Net Voting

Analysis of current net voting systems and a design for a Swedish system

Course:

Degree Project in Computer Science, First Level
DD143X, Royal Institute of Technology

Authors:

Emil Arfvidsson
Professorsslingan 10 lgh 1316
114 17 Stockholm
0737334683
emilarf@kth.se

Alexander Georgii-Hemming Cyon
Jägarstigen 78
181 46 Lidingö
0707478804
aghc@kth.se

Supervisor:

Alexander Baltatzis

Emil Arfvidsson, 890122-4975
Alexander Georgii-Hemming Cyon, 870608-0333

Abstract

This essay contains the results of an investigation about how a "perfect" internet voting system in Sweden would be implemented. No implementation has been done, this paper is merely an investigation on a theoretical level how to go about to design such a system. Which security schemes should be used in order to maintain the integrity of the voters? How should the system identify each voter? What new problems does the conversion to this internet voting system bring? Can voting coercion be avoided? Those are some of the questions studied and answered.

Sammanfattning

Denna uppsats är resultatet av en undersökning om hur ett "perfekt" nät-röstningssystem kan se ut i Sverige. Ingen implementation har utförts; uppsatsen behandlar design och framtagande på en teoretisk nivå. Vilka säkerhetsmekanismer behövs för att säkerställa röstares integritet? Hur ska systemet identifiera en röstare? Vilka problem inför nät-röstningssystem som inte fanns i det traditionella röstsystemet? Kan man undvika röststöld? Dessa är några av de frågor som behandlas och besvaras.

Statement of collaboration

The work with this essay can be divided into three parts:

1. Background reading and information gathering.
2. Designing the new system.
3. Essay writing.

The writers did not implement the system they designed. They focused on information gathering. Information gathering was performed continously during the whole project. There was no clear distribution of work in the background reading process between the writers. Emil and Alexander both spent equal parts of time in that stage.

Rough approximation of who did what:

Part	Author
Abstract	Alexander
Statement of collaboration	Alexander
Introduction	Alexander
Background	Alexander
Problems	Emil
Design	Both (mostly Emil)
Reflection	Alexander

Contents

1 Introduction **1**
1.1 Introduction . . . 1
1.2 Assignment . . . 1
1.3 Limitations . . . 2
1.4 Terminology . . . 2

2 Background **3**
2.1 Why net voting? . . . 3
2.1.1 Advantages . . . 3
2.1.2 Disadvantages . . . 3
2.2 Implementation attempts . . . 4
2.2.1 Earlier attempts . . . 4
2.2.1.1 NEDAP . . . 4
2.2.1.2 I-voting in Estonia . . . 4
2.2.1.3 Diebold AccuVote . . . 4
2.2.2 Why they failed . . . 5
2.3 Systems in use . . . 6
2.4 Design of the Estonian I-voting system . . . 8
2.4.1 Main principles . . . 10
2.4.2 Voter registration . . . 10
2.4.3 I-voting prerequisites . . . 10
2.4.4 Security procedures . . . 10

3 Problems **11**
3.1 General analysis . . . 11
3.2 Security issues . . . 11
3.2.1 Identification issues . . . 11
3.2.2 Integrity and privacy issues . . . 11
3.2.3 Trust in the system . . . 11
3.3 Usability issues . . . 12
3.3.1 Voting methods . . . 12
3.3.2 Accessibility . . . 13
3.4 Performance requirements . . . 14

4 Design **14**
4.1 Voