect the anonymity of the voter, and also simultaneously make the voting process secure. For as security and integrity go hand in hand, the need for the traditional role players such as Alice and Bob to know each other. Double envelope system removes the need for Alice and Bob to know something in common, yet make a decision. Say Alice casts a vote and Bob is at the other end counting the vote. However if Bob is tallying the vote he comes to know that Alice cast a vote and that her choice was so and so , if Alice gave her cover directly to Bob, that is. However on the other hand if Alice made 2 covers, posted the real vote inside a cover and that whole package in another cover, and used an intermediate such as Charles, who would strip one cover and then pass it over to Bob, then Bob cannot trace back the route, to Alice without Charles, and thus can count the vote in absence of this knowledge.

The entire framework of the voting process is tightly bound with public key infrastructure. As such all authentications is based on the principles of the former.

The authenticating party infrastructure or rather the server side infrastructure is mainly four machines [21].

1. A vote forwarding server
2. A vote storing server

3. A Vote Log server

4. A Vote counting server

The software for the client is published for Windows, Linux and Macintosh systems. The clients respectively could be downloaded from a prescribed website. “Apparently the client is tailor made for each election and uses an election specific public key” [21].

And primarily three processes are of concern

a. Vote Casting Process

b. Vote Verification Process

c. Vote Tabulation Process.

A client with the client software wishing to cast a vote, first authenticates the process with a PIN and his/her ID card. Further a TLS connection is established by the client to the server and connected to the forwarding server (As mentioned in the server end infrastructure). After confirming the validity of the voter the system then returns the defined set of candidates for the voters region. Utilizing the protocols, the user picks a candidate and the client encrypts the message with the voter’s private key. (RSA public key infrastructure methodology).

As a counter action towards any forceful voting/coercion the process is repeatable for a set number of interval. However this is to be noted, as in an E2E (End-to-End verifiable) scenario, this would provide additional overheads on the system.

Before counting or tabulating the votes it is to be observed there is a verification feature provided. The process lets the user verification of up to a period of 30 minutes and to a count of three time after a vote has been casted. The tabulation itself begins after the online process has ended and the encrypted votes are transferred to another standalone machine from the storage server. Obviously any traces back to the user such as digital signatures are removed and only the encrypted votes are transferred henceforth.

Now there is something to be noted at this point of time. The process of adopting the double envelop standard brings the problem of End-to-End Verifiability, a property that is a must do, in today’s information age, and thus of Internet or Online voting. Concepts such as mix-net can be used to overcome this problem of no E2E verifiability and additionally more transparency can be brought into the picture.

4.2. Probable Risk Areas

4.2.1 Protocols Relating to Procedure

Election officials need to have strict protocols in order of all possible events happening. Failure to adhere to such well-defined protocols or failure to implement any of such protocols can make the officials resort to undefined practices and push the process in serious jeopardy. A report to the 2013 municipal elections in Estonia claim officials restarting bypassing drive error messages which was or otherwise could be a serious tampering concern.

4.2.2. Relating to Operations

Infection of computers during a pre-election computer can relate to comprising the entire election. Thus care must be taken or rather proper operational protocols must exist in preventing a security breach. Possible entry points for operational related mishaps are

a. Pre-Setup for Election
b. Regular/ Maintenance Tasks
c. Counting/Tabulation Process

4.2.3 Code Vulnerability

The i-Voting software for the server has approximately 18,000 lines of code in various languages and a large number of libraries that are of different sources. The fact of using shared libraries brings along with it known and unknown bugs along with the integration of this into i-Voting software. Apart from this there are vulnerabilities specific to the software itself.

One amongst them that was found in the 2013 version and described by the security team who did an analysis was the client side HTTP request. A DOS type attack described as follows

"If a client sends an HTTP request containing unexpected header fields, the server logs. The field names to disk. By sending many specially crafted requests containing fields with very long names, an attacker can exhaust the server's log storage, after which it will fail to accept any new votes. In the 2013 election, the size of the log partition was 20 GB. We estimate that an attacker could fill it and disable further voting in about 75 minutes" [21].

A DoS attack are always possible for any voting system and it is too common. But Disruption attacks can be also be a type of Dos attack in this scenario which is difficult to prevent. The positive side being, DoS attacks are always easy to detect. In case of a Disruption attack which is carried out in a covert manner, where the attacker try to delay the certification of the election [32].

4.3. Defining a Threat Model

The thread model for an election infrastructure must include and range from state sponsored attackers to well-funded criminal organizations or a dishonest election insider, all for various benefits of their own. That being mentioned the idea here is to communicate that a government process as important as this would definitely attract threat creators with high amount of resources both financially and time wise. Buying zero day vulnerabilities for above mentioned shared dependencies is but a matter of sooner or later.

Designing a threat model is a kind of laxative measure in terms of i-Voting systems. The idea sometimes is to hide the architecture in its entirety thus leaving the system less prone to detailed analysis and reverse engineering schemes. However as always in cyber security a well-informed user is always in command. Mere obfuscation sometimes do quite the opposite and leave gaping holes in the system as a whole. The Estonian i-Voting system architecture we have at hand is a high level schema. For simplicity we skip on elaborate models, which require intricate knowledge and more resourceful analysis of the Estonian i-Voting system which is inclusive of the PKI (Public Key Infrastructure) National ID and Mobile ID infrastructure.

The task of a describing threat model is generally in 3 phases, as deemed by OWASP standards [33].

1. Decomposing the Application/System, ie understanding the working of the i-Voting system.
2. Ranking and classifying threats. We use the offensive STRIDE model to categorize attacker centric threats. Asset centric and software centric threats may also be considered.
3. For phase three we utilize the listed information to gain insight and threats and further determine effective countermeasures and possible mitigation strategies.

Phase 1.

Below is a simple DFD (Data Flow Diagram) describing User Login.

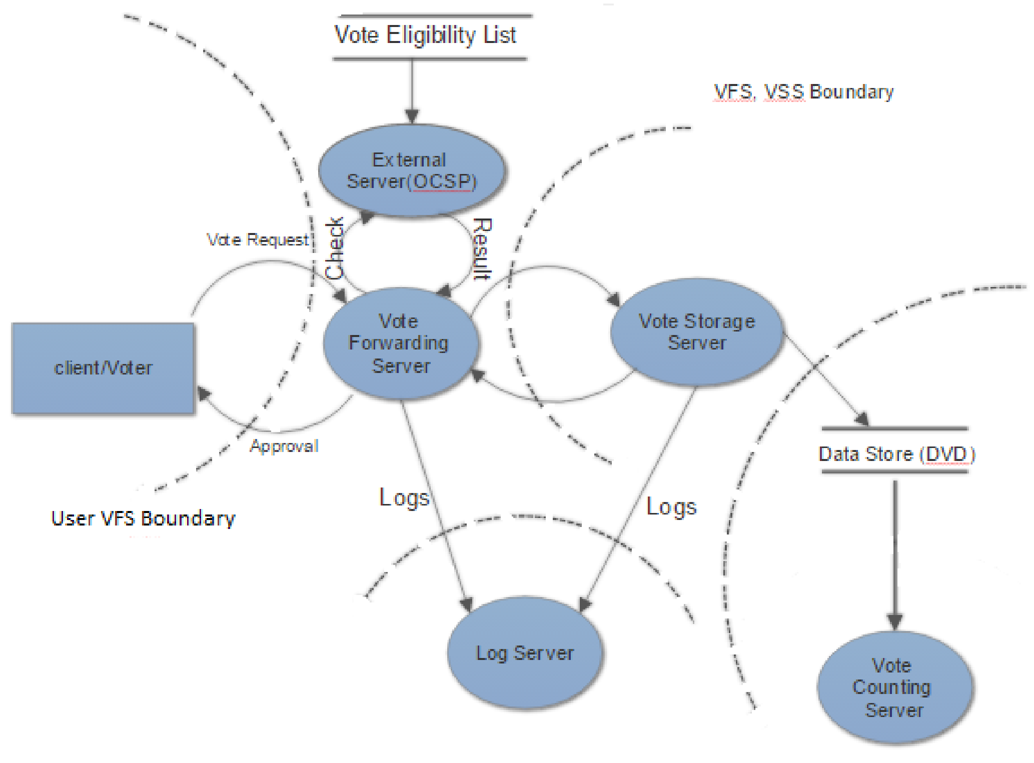
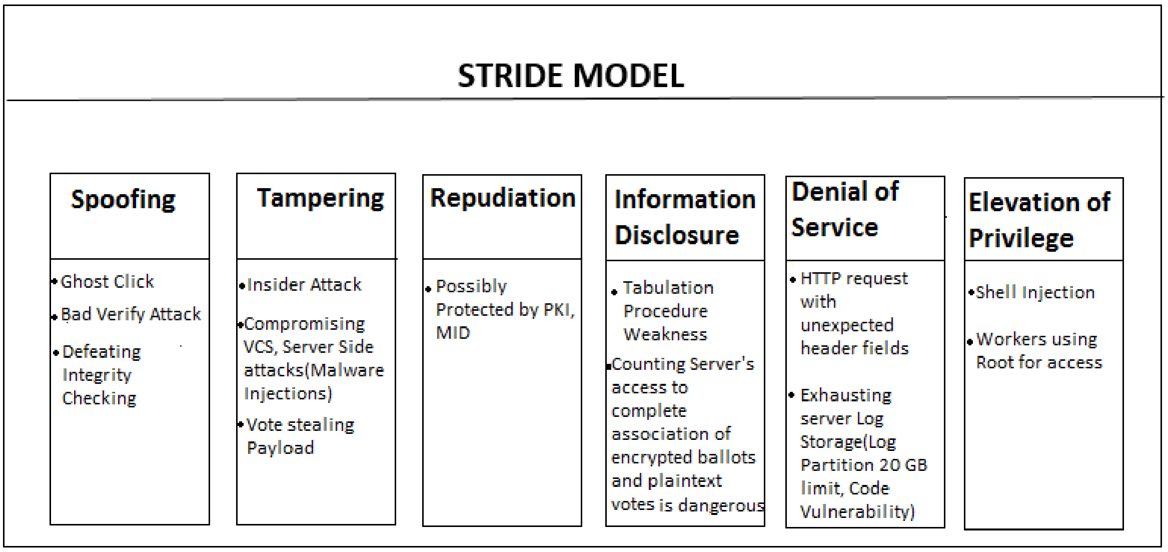


Figure 3. User Login DFT [21]

Phase 2.

A STRIDE model categorizing the threats posed by an attacker is depicted below.



STRIDE MODEL

Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
- Ghost Click - Bad Verify Attack - Defeating Integrity Checking	- Insider Attack - Compromising VCS, Server Side attacks(Malware Injections) - Vote stealing Payload	- Possibly Protected by PKI, MID	- Tabulation Procedure Weakness - Counting Server's access to complete association of encrypted ballots and plaintext votes is dangerous	- HTTP request with unexpected header fields - Exhausting server Log Storage(Log Partition 20 GB limit, Code Vulnerability)	- Shell Injection - Workers using Root for access

Figure 4. STRIDE Model [21] [34].

Phase 3.

“Thus the main idea, introduced by E2E is not to create an unbeatable system but rather employ a transparent system that alerts its owners if it has been abused.”

It is highly impossible to build a system that is not impenetrable, so the best thing to do would be design and implement a system that could detect any alterations in the process and also capable of resisting major attacks.

Malicious Intents/Attacks

Attacks initiated from a client side or server side depends on the goals of the malicious user has, perhaps to disrupt or in other circumstances have a devious outcome.

Client Side

A major concern from the client side is that, client side machines are vulnerable to malware very easily. The malware could then be used to steal PINS and perhaps vote for an attacker favored voting candidate. This is commonly described as the 'Ghost Click attack' [21]. The Ghost Click attack can be further escalated to a bad verify attack as well.

Server Side

One of the major concern for internet voting systems are Denial of Service attacks and in main concern Distributed Denial of Service. The DDOS has several variants including the amplification attacks which abuse current protocols in use to take a server down, by overwhelming it with unreasonable amount of requests.

There are several and quite alarming weaknesses both technically and policy wise in the existing system. A major solution is a look towards implementation of the E2E scheme. Apparently a paradigm shift towards this goal is beneficial. Another possibility is the use of VPN type technology to create a local boundary for Estonia voters. If system designers can employ a way to create such a system, majority of off-site DOS attacks could be deescalated for a better i-Voting process.

4.4 Vote Buying

Amongst the fundamental requirements of any voting system, is the necessity of a receipt-free ballot casting process. This would ensure secrecy as the voter will not be able to prove his/her vote to a third party and thus the threat of coercion and vote-buying would be minimal. However, i-Voting systems with individual ballot verification methods ensure that the voters can verify their votes with a confirmation message, which could easily violate ballot secrecy. In order to tackle this issue, the voting systems have enabled multiple casting of votes, both online and offline, of which the last one will be counted. The current Estonian i-Voting model consists of such re-voting features which allows a voter to cast a vote ‘n’ number of times, counting only the last vote. In this case, if a voter turns up at the polling station and vote, the online vote will be cancelled and only the paper ballot will be considered. Although re-voting reduces the possibilities of coercion or vote-buying, in some situations it might not be promising enough. Considering the example of the 2015 Estonian parliamentary elections, in which around 36% of registered voters did not cast their votes, the non-voters could be highly susceptible to coercion or vote-buying as they would not be interested in the elections and would not take the pains to place a second, considering they did not vote in the first place. Here makes a case which is based on the possibility that the voters were disinterested, which is contestable. In the current situation, however, the re-voting system is able to address the issues with regard to coercion and vote-buying [35].

Chapter 5. E2E Verifiability: Requirements, Cryptography and Models

End-to-End Principle – can be defined as “in a general purpose network, applications specific functions ought to reside in the end hosts of a network rather than in an intermediary node so that it can be implemented completely and correctly in the end hosts” [36] [37]. The general idea of this concept is that only traffic should be carried out by the network core and all other additional services are to be maintained at the edges of a network by end points and the network core should not interfere with it.

5.1 End-to-End Verifiability

Traditional voting methods do not provide many benefits as internet voting. In traditional voting, a voter can only check whether his vote is cast as intended when he submit the ballot paper in the ballot box. The voter won’t receive any verification about his vote being counted as recorded. Online voting has many advantages over the traditional voting. The main being providing an evidence to voters that their vote is properly cast and the election outcome is free from any error. End-to-end verifiability should work in such a way that voters have to verify that their votes are counted as recorded without the need to trust any voting software. Also E2E verifiability helps the observers and independent auditors to check the counting process without the need for any special access to the voting process [38].

Verifiable voting protocol improves the situation by providing voters, the ability to check certain properties of their individual ballots. The individually verifiable voting protocol helps the voter to check whether the casted e-vote was correctly accepted by the ballot box. In the 2010 International Conference on Electronic Voting Technology on Trust Worthy Elections (EVT/WOTE ‘10) Stefan Popoveniuc, John Kelsey, Andrew Regenscheid and Poorvi Vora proposed a requirement for end to end verifiable elections. An end to end verification has the following properties [39]:

- It helps the voter to check whether his/her ballot represents a vote for candidate to whom he/she intended to cast the vote
- To check the valid ballot contains negative votes or over votes
- The voter can check his/her vote is recorded as he/she casts it
- Anybody is able to check the electronic tally of recorded ballots
- Voters and general public has the same view of election records

Maintaining election verifiability being the most difficult objective to achieve. There are specific cryptographic techniques used to achieve election verifiability. Usually an E2E verifiable systems use both the paper trail and electronic ways to achieve verifiability. Pret a Voter, Punchscan and Scantegrity are some examples that provides E2E verifiability that use the combination of a paper trail and electronic methods. Well each of these technics have its own advantages and disadvantages. As our main concentration is internet voting which does not require paper trail but still use the existing crypto graphical methods to produce receipts which helps the voters to verify their votes that are not corrupted and is properly recorded and counted in the voting process. The idea of E2E verifiability is shown in the figure 5.

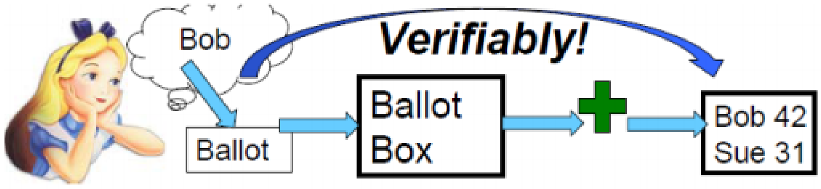


Figure 5. End-to-End Verifiability – Alice should be able to verify her vote for bob has been counted in the final election process [40].

"E2E systems generally works in such a way that verification should be possible for anyone without revealing for the system or any outsiders which candidates were voted in the election" [40]. A ballot is always encrypted at the starting stage where a voter can verify the encryption which allows them to check whether the vote is recorded correctly. The encryption also allows the system to generate a receipt to the voter regarding the recorded vote. By making cast ballots public, a voter can check the votes are collected as intended. For this the ballot has to be made identifiable to the participating voter. Only few E2E models have implemented this so far. Also an E2E voting system should satisfy the condition that only a participating voter, but anyone can have the possibility of verifying the final counting of the collected vote. The process should satisfy universal verifiability. Fig 6 shows how universal verifiability works where a voter can audit all the steps in an election process.

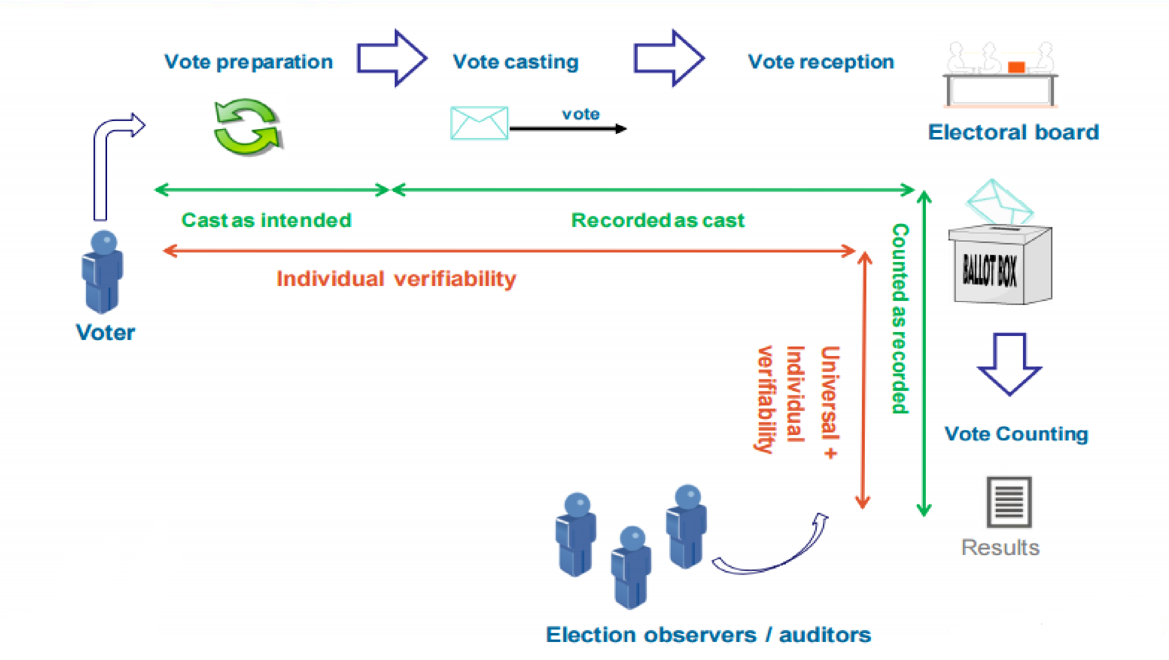


Figure 6. Individual and Universal Verifiability in Election Process [41].

Helios is an open audit system which uses crypto technics like El- Gamal and Homomorphic Tallying and it satisfy all the conditions of an E2E verifiable voting system. Helios model is explained further in this chapter. In a voting system, in order to protect communication between the voter’s device and the election server and for verifiability for the voters, various cryptographic technics are used.

5.2 Requirements for an Ideal End-to-End Verifiable Voting System

For an ideal E2E verifiable voting model, there are specific requirements to be fulfilled. These can be divided in to two categories, they are technical and non-functional requirements where technical requirements are used for the design and implementation of the voting system and non-functional requirements have no control over the system and it is more comprised of working procedure of the election and the set of guidelines imposed on the system by the external entities [42].

5.2.1 Technical Requirements

Technical requirements are divided into ten categories [42]:

- Functional - The main aim of functional requirements deals with casting and recording of the votes along with the voter records. These requirements should always fulfil the criteria that the system should be able keep data of casted voters even if there is a disruption or failure of the servers.
- Receipt freedom is another functional requirement. It means that for the voter it must be impossible to prove how she has voted. “Any person can create digital evidence when voting, but even then it must be impossible for voter to prove how she voted. E2E protocol with a receipt freedom can be recorded. Therefore, it must be allowed for the voter to vote many times, which means only the last ballot will be counted. Also, it is important that an observer can independently make sure that the ballot was cast. It must be ensured even when the voting computer is not followed by the protocol and in a way that is easy to use” [42]. There are two different election formats: one is where the voter can cast multiple ballots and the last ballot will be counted and the other where voters are not allowed to cast multiple times. It is important to maintain voter’s anonymity in the election. During the election it is important to maintain real time connection between a voter and their ballots. [38].
- Usability – The usability of the system has a significant matter and many requirements of the system are related to it. After casting the last ballot, a voter must be sure that her ballot will be counted by receiving a last note confirmation. If a voter is not sure, she must be able to vote again. Before deploying a new E2E system, it must have been tested and the results of the usability must be available to everybody before the elections [42].
- Accessibility – One of the main goals of E2E system is to make voting easier for people with disabilities. Developers have several aspects to consider: system must be compatible with other technologies, system has to be developed in a way that people can use accessible devices and it is necessary that the system has voting options that are adapted for voter’s needs. In addition to usability testing it is also mandatory to test accessibility which also must be made public before the Election Day [38].

- Security and Authentication – These two requirements are closely related and form the biggest set of technical requirements. The data integrity must be safe throughout the system, it must keep up the integrity of the voter's information and it should be possible to find out where the information came from. System security equipment must be under the control and checked regularly. Security being the key requirement for an ideal i-Voting model safeguarding the integrity of election data and maintain voters data protected. Security should ensure the system is capable of resisting large scale coordinated attacks to the system as well the voter's devices. It should also address authenticity of election as only eligible voters are allowed to vote. Fulfilling the requirement of transparency requires maintaining public trust by giving voters and observers the chance to check elections results are correct and election was conducted accordingly. By putting the source code, logs and all documentation for public review will ensure transparency [42].
- Auditing – Compared to other voting systems, E2E is one of the most outstanding system because its ability to perform comprehensive audits of system activity. Audit features must be implemented into all levels of the system from the beginning. Audit logs must be locked and as complete as possible. "Potential issues and threats are supposed to be reported by the system making the data available to the election observers in real time. When there occurs any problems with legitimacy of all the notes, it must be able to report the number of affected ballots"[42].
- System operational – It is a requirement which ensures that the system is ready and updated. Manifests of the system used to run any election must be published and include information about well-defined procedures. These procedures must be followed before every election period by election officials. They also need to check all equipment and approve it for use. During the election period, the key equipment must be kept safe by election officers. They have to have a back-up plan for system failures. Elections staff must be always ready to react, if there occurs any problem during the election. Moreover, they need to make a report after every election containing every problem which came up during the election. It must be published shortly after the election [42].

- Reliability – E2E system has strict reliability requirements to make sure that the system is levelheaded while it is under normal conditions and while under attack. To control whether all the requirements are satisfied, they are doing mock elections. They test whether the back-end components of the system are able to run continuously. "During the election period, the system must be accessible 99.9% of the time and it must be able to recover from any failure within ten minutes. The system must be able to survive DDos attacks and works perfectly"[42].

- Interoperability and certification – E2E system is ought to use open data and communication standards for interoperability. Election Markup Language should be used for data interchange and configuration with the system. It is a necessity for election officials to publish the log data for the system and the documentation. All the functional requirements mentioned earlier must have and associated set of automated tests. It is need for providing evidence for certification of an E2E system.

5.2.2 Non-Functional Requirements

Non-functional requirements are divided into five categories [42]:

Operational – Operational requirements deal with seven different issues which is shortly described below

i. Voter assistance – This can be fulfilled by giving support and guidance to all voters through a widely-known communication channel. Voters must be informed how they can protect their privacy more efficiently.

ii. Election and registration timing – All stages of the election must be clearly stated with a timetable.

iii. Voter registration – Election officials have to update voters' register regularly. Voter has to have an access to her information on register and she must have an opportunity to ask corrections.

iv. Candidate nominations and lists – All voting options on electronic ballots must be presented equally.

v. Receipt freedom – Receipt freedom is a must in an E2E system. The voting machinery can be supervised or unsupervised. If it is supervised, then immediately after casting a vote, voting information must disappear. In an unsupervised environment, there is a possibility to record voting. Third parties must not be able to use these.

vi. Election integrity – An E2E system will be made available for testing by officers and voters before and after elections. After the system has stopped accepting electronic ballots, it is allowed to show preliminary results. When the voting period has ended, the system must make public the tally information. The counting process will be kept recorded by the system and if some votes get affected, then it needs to be recorded that their integrity had been violated.

vii. Openness – Any deployed E2E system should be functioning as an open system. For developing systems and procedures for future elections, it must be able to apply conclusions drawn from the audit process for developers and election officials.

Procedural – It is greatly important that information about how some procedures, such as provisioning, certification, maintenance, availability and use, work and that the specific components of a system are disclosed. Electoral officials and an independent body must work closely together. After introducing the system, election officials must make sure that voters understand everything and are enough educated for voting. Also, their task is to be sure that the system is genuine, reliable and secured. Election officials and people who they have given a right for that are the only people who have an access to the central infrastructure. The system must keep the votes protected and sealed until the counting process begins. Besides that, recount must be possible as well as partial or complete re-runs of elections [42].

Legal – To avoid potential legal problems with unintended consequences, legislations have to include requirements such as the system must be easy to use for voters, electronic voting must hinder voter participation, and system should maximize the opportunities they have created for people with disabilities. It must be ensured that only one vote by each voter will be counted. Voters must have a possibility to change their choices during an electronic voting before casting their vote and they must have a chance to stop the casting of the ballot without recording the earlier votes nor making any public disclosures. Manipulating a voter during the voting process is not allowed and system has to pay close attention to it.

Assurance – First requirement is that client side software must be totally free of known bugs and software stack combinations. Voter authentication should be always directly proportional to strong security. All the aspects of Internet voting system must be available for everybody to download.

Maintenance and Evolvability – Election officials must have the possibility to update the election system to make it more comfortable for changes.

Voter Privacy: *can be defined as the decision of the voter should remain anonymous and coercion resistant.*

To ensure voter privacy, there are steps to be followed from the moment voter casts his vote till it reaches to the server and also when the votes are decrypted. Many argue that encrypting the transmission channel of the vote can maintain voter privacy. This argument can be proven wrong as the votes are decrypted in clear texts, an unauthorized person can easily read a clear text in case of any privacy breach giving an opportunity to manipulate the votes.

When it comes to individual verifiability and receipt-freeness there is a serious disagreement. Most receipt freeness systems allow the voters to verify the ballot recording process but it fails to verify the ballot counting process as there can be many situations where the ballots can be altered during storage or transit or purposefully make the votes lost or left out in the final counting process [43]. This has a positive side and a negative side as well. Positive being the voter can check the result directly and have a proof to know if the election authority has been honest or dishonest. This proof has a negative side when a voter can provide this proof to coercers and they can verify the result makes the receipt freeness violated. This made researchers to come up with non-transferable proofs like Designated Verifier Proofs [44]. But this proof fails to achieve the ballot counting process. Universal verifiability can be used to obtain ballot counting.

As the Estonian i-Voting model does not acknowledge end to end verifiability, this chapter focus on the existing End-to-End verifiable voting systems, the cryptographic foundations that can be used in E2E voting systems ensures both the voter privacy and end-to-end verifiability which ensures high transparency in the process so that a voter do not have to trust the system. Here a voter can verify their votes have been "cast as intended, recorded as cast and counted as recorded" [42].

We will be discussing about various protocols that will help to achieve maximum transparency (E2E verifiability).

5.3 Mix-net Voting

Introduced by Chaum, mix-net is a cryptographic protocol which provides anonymity for a group of senders and use a set of mix servers which is based on a public key [39] [40]. The input in a mix-net will be encrypted data and data will be subjected to shuffling and reorganised and later decrypt it. Main advantage of mix-net is to hide the correspondence between an input and output data. This property of mix-net can be used in voting system to ensure privacy (verifiability) and anonymity [47]. A mix-net can be built on a single algorithm shuffle which is given a public key along with a sequence of cipher texts which later produce a proof as well. That proof will be in a Non interactive Zero knowledge Proof which satisfy the conditions that values generated are correct. It also helps an observer to verify that no messages were modified, deleted or added in the system.

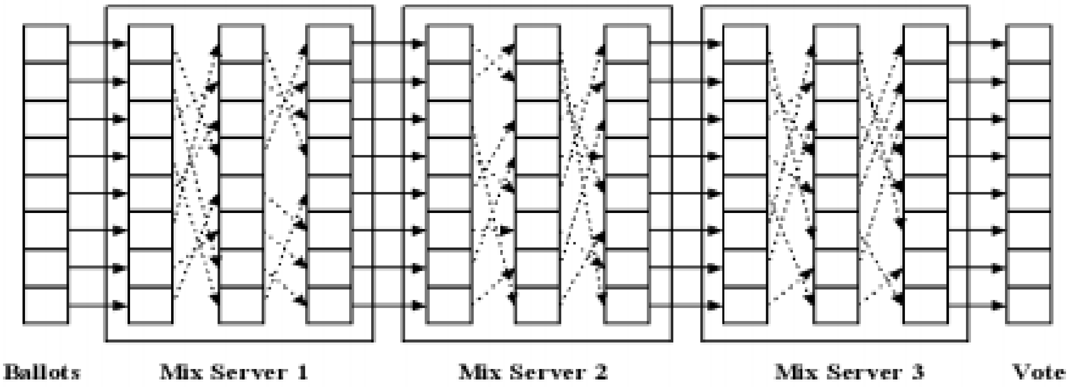


Figure 7. Mix-net – The nodes in this mix-net decrypt the input messages partially and applies a random permutation to the order of messages and send it to the next node [32].

A mix-net consists of a set of nodes that decrypt input messages partially and gives a random permutation to the order of message it receives before sending to the next node of the mix-net. A public key {p} is used by the sender to create messages in each node and the message is encrypted successfully in the reverse order. In figure 7 the mix-net encryption of a message 'm' would be [32]

$$\textbf{\textit{Mix-net encryption, ME (m) = E}}p_1\,(Ep_2\,(Ep_3\,(Ep_4\,(m))))$$

Later mix-net performs decryption with a private key {k} for each node

$$m = Dk_1\ (Dk_2\ (Dk_3\ (Dk_4\ (M\ E\ (m)))))$$

The above equation is known as a Chaumian mix-net and the input should be always untraceable to the output in each node making it the minimum requirement for a Chaumian mix-net. Two types of mix-nets, Decryption and Re-encryption mix-net is discussed below by illustrating an example and how a mix-net is used as a component in a voting system to provide anonymization.

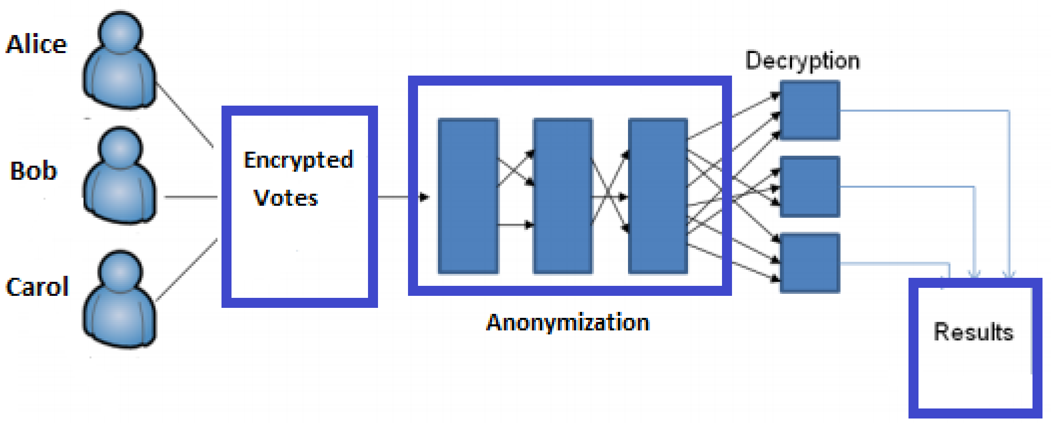


Figure 8. Mix-net Providing Anonymity [48]

5.3.1 Decryption Mix-net

An input message is encrypted with a set of public keys and later each mix node will remove a layer of encryption using a private key and the node will shuffle the message in order and pass it to the next node. This was first proposed by David Chaum in 1981. The concept of Decryption mix-net can be explained as follows [46].

Alice makes a message {M} that is to be delivered to Bob which she uses Bob's public key K_b. Before sending the message Alice also add the address of Bob which can be denoted as B and seal the result with the mix component's public key K_m. Then we can see the input of the mix component as [46]

$$I = K_m\ (R_1,\ K_b\ (\ R_0,\ M),\ B)$$

Here R_1 and R_0 are random strings of a bits. Then the mix component will decrypt the input message with the private keys and discard the random strings by the following output [46];

$$X = K_b(R_0, M), B$$

We can see any mechanism in the system will be able to forward the output X to Bob which can be decrypted using Bob's private key. By providing a signed receipt to Alice when she submit the message to the mix component, she will be able to provide some proof to know whether the mixing component outputs the data X incorrectly or not at all [46]. In case if Alice is wronged she will be supplied with this receipt

$$Y = (K_a^{-1}(C, K_a (R_1, K_b (R_0, M), B)))$$

K_a^{-1} is Alice private Key and C can be denoted as a large constant. The missing out will can be given by Alice in the form of

$$X = (K_b (R_0, M), B)$$

Where the retained string R_1 will be;

$$K_a(Y) = C, K_a (R_1, X)$$

We can see a mix-net always sign each output batch as a whole and if an item X is missing from the batch it can be always supported by a copy of the signed batch as it is a series of mixes that create a mix-net. We can see any single mixes can provide secrecy for the entire mix-net [46]. In Decryption mix-net, when a message is sent from Alice to Bob, it is prepared for a series of N mixes same as a single mix components and will be encrypted for each succeeding mix. The public keys of all the mixes $(K_1, \ldots. K_k)$ will be known to the initial encryption components.

$$K_n (R_n , K_{n-i} (R_{n-1}.., K_2, (R_2, K_1 (R_1, K_b (R_0, M) B))..))$$

Each mixes in the mix network will strip off the encryption one by one by applying a corresponding encryption algorithm and will be given a secret random permutation number to the decrypted inputs. Each mix component can partially decrypt the data items as the each component has its own pair of private and public keys. So the result of the last mixing component should be the same as of the single mixing component [46].

$$X = K_b (R_0, M), B$$

Analogous to one single mix component if there is a series of mixes failing to properly process: a message X can be proven with requiring a receipt from the first mix component in the mixing network since there will be mix N which use the signed output of the N-1 mix to show the absence of an item X from the input. In a voting system, a mix-net can take the encrypted ballots as the input and with the computation process we can make sure the ballots won't be tracked back to the voters. By providing an encryption receipt of the casted ballot, a voter will be able to find if there is any change produced by the mix-net as there will be a bulletin board display for the output of the mix-net.

5.3.2 Re-encryption Mix-net

In re-encryption mix-net, the role of a mix phase is just to mix without any partial decryption. There is a decryption phase added at the end which is used for a final decryption. In this process the inputs will be scrambled without changing the set of cypher texts making it possible for each resulting cypher text to easily recover the voter connected with it. Because of this; an additional operation is needed make the mix not recoverable. In this type of mix-net, each mix phase will be followed by this additional operation [49].

Usually an encryption scheme called El-Gamal is used in these mix-nets due it to its good re-encryption properties.

In El-Gamal encryption scheme; the encryption of a message '*m*' with respect to a public key (p, g, y) which is consisted of a pair (g^r, my^r) and all the operation here are done modulo p and $r \in_R Z_q$ as q here is a large prime which divides p-$1$and g which generates elements in the subgroup whose order divides m and q. 'x' which is denoted as the secret key that is corresponded to (p,g,y) will be $g^x = y(mod\ p)$. Any encrypted message $(a, b) = (g^r, my^r)$ in the El-Gamal encryption scheme can be re-encrypted by taking a random $s \in_R Z_q$ computing $(ag^s , by^s) = (g^{r+s} , my^{r+s})$.

Work flow of an El-Gamal re-encryption mix-net can be explained in the following steps [49]:

1. In some distributed manner an El-Gamal public key (p, g, y) is generated.
2. During the initial encryption phase, system encrypts all the data items or the ballots $B_1, \ldots.B_n$ using the El-Gamal algorithm along with the public keys mentioned in the step 1. After this all the resulting cypher texts ($C_{1,0}, \ldots..C_{n,0}$) will be posted on a bullentin board.

3. During the *i*'th mix phase stage, a set of cypher texts ($C_{1,i-1}$, ….$C_{n,n-1}$) will be put on the input and re-encrypt each cypher text and later using a secretly chosen random permutation, the resulting cypher texts will be subjected to permutation.
4. During the final process, a set of cipher text ($C_{1,k,}$….$C_{n,k}$) will be received by the final decryption component. These cipher texts are decrypted in a distributed matter and the original data is obtained.

A voting system is verifiable when all the voters are able to check whether votes are counted in the final stage and it is said to be robust if a small set of servers are not able to disrupt the election process. The above mentioned protocol is neither verifiable nor robust. To achieve these properties; several additional components are added to this protocol. In order to be a provable mix-net each mix-net has to prove it has done the correct action. As each mix_i have to prove that there exists a permutation π in a way that $C_{j,i}$ is a re-encryption of $C_{\pi(i),i-1}$ for j = 1, …. n [50].

Zero Knowledge Proof (ZKP) – can be defined as a "cryptographic interactive method for a party to prove that the given statement is accurate and any verifier does not learn anything except that the given statement is true" [51].

Provable Mix-net (Sako-Kilian Mix-net) – This mix-net use El-Gamal re-encryption technic. Here all the inputs are El-Gamal cypher-texts and before decryption they are re-organized and shuffled jointly and are connected to proofs of correctness [52]. In this type of mix-net, N inputs are taken by the mix server and are re-encrypted. The re-encrypted factors used in this mix-net is in the form of $\{S_i\}_{i\in[1,\ N]}$. Then cypher-texts are subjected to permutation by the mix server in proportion to a random permutation which is noted by 'πN' which gives d_i = Reenc($C_{\pi(i),}s_i$). Additionally a shadow mix is also produced by the mix server to prove the inputs are mixed correctly. There exists an arrangement called shadow-mix shuffle proof which is shown in Fig 9. In this scheme in order to verify the mixing computations an auditor can ask for the proof of correct decryption.

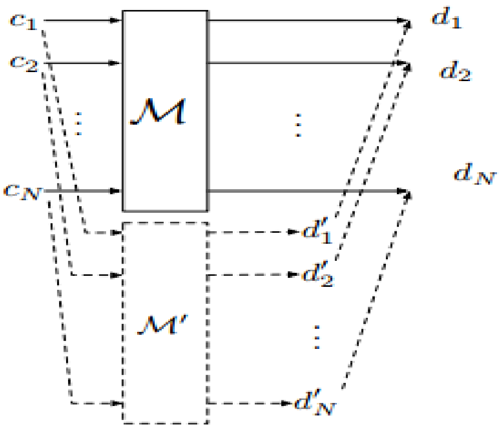


Figure 9. Shadow Mix [53]

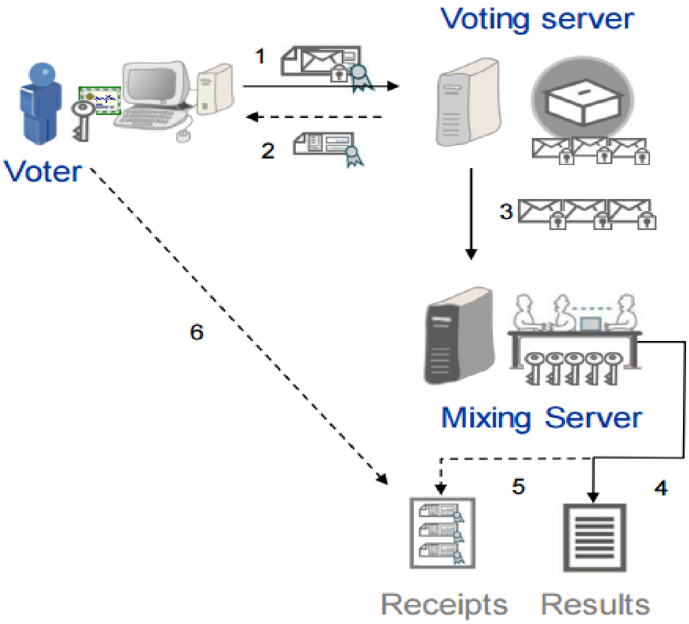


Figure 10. Implementation Model of I-Voting Process with Mix Server Shuffling [41].

5.3.3 Verifiability in Mix-net

Using Zero Knowledge Proof of Plaintext Equivalence a verifier will be able to prove that he knows the secret value without revealing any details about the secret value. Thus he will be able to demonstrate the correct encryption. Also Zero Knowledge of Proof of Correct Decryption can be used in the auditing process. All the proofs are universally verifiable in mix-nets as they anyone can see that both the input and output have not been changed and are based on the same original plaintext [54].

To create an anonymous channel for voting, we could use both the re-encryption and decryption mix-net. But re-encryption mix-nets have certain advantages over the decryption network. In re-encryption mix-nets, there are separate process for re-encryption and decryption. So the correctness of the data will not be affected even if there is any problem with one of the mix server. But in decryption mix-nets, lack of one mix server will cause the mix-net vulnerable to DOS. Also ZKP can be used for auditing purposes in a re-encryption mix-net. Some common ZKPs used in this mix-nets are Schnorr Identification Algorithm and Fiat-Shamir heuristic [55]. Hence mix servers can be verified without acknowledging the ballot information and re-encrypted value. But in a decryption mix-net auditing process can be challenging and there is always a possibility of some data leakage as the auditor has to audit each mix server one by one [54].

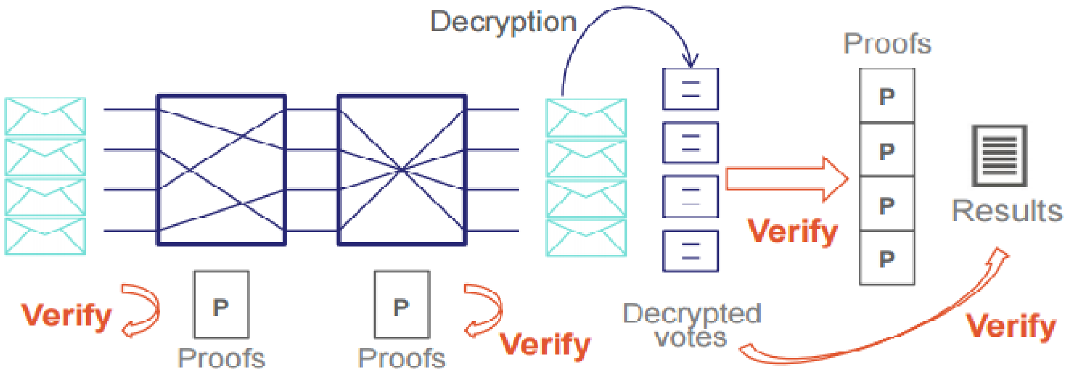


Figure 11. Universally Verifiable Mix-net [41].

One of the biggest disadvantage of re-encryption mix-net is that it fails to use the same re-encrypt value when it comes to ballot encryption making the permutation link between the inputs and outputs easily available to an outsider or an attacker. Even if the mix servers use different re-encrypt values for each ballot, remembering such great random values and their link to each ballot is impractical in a large scale election making the audit process difficult. But in decryption they do not have this problem as the mix-servers do not require anything to remember because permutation links and random value for ballots can be obtained by decrypting the input ballots again [26].

5.4 Homomorphic Encryption

Homomorphic encryption functions – can be used to find the sum of encrypted values without decrypting them making it a desire property to use in i-Voting as the sum can be found in encrypted form too. In homomorphic encryption a function 'P ( )' should satisfy the condition that from the functions P(x) and P(y) we should be able to retain P (x ⊥ y) without decrypting the x or y [56]. ie

$$\boldsymbol{P\ (x) \perp P\ (y) = P\ (x \perp y)}$$

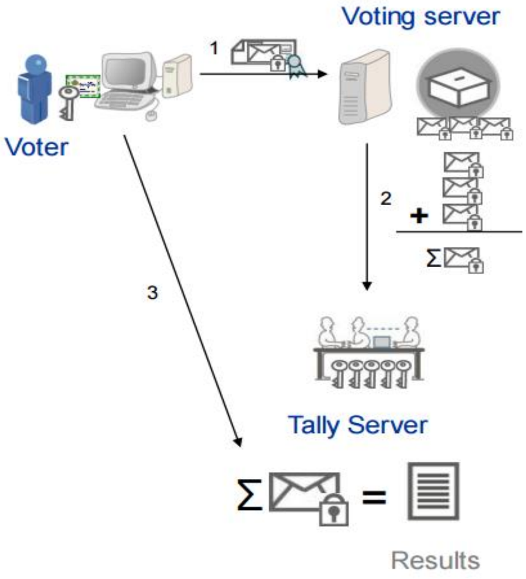


Figure 12. Homographic Properties Used in a Voting Process. Before casting the votes, all votes will be digitally signed. Encrypted result will be obtained in the process [41].

El-gamal and Paillier are the common homomorphic algorithms used and they both work on the principal of additive property. El- Gamal uses multiplicative homomorphism functions.

For example consider m_1 and m_2 are two messages and if the encryption of these messages are multiplied we get the result as the products encryption value. In El-Gamal the randomisation get added together when a message is multiplied together [41].

$$P(m_1) * P(m_2) = P(m_1 * m_2)$$

This property of El-Gamal can be used in voting as the votes can be represented in a numerical format and sum of votes for each candidate can be obtained in encryption form. When a voter selects a candidate it will be represented as 1 and the candidates not selected will be denoted as 0.

$$E(V_1) \oplus E\ (V_2) \equiv E(V_1+V_2)$$

In El-Gamal, we have the following components. p can be noted as a large prime and p=2q+1. m is the message and x is the private key and public keys are noted as (h, g, p) where h = g^x mod p. w will be noted as a random number.

Encrypted message will be noted as c= (a,b) = (m.h^w^ , g^w^)

As mentioned earlier, a binary value ‘v’ will be taken which is equal to ‘1’ if the voter selects the candidate and candidates not selected will be noted as ‘0’. A predefined value of root ‘g’ is added to the value v before the votes are encrypted. In an election of two candidates, the encryption will be denoted as [41]

$$\textit{c which is the encrypted vote} = (g^v.h^w\ , g^w)\ v = \{1,0\}$$

If c’ and c” are two votes which uses the same public key for encrypting. When they are multiplied we get [41],

$$C' = (a',b') = (g^{v'}.h^{w'}, g^{w')}$$

$$C'' = (a'',b'') = (g^{v''}.h^{w''}, g^{w''})$$

$$C = C'.\ C'' = (a', b)\ .\ (a''.\ b'') = (g^{v'}.h^{w'},g^{w})\ .\ (g^{v''}.h^{w''},g^{w''}) = (\ g^{v'+v''}.h^{w'+w''}, g^{w'+w''})$$

By this operation we can get the total number of votes for the candidates by looking in to $\boldsymbol{gv'+v''}$ where v’+v” will be the total number of selected votes.

5.4.1 Verifiability in Homomorphic Encryption

Verifiability in homographic tallying can be achieved by introducing a Zero knowledge Proof which helps to determine the votes were counted as casted. Discrete logarithms are used in this process. From above equation, c = (a,b) = (m.h^w, g^w). Using the private key x, m is recovered in the decryption process. Since there are multiple data structures which is denoted by (g, b, h, v) and the encryption factor is denoted will be h^w=a/m. The secret value w satisfies the condition w=$\log_g$h=$\log_b$v. Hence a prover will be able to prove he know the secret value without revealing the value w. In this process anyone can use the encrypted votes to calculate the result of the election as the process will create proofs of correct decryption [41].

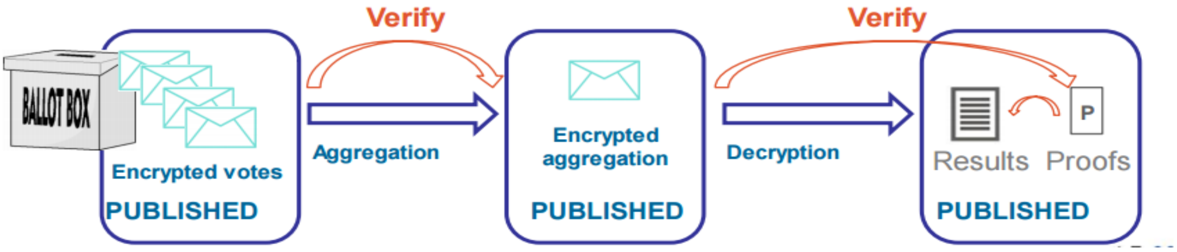


Figure 13. Verification in Homomorphic Tallying [41].

Fig 14 is a hypothetical E2E model which uses both Mix-net and Homomorphic Tallying. Here the vote is encrypted and put on a bulletin board where anyone can check the registration data base and see whether the voter is eligible to vote. Mixnet is used by the election officials for anonymization and later decrypt them jointly. Also a proof will be provided and later posted so that any observer can verify the tallying[57].

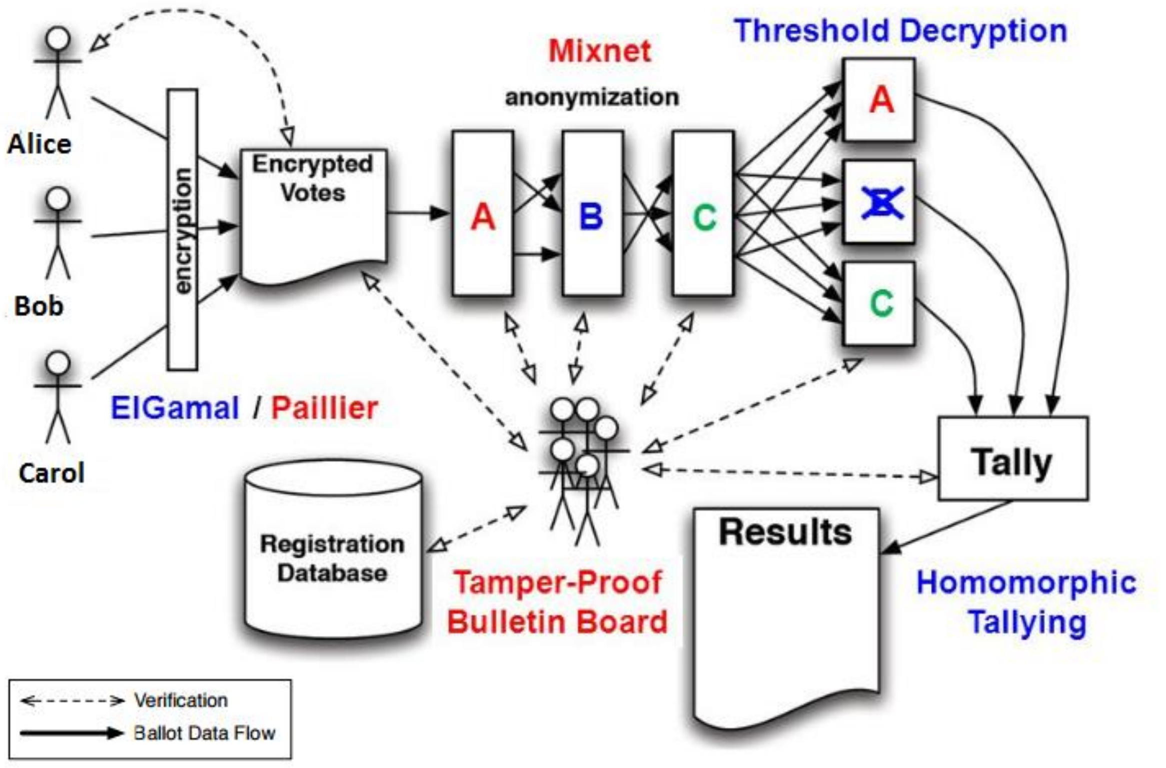


Figure 14. Mixnet and Homomorphic used in a E2E voting model [57].

5.5 E2E Models in Practice

Many E2E voting systems have already been used for elections such as university elections, and pilot elections. However, almost all of the established systems have been developed for paper ballots and hence rely on a paper trail. In retrospect, the double envelop based encryption system used in Estonia had evolved from a previous model that existed for the automation of paper mails. This section will be describing the existing E2E models used.

5.5.1 Helios Voting Model

Helios is a web based E2E i-Voting model that has succeeded in implementing ballot secrecy along with verifiability. It was first used in the elections of a Belgium university to select the president in 2009. Since many universities been using the system to conduct various small scale elections. It is an open audit system which can be accessed over a web browser. This voting system uses existing web programming technics and crypto technics to achieve E2E verifiability. Helios provides the following features [53]

- Ballot casting assurance where a voter can verify the votes are successfully captured by the system.
- Encrypted votes are recorded on a bulletin board which is public verifiable.
- Universal verifiability allowing anyone to verify the recorded votes are correctly counted.

Helios uses ‘The Benaloh Protocol’ to provide ballot assurance. During the voting process proofs of correct plain text is attached to the homomorphic tallying to provide verifiability. Helios consists of mainly 4 components, ie an election builder, a voting booth, a server which acts as ballot casting server and an audit server.

In Helios the voter receives an email which contains ballot finger print after he has cast the vote. The bullet board provided by the Helios will display the ballot finger along with the voter identification number making possible for the voter to see whether his vote is counted correctly [58].

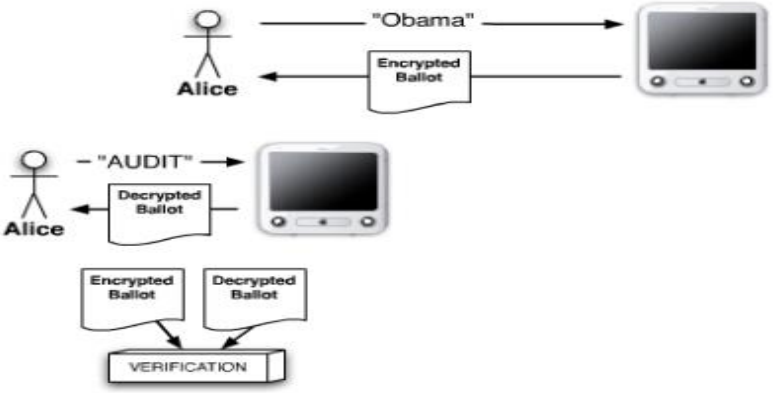


Figure 15. Verifying an Encrypted Ballot [58].

5.5.2 Pret A Voter

This voting model was created by Peter Ryan and uses candidate randomization for casting a vote. This voting model use two parts paper ballots which is usually printed as a single sheet where the candidate name appears on one part of the ballot and an area where voters have to select the candidate they wish to vote for. There will be an ID number or a barcode along with it. This model uses randomized candidate names and the voter makes the selection of the ballot and tear the sheet in to two and voter can keep one part for verification. A crypto mapping is used to find the relation between the random candidate list and the ballot ID number and is casted ballots is decoded in to readable ballots at the later stage of election and all the decoded votes are posted on an online public bulletin board. Individual verification is done by checking whether the ballot ID number is included in the public bulletin board [59].

5.5.3 Scantegrity II

This was first used in Takoma Park elections in 2009 and it was the first E2E verifiable system used for a government elections with ballot privacy. A program called "pseudorandom number generators" generates a random seed numbers before the elections and these are distributed among the election officials using secret sharing scheme. In secret sharing scheme, the random seed is split it to multiple parts and distributed. The secret information is revealed only after combining the parts (sometimes the whole parts needed to be combined to reveal the information or only few parts depending on the secret scheme used). An Alphanumeric code is also generated and printed on each ballot which will be used for the election candidate selection. Scantegrity II uses the same idea as of an optical scan paper ballots which uses an invisible ink to select the candidate. Individual verifiability is provided by this model as a voter can record the code which they get from the invisible ink and also the ballot ID number. A public bulletin board displays the ballot ID and the displayed code. Individual voters as well as public can verify the final tally after the elections [60].

5.5.4 Remotegrity

Remotegrity is a code voting system which is usually used in an unsupervised environment for remote elections. In Remotegrity a crypto generated code is used by the voter to select the candidate. Code voting system has been made secure with a set of different codes which both come with serial numbers. Codes will be received by the voter: one set of codes is used for voting and the other for authentication. Thus it is not possible for an outsider to assume how the voter has voted.

The ballot for voting contains a scratch-off field which covers the codes. Authentication card will be sent via mail and it is comprised of three kinds of codes: authentication-, a lock-in- and an acknowledgement code. In this system, a voter needs to go to the election website and enter both serial numbers, then the codes of her choices and lastly scratched off authentication code. After some hours she can check from the same website whether her acknowledgement code is next to her voting code. If it is correct, a voter has to scratch off her lock-in code and post it on the website to confirm that the vote was correctly posted. Codes will be calculated in a provable way for the tally in Remotegrity.

Authentic codes, voting codes are generated by two separate computers and another computer which collects the votes. Therefore, computers do not share any information and it makes the Remotegrity system even more secure [61].

Chapter 6. Analysis of E2E models: Drawbacks & Security Challenges

As its formulators acknowledge, end to end verifiability becomes crucial and inevitable to i-Voting; even though i-Voting is not the electoral form they would recommend. Various end-to-end verifiability systems promise better possibilities with regard to verifiability, security, ease, etc., and also instil an assured sense of technological progress. But, it is not without its demerits and limitations. Most of the E2E models have been subject to limitations and security lapses, however negligible it may seem. The E2E systems do mitigate some of the major limitations of the traditional in-person voting systems and remote voting systems, amongst which are issues regarding reliability of equipment, internal tensions regarding the procedure and mutual trust, accessibility, integrity of postal systems, etc. But as specified, they are not free of all these limitations. Also, there are unique limitations that are specific to each of these systems. These are as discussed below [42].

6.1 Drawbacks of the Existing E2E Voting systems

Maintaining vote secrecy has been a constant challenge for each of the E2E voting systems. In case of systems like Prêt à Voter, where they rely on techniques like maintaining a random candidate order with randomly printed codes on the ballots, the confidentiality could be breached if an insider accesses and leaks the candidate positions. In order to avoid this, it was recommended by researchers that printing ballots be made available at polling booths/places. However, the high probability of technical difficulties and additional expenditure renders the recommendation infeasible. In systems like Scantegrity II and Remotegrity, which limit the knowledge of insiders with regard to votes, through means of invisible ink or scratch-off fields respectively, secrecy can still be breached in case of lapses on the side of voters and poll workers in carrying out the procedures [42].

Receipt freedom- which is an integral part of vote secrecy - needs to be checked and discouraged as these enable both coercion and vote selling. This claim becomes valid when posited in terms of breaching vote secrecy, while its usefulness in case of dispute resolution is a factor worth considering. RIES is a system that has made a deliberate secrecy trade off by implementing a provision for universal verifiability, along with individual verifiability to an extent, hence doing away with receipt freedom. However, individual acts of disclosing one's credentials or encrypted vote may lead to gross violation of ballot secrecy through the very means of public information [42].

Ballot stuffing is one of the threats towards attaining a fair election result. While this could be easily dealt in case of traditional voting methods, due to the visibility of actions, its susceptibility in case of i-Voting is much higher. This is not an inherently verifiable property of the system. It is wholly dependent on the accuracy of the poll workers' accounts and trust. The Helios system has developed a model which relies on individual verifiability of votes by means of their email addresses. This limits the protection against insider ballot stuffing and hence is open to the threats from within [35].

In case of verifiability, the basic feature of E2E systems, not all systems are adequately equipped with dispute resolution mechanisms that are convincing enough. The existing cryptographic protocols which provide evidence of the voter's choice are either in the form of paper or another electronic device such as a smartphone, apart from the machine used to cast vote. These are not adequate to prove the inaccuracy or election fraud. Moreover, it is open to the danger of exploitation by dishonest voters [42].

As mentioned above, each new modification to ensure security and transparency demand sophisticated equipment and infrastructure. These, as we know, are prone to consistent failures and defects. Some of the issues that may frequent are [42]:

E2E systems must be maintained and checked at regular intervals for resilience to failures (since recovery becomes crucial in case of system failures) without compromising with its properties.

Since several E2E systems use "write-only" online public bulletin boards to post encrypted ballot information, it becomes difficult to organize them and impossible to change/remove. In order to update these bulletin boards, networking becomes essential-either via traditional means or via devices for information transfer. Each of these networking schemes is vulnerable to security threats and denial of service attacks- which would be discussed in the following section [42].

Usability is a crucial element to elections. It becomes one of the basic features that lead people to choose i-Voting. As we know an election system must make voting easy and assist voters sufficiently so that it doesn't lead to disenfranchisement. While verifiability becomes the goal, the added complexity to the E2E systems makes it difficult and time consuming.

Since researchers are still trying to overcome these barriers, the voters are presented with a task of mastering the system which would benefit them in its entirety. “In this regard, in 2014, a team of researchers from Rice University had sought to measure the usability of three E2E systems, namely, Helios, Prêt à Voter and Scantengrity II, by examining their effectiveness, efficiency and satisfaction” [62][42]. Their results pointed towards the failure of the systems in terms of usability, even for voters disinterested in verification. Hence, the voters sometimes did not even realize that they were unsuccessful in completing the process, or failed with regard to operating it. On the contrary, traditional voting systems fared a 100% in terms of success and was much efficient, comparatively. This study suggested that including validation mechanism would improve verifiability but at the same time shall render the system unusable for the voters.

While one of the goals of E2E verifiability systems have been to make it user-friendly and accessible, even to visually impaired voters, this has not been materialized. In addition to even marking a ballot, some of the systems lack features that would enable disabled voters to cast votes without help. “For accessibility to disabled voters, protocols like using accessible devices with an audio, sip-puff, or switch interface to read and mark the unencrypted ballot have been suggested which would enhance the trust of the voters in the system”[42]. While this remains a pre-requisite for even non-E2E systems, a well-designed E2E system a much smaller base to ensure trust. However, considering the usability issues mentioned above, the possibilities of an efficient system seems to be in need of much more research and tests [42].

Along with all the above listed internal deficits, which are still areas where research and development are in progress, what needs to be considered is the social and political constrains involved in implementing the systems in large-scale elections. While track records of success and limitation of resources as the major challenges, it is important to note that any aspect of the E2E systems cannot be compromised. Such an implementation could deter public confidence and hence call for a redundancy regarding the progress and implementation of E2E systems, the underperformance of any existing End-to-End system can cause the public to discard its possibilities [42].

6.2 Security Challenges with E2E Voting Systems

6.2.1 Authentication

Voter Authentication is central to user verification in any i-Voting system. In Estonia, it is reliant on the ID cards. Strong positive identification of the voter is a requisite of voting system, as it is a security issue. However, it is a separate security issue and not a part of E2E system. Following are some of the crucial aspects concerning security in any i-Voting systems [63]:

- "It must verify that potential voters are duly registered or eligible to vote in the jurisdiction they attempt to vote in; and prevent anyone from voting more than once"[63]. It must also prevent attempts of the sale of votes, coercion in voting, and proxy voting.
- Passwords, challenge–response systems, email confirmations etc. are commonly used authentication methods. Such methods are sufficient for ecommerce situations where secrecy is not that important or fraudulence can eventually be detected.
- Possessing technical wherewithal to impersonate one voter implies the possibility of replicating multiple voters. Many data leakage incidents (mostly personal data) in the recent past points to the high possibility of such a threat. Hence authentication systems based on personal information is an already compromised option.
- The traditional voter authentication method is based on wet ink signature matching. Along with this some states have adopted the additional measure of Voter ID. But, so far no fool proof technology has been developed to implement wet ink process using computer or mobile.
- Unforgettable transmission of Voter ID documents poses serious security threats. Implementation of voter identification system based on biometrics such as finger prints or retinal scan is a suggestion made by many people. But technological challenges to this are many. Mobile phones and tablets use finger prints to identify users and authenticate usage on their respective devices however the verification for access to remote services over the internet cannot be similarly ensured. Hence, there is a need to consider stronger methods like taking the help of cryptographic ID cards.

- "Cryptographic ID cards would in principle enable voter authentication from any Internet-connected computer or device that could read them. But its initial implementation is an expensive affair" [63]. However, this is context dependent on the economies of scale and IT infrastructures in different countries, it is particularly irrelevant in the case of Estonia as there is already a pre-existing ID card platform on which most of the public services are based.

6.2.2 Client Side Malware

Malware threat poses a major challenge to online voting systems. It is difficult to prevent malware attack using commercial anti-virus softwares. There are numerous vulnerabilities in modern computer that a comprehensive defence is impossible. Fundamental weakness attributed to existing E2E systems involves its inability to prevent or detect the malware incursions before the votes are reconciled.

Malwares on Client side Platforms – When it comes to malwares, we can see most of the traditional antiviruses are not very much effective against the latest malwares. In an online voting system usually voters use a personal computer or a smart phone with an internet connection, the possibility of malware infection is very much leading in to either modification of the votes or removal of the votes [35].

Therefore, some of the ways in which malware can distort the election are as follows [42]:

- Before the submission to the E2E verifiability system, Malware can modify the voter's choices.
- Malware could send a copy of the vote to a third party.
- Malware could also prevent the voter from successfully casting his/her vote.

6.2.3 Network Attacks and DDoS Attacks

Similar to the threats posed by clients' side E2E software, it is also possible that the attack takes place from the server side. The existing E2E system is subject to several attack possibilities, predominantly though network attacks by modifying or configuring the software through the Internet. Through control over a router, DNS server, or any other element of internet infrastructure it is possible to prevent votes from reaching their destinations. “The possibility of detection of such malicious attacks is an advantage that E2E systems have over other Internet voting systems” [42]. It is possible to disrupt the E2E protocol and prevent votes from being delivered. While this can be detected, loss of votes cannot be prevented or estimation of number of votes affected is impossible [35]. It is important to note that Distributed Denial of Service (DDoS), which is a dangerous form of network attack can seriously hamper the election procedures. Here, the attacker floods the server causing the system to crash or slowdown. Voters might experience total response less-ness from the system or extremely long waits between each steps. This could result in the disenfranchisement of large number of votes. Defending against DDoS is important for two reasons [35]:

- DDoS is easiest of all network attacks to perpetrate.
- DDoS can prevent anyone in the target location from voting causing the disenfranchisement of thousands of voters.

It is possible to tone down the severity of DDoS attacks but an ultimate solution is out of hands so far.

Chapter 7. Building Trust in Internet Voting

In order for i-Voting tone effective there is the need to build trust in this system. All the parties participating in the electoral process need to be able to understand and be assured of the process involved in order for them to trust in this system. Another major obstacle is the digital divide, the problem being with the population who are not comfortable with using modern technology, particularly the senior citizens and the low income cluster of the population who have will or very limited experience with the digital world. The digital divide, hence, can be classified generally on the basis of income and age. Recent studies conducted in this area shows that people between the age group of 18 to 35 normally using government sites for tax filing and license renewals are comfortable with Internet voting concept [2].

But the older and economically backward classes of society may not be easily willing to accept this system. People mostly experience issue in terms of skills necessary to operate a computer system, which includes the use of hardware and software effectively to attain the desired result. Also with limited access to computers at home in the low income classes its use is very rare.

If governments across the word are planning to replace traditional voting with I voting, they would need to consider the above issues and will need to figure out appropriate solution. We will need to ensure that the access and skills divide barriers are addressed before completely replacing the traditional voting system with Internet voting. For these issues to be addressed governments can work with non-profit organisations designed to help senior citizens. In order to address access divide, voting kiosks can be installed in public libraries, atms, etc. There is also the need for general public to understand the security features of an i-Voting system to have trust in it [2].

To attain this goal, the voters must be able to very and confirm that their votes are correctly recorded. Ideally the source code can be made available to general public, but not many will be able to comprehend this. Another method is end to end verification.

This is an important aspect of instilling trust in voters. In this way voters will be able to verify that their votes have been correctly recorded by the system. Malicious attacks can also affect Internet voting adversely, but these risks can be mitigated to an extent by use of election forensics. In the cases of multiple failures of the system or systems unavailability will definitely need to troubleshoot instantly as this maybe a possible malware attack. Election forensics need to be effectively used in such cases to identify the root cause and fix this or even reschedule elections if required. Only when all the above factors are accounted for and studied thoroughly for appropriate solutions can a full-fledged i-Voting system can be introduced for major elections [2].

7.1 i-Voting Acceptance

Internet voting acceptance has proved to be diverse in different countries owing largely to the peculiar socio-political conditions and the governmental efforts towards ensuring high acceptance of internet voting. Using internet voting for national elections, until now, is not a widespread practice. Only Estonia, Switzerland and Norway had made legally binding i-Voting a reality in national elections. Researches and studies about the current acceptance of internet voting and its future prospectus has overwhelmingly emphasized that acceptance of internet voting largely relies on the trust of the general public in the system [64].

7.2 Estonian Case

Priit Vinkel in his work “Internet voting in Estonia” compiled in the edited work Information Security Technology for Applications draws three “pillars of success” of Estonian i-Voting, which are as put by Vinkel himself: “Open Receptive Society”, “Secure remote e-authentication” and “Effective measures to guarantee compliance with Electronic Principles”. These features, as Vinkel points out had helped build trust in the system thus leading to high internet voting acceptability in Estonia. Closer studies of internet voting experiments in countries across the globe have proved that from the point of view of acceptance, i -voting has moved from hopeful introduction, to complete rejection due to various concerns, or to more serious considerations of the concerns and studies for solutions developing a more balanced approach [65].

We can see, during the first span of i-Voting, the typical i-Voters in Estonia were ethnic Estonians in a particular age group who had good computer know how. Studies by Mihkel Solvak and Kristjan Vassil shows, there is a clear change in i-Voting participators over the course of time. From the 4th election, the bridge between the populations who use i-Voting and physical voting have changed. More people tend to cast vote online in Estonia, showing i-Voting didn’t remain as an activity just for the privileged but have diffused among the overall population of Estonia. From this we can conclude, Digital Divide do cause problems among the population. But Estonia stands as a prime example to show how a country successfully used the technology as an enabler for Political participation. With well policies with resulted in short course of time, the Digital Divide Bridge can be reduced [66].

i-Voting acceptance cannot be merely gained by introducing i-Voting in place of traditional voting. Citizens of most democratic nations consider elections and their role as voters with much dignity where ease of voting alone cannot play much significant role to encourage them to switch from traditional voting to i-Voting. Concerted efforts from the part of the authorities concerned to build transparent and secure systems along with programmes aimed at winning the trust of the general public alone can help to ensure a high i-Voting acceptance. We can deduce from our discussion from the example of Estonia how the technological and sociological concerns can be successfully fought in the path towards digitising elections. The socio-political context and technological potential of different nations is also a major reason behind the different rate of i-Voting acceptance in different countries. However, hopefully, despite all the hindrances there is raise in the numbers of votes casted through i-Voting and a general understanding about an inevitable progression towards digitising elections [64].

Chapter 8. Conclusion

Ever since the emergence of i-Voting as a central concern, especially in the context of Europe, Estonia and Switzerland have offered diverse but compelling examples as models. The general thriving towards this end is the result of an urge to modernize the electoral system and ensure accessible and secure voting. While ease, transparency, security and belonging-ness becomes the central motifs to sustaining democratic credibility, what backfires are the numerous possibilities of security lapses. Estonia, as mentioned above, has been one of the pioneers of internet voting system. The research, which is an assessment of the various facets of internet voting, focuses on its developments and application in Estonia. i-Voting, in general and with specific respect to Estonian experiences, and the various concerns it raises has been one of the major points of departure. Although the paper concentrates on the Estonian case, it has also attempted a brief analysis of the i-Voting experiences and debates in Switzerland. Switzerland has developed a complex i-Voting system that would go in par with the existing electoral systems and socio-political scenario of the nation. However, the major debates that loomed large in the process helps to develop a broader understanding of the challenges towards a global implementation of i-Voting. Apart from few issues directly related to the specific conditions of Switzerland, the discussion of debates like digital divide and security threat provides further ground to develop the research on Estonian i-Voting; the focus being security lapses.

The 2015 parliamentary elections in Estonia saw the rate of i-Voting to 30.5%, enabling the Estonian voters to cast their ballots from around the globe. Usually elections become events that hamper the smooth running of public activity and work, while in Estonia, due to the implementation of i-Voting system, a considerable amount of working days remain unaffected, thus retaining the wages. Estonia, with its large population of internet users, takes pride in the i-Voting system and thus its secure maintenance becomes a significant concern.

The technological aspects of Estonian i-Voting, the prime topic of research, as discussed in the third chapter (Estonian voting model, its processes and infrastructure) and the fourth one (dealing with its security aspects) points towards certain vulnerabilities in the system, associated with transparency and other major attacks. The research finds a need for more effective measures to ensure the transparency level of i-Voting system which is an important prerequisite for building trust among the voters. What could be the possible alternatives or alterations that could ensure higher security credentials to the existing i-Voting system in

Estonia? This being the major question, Author has tried to demonstrate an existing proposal to the system regarding its security concerns, which is the end-to-end system of verifiability. The paper puts forward this proposal to ensure a verifiable internet voting system, presenting a model based on the aforementioned end-to-end verifiability, which is not yet acknowledged in Estonia.

The end-to-end verifiability system qualifies as a possible remedy to several lapses in the existing Estonian i-Voting system. However, the concern of this paper is if the end to end voting system qualifies to solve the problems of current Estonian i-Voting model, the author emphasize is the inevitability of the same for the internet voting models. Since individual systems are more susceptible to malware, and ID cards could easily be accessed and voting preference re-written, the resulting course of actions could be dangerous. Hence, the users must be able to verify their votes after they are cast; along with the assurance of anonymity. Moreover, the system also aspires to serve voters with physical disability- of vision impairment, hearing, comprehension or motion- but can use computing devices, although within limits. This could help procure the preferences of a significant population with disabilities and thus enhance and ensure their participation in the democratic process.

Although this new proposal does not assure a system that is completely free from attacks, it promises to resolve all the key transparency problems so that voter does not have to trust on the system or the election official. For this, a high quality end-to-end verifiability is to be designed, installed, verified and operated before its implementation in the elections; assuring a minimum level of ease and accessibility. A poorly implemented system would result in privacy violations, programming errors and security risks. Since the end-to-end verifiability also comes with its difficulties, the research provides a study on various crypto-techniques that ensures both voter privacy and end-to-end verifiability providing a system where a voter can verify whether their votes have been “cast as intended, recorded as cast and counted as recorded” [42].

8.1 Recommendations

Some of the recommendations by the researchers on the basis of their experience in these specific fields of research and software development are [42]:

- Implementing a shift in Domain Modelling is one of the major recommendations that will help to design a functional E2E voting system. Also Business Object Notation (BON) and

Extended Business Object Notation (EBON), over the Unified Modelling Language (UML), as the suitable language and design/refinement method for informal domain analysis and modelling, formal modelling, and implementation-independent high- and medium-level specification.

- Moreover, BON can also be used as an architecture specification and concept specification language replacing UML. Each of the languages must be used in lieu with its protocol specifications.
- Static Analysis tools and Dynamic Analysis tools comprise the next set of recommendations, where static analysis tools “process the system’s source code and specifications to provide information about the system without executing the code”, while dynamic analysis tools monitor a running system measuring the aspects of its operation and detects undesirable behaviour. The researchers also points out that dynamic analysis tools can also be used to detect issues related to memory (leaks, corruption), concurrency (deadlock, spinning, data races), resource allocation (unclosed sockets and files), and security (buffer overflows and other vulnerabilities). Some of these issues are mitigated through the various language methods [42].
- Another important suggestion would be model checking that would comply with all the specifications. While recommending against centralized version control systems such as Subversion and CVS, for these affect working-especially for offline workers, tracking tools must be used extensively.
- Continuous integration and configuration management, and testing are also suggested as crucial to software development in E2E verifiability.
- The hardware and software components of a computing system, its roots of trust, are always relied upon. As suggested by the researchers, the only available way to ensure the integrity of a system’s roots of trust is by using a piece of dedicated hardware called a Trusted Platform Module (TPM). Although embedded in several systems these days, the availability of TPM functionality is not enough. Therefore, it is essential that the roots of trust of the system be explicitly enumerated and that the chain of trust for each originates in secure hardware while building an E2E system [42].
- Most importantly, the awareness to be spread among social and political domains is crucial to the implementation of E2E systems. The complete implementation shall never be compromised with or the system altered, as this could pose threat of fraudulent activities in the election process.

References

[1] "Statistics - Internet Voting - Voting methods in Estonia - Estonian National Electoral Committee." [Online]. Available: http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics. [Accessed: 30-Jan-2016].

[2] N. Lars Hopland Nestås, Bouvet ASA, Norway Kjell J. Hole, University of Bergen, "Building and Maintaining Trust in Internet Voting."

[3] "Electronic ID Card - e-Estonia." [Online]. Available: https://e-estonia.com/component/electronic-id-card/. [Accessed: 11-Apr-2016].

[4] C.-K. W. C.-K. Wu and R. Sankaranarayana, "Internet voting: concerns and solutions," *First Int. Symp. Cyber Worlds, 2002. Proceedings.*, pp. 1–6, 2002.

[5] R. E. Voting, A. Efficiencies, and C. Savings, "OSCE Chairmanship Seminar on Present State and Prospects of Application of Electronic Voting in the OSCE Participating States The Most Severely Disenfranchised Voters – Persons with Disabilities and External Voters – Can Be Provided Secure , Private and I," no. September, pp. 16–17, 2010.

[6] D. Bochsler, "Can Internet voting increase political participation ? Remote electronic voting and turnout in the Estonian 2007 parliamentary elections," no. June, pp. 3–4, 2010.

[7] "Elections and Technology —." [Online]. Available: http://aceproject.org/ace-en/topics/et/onePage. [Accessed: 11-Apr-2016].

[8] R. Gibson, "Elections Online: Assessing Internet Voting in Light of the Arizona Democratic Primary," *Polit. Sci. Q.*, vol. 116, no. 4, pp. 561–583, 2001.

[9] A. G. Fowler, "Five Studies on the Causes and Consequences of Voter Turnout." 08-Oct-2013.

[10] "Switzerland's Political Systems: Direct Democracy on federal, cantonal and communal level." [Online]. Available: http://direct-democracy.geschichte-schweiz.ch/switzerlands-political-systems.html. [Accessed: 13-May-2016].

[11] "OFCOM - Strategy for an information society in Switzerland."

[12] J. Gerlach and U. Gasser, "Three Case Studies from Switzerland: E-Voting," *Berkman Cent. Res. Publ.*, p. 17, 2009.

[13] O. Governement, *Conference for E-Democracy and Open Governement 21-23*, no. May. 2014.

[14] A. Driza Maurer, O. Spycher, G. Taglioni, and A. Weber, "E-voting for Swiss Abroad: A Joint Project between the Confederation and the Cantons," *Proc. 5th Int. Conf. Electron. Voting (EVOTE 2012)*, vol. 205, pp. 174–189, 2012.

[15] F. Mendez and U. Serdült, *Design, Development, and Use of Secure Electronic Voting Systems*. IGI Global, 2014.

[16] "A Security Analysis of the Swiss Electronic Voting System | Information Systems." [Online]. Available: https://diuf.unifr.ch/main/is/student-projects/thesis/security-analysis-swiss-electronic-voting-system. [Accessed: 13-May-2016].

[17] *Innovating Government: Normative, Policy and Technological Dimensions of Modern Government*. Springer Science & Business Media, 2011.

[18] 21. Lorenz Engi & Francine Hungerbühler, , Medialex 1/06, pp. 17-27, *E-Voting -- Stand und Entwicklung in der Schweiz.* .

[19] R. M. Alvarez, T. E. Hall, and A. H. Trechsel, "Internet Voting in Comparative Perspective:

The Case of Estonia," *PS Polit. Sci. Polit.*, vol. 42, no. 03, p. 497, 2009.

[20] "Estonian Public Broadcasting. Center Party petitions European human rights court over e-voting."

[21] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, and J. A. Halderman, "Security Analysis of the Estonian Internet Voting System," *Proc. 21st ACM Conf. Comput. Commun. Secur.*, no. May, p. 12, 2014.

[22] "Report on the Estonian Internet Voting System | Verified Voting." [Online]. Available: https://www.verifiedvoting.org/report-on-the-estonian-internet-voting-system-2/. [Accessed: 13-May-2016].

[23] A. H. (European U. I. Treschsel, R. M. (CALTECH) Alvarez, and T. E. (University of U. Hall, "Internet Voting in Estonia," 2008.

[24] AS Sertifitseerimiskeskus, "The Estonian ID Card and Digital Signature Concept," pp. 1–16, 2003.

[25] "Internet Voting - Voting methods in Estonia - Estonian National Electoral Committee." [Online]. Available: http://www.vvk.ee/voting-methods-in-estonia/. [Accessed: 13-May-2016].

[26] T. Martins, "Internet Voting in Estonia," *Tech. Rep.*, vol. 7161, pp. 4–12, 2010.

[27] "The story of the ID-card > ID-card project archive > ID-card and Digi-ID > ID-CARD > ID.ee." [Online]. Available: http://www.id.ee/index.php?id=30673. [Accessed: 13-May-2016].

[28] R. Cimander, A. Aarma, and J. Ain, "eID in Estonia," 2006.

[29] S. Heiberg and J. Willemson, "Verifiable internet voting in Estonia," in *2014 6th International Conference on Electronic Voting: Verifying the Vote, EVOTE 2014 - IEEE Proceedings*, 2015.

[30] P. Elections, "PARLIAMENTARY ELECTIONS 6 March 2011," no. May, 2011.

[31] R. Langner, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve," *Arlington, VA Langner Gr.*, no. November, 2013.

[32] Richard T. Carback III, "Engineering Practical End-to-End Verifiable Voting Systems," 2010.

[33] "Application Threat Modeling - OWASP." [Online]. Available: https://www.owasp.org/index.php/Application_Threat_Modeling. [Accessed: 15-May-2016].

[34] S. Wolchok, E. Wustrow, D. Isabel, and J. A. Halderman, "Attacking the Washington , D . C . Internet Voting System," pp. 1–18, 2012.

[35] K. Dhillon, "Challenges for Large - Scale Internet Voting Implementations," pp. 1–13, 2015.

[36] "End-to-end connectivity | World Public Library - eBooks | Read eBooks online." [Online]. Available: http://www.worldlibrary.org/articles/End-to-end_connectivity. [Accessed: 18-Apr-2016].

[37] J. H. Saltzer, D. P. Reed, and D. D. Clark, "End-To-End Arguments in System Design," pp. 509–512, 1991.

[38] F. Khaki, "Implementing End-to-End Verifiable Online Voting for Secure, Transparent and Tamper-Proof Elections," 2014. [Online]. Available: https://www.scytl.com/wp-content/uploads/2014/11/IDC-report_Implementing-End-to-End-Verifiable-Online-Voting_Enabling-Secure-Transparent-and-Tamper-Proof-Elections.pdf. [Accessed: 11-Apr-2016].

[39] S. Popoveniuc, J. Kelsey, A. Regenscheid, and P. Vora, "Performance requirements for end-to-

end verifiable elections," pp. 1–16, Aug. 2010.

[40] R. L. Rivest, "Perspectives on ' End to End ' Voting Systems Change happens ! Change happens !," 2009.

[41] J. Puiggali, "Scytl Secure Electronic Voting: Mathematics in the Elections : beyond the simple counting of votes," no. November, 2011.

[42] S. M. SUSAN DZIEDUSZYCKA-SUINAT, JOSEPH R. KINIRY, DANIEL M. ZIMMERMAN, DANIEL WAGNER, PHILIP ROBINSON, ADAM FOLTZER, "THE FUTURE OF VOTING:END-TO-END VERIFIABLE INTERNET VOTING."

[43] M. Nüttgens, O. Thomas, and B. W. Eds, *GI-Edition in Informatics*, vol. c. 2011.

[44] "Designated-Verifier Proofs – Bookmetrix Analysis." [Online]. Available: http://www.bookmetrix.com/detail/chapter/bdbbc84e-73ff-47e5-8662-dd50e9319193#downloads. [Accessed: 13-May-2016].

[45] D. Barstow, W. Brauer, P. Brinch Hansen, D. Gries, D. Luckham, C. Moler, A. Pnueli, G. Seegmüller, J. Stoer, N. Wirth, and C. G. Günther, Eds., *Advances in Cryptology — EUROCRYPT '88*, vol. 330. Berlin, Heidelberg: Springer Berlin Heidelberg, 1988.

[46] D. L. Chaum, "Untraceable Electronic Mail , Return Addresses , and Digital Pseudonyms," vol. 24, no. 2, pp. 84–88, 1981.

[47] C. A. Neff, "Verifiable mixing (shuffling) of ElGamal pairs," *VHTi Tech. Doc. http//www. votehere. net/ …*, 2003.

[48] B. Adida, "Mixnets in Electronic Voting," no. January, 2005.

[49] L. R. Rivest, "Lecture 18 : Mix-net Voting Systems Re-encryption Mix-nets," pp. 1–5, 2004.

[50] R. Rivest, "Rivest 2004 Lecture 19 : Verifiable Mix-Net Voting," pp. 1–5, 2004.

[51] I. S. Hohenberger, "Lecture 3 : Zero-Knowledge Proofs Zero-Knowledgeness," *Methodology*, pp. 1–5.

[52] D. Wikstr, "Mixnets for Voting," 2010.

[53] B. Adida, "Helios: Web-based Open-Audit Voting.," *USENIX Secur. Symp.*, pp. 335–348, 2008.

[54] P. Locher, R. Haenni, and R. E. Koenig, "Coercion-Resistant Internet Voting with Everlasting Privacy."

[55] D. Bernhard, O. Pereira, and B. Warinschi, "How not to prove yourself: Pitfalls of the Fiat-Shamir heuristic and applications to Helios," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7658 LNCS, pp. 626–643, 2012.

[56] R. Rivest, "Lecture Notes 15 : Voting , Homomorphic Encryption," *None*, 2002.

[57] B. Adida, "Advances in Cryptographic Voting Systems," *Electr. Eng.*, pp. 1–254, 2006.

[58] B. Adida and C. A. Neff, "Ballot Casting Assurance," *Proc. USENIX/Accurate Electron. Voting Technol. Work. 2006 Electron. Voting Technol. Work.*, 2006.

[59] P. Y. A. Ryan, D. Bismark, J. Heather, S. Schneider, and Z. Xia, "Pret A voter: A voter-verifiable voting system," *IEEE Trans. Inf. Forensics Secur.*, vol. 4, no. 4, pp. 662–673, 2009.

[60] D. Chaum, R. T. Carback, J. Clark, A. Essex, S. Popoveniuc, R. L. Rivest, P. Y. A. Ryan, E. Shen, A. T. Sherman, and P. L. Vora, "Scantegrity ii: End-to-end verifiability by voters of optical scan elections through confirmation codes," *IEEE Trans. Inf. Forensics Secur.*, vol. 4,

no. 4, pp. 611–627, 2009.

[61] R. Carback, D. Chaum, J. Clark, and F. Zagorski, "Demo : Remotegrity Are usable and secure remote voting schemes possible ?," pp. 3–4.

[62] C. Z. Acemyan, P. Kortum, M. D. Byrne, and D. S. Wallach, "Usability of Voter Verifiable, End-to-end Voting Systems: Baseline Data for Helios, Prêt à Voter, and Scantegrity II," *USENIX J. Elect. Technol. Syst.*, vol. 2, no. 3, pp. 26–56, 2014.

[63] J. B. A. CONCURRING, D. J. RONALD L. RIVEST, PHILIP STARK, VANESSA TEAGUE, and V. T. CANDICE HOKE, RONALD L. RIVEST, BARBARA SIMONS, PHILIP STARK, "End-To-End Verifiable Internet Voting: Expert Statements," no. July, 2015.

[64] F. B??langer and L. Carter, "The digital divide and internet voting acceptance," *4th Int. Conf. Digit. Soc. ICDS 2010, Incl. CYBERLAWS 2010 1st Int. Conf. Tech. Leg. Asp. e-Society*, pp. 307–310, 2010.

[65] P. Priit Vinkel, "Internet Voting in Estonia."

[66] M. S. Kristjan Vassil, "E-voting in Estonia : Technological Diffusion and Other Developments Over Ten Years."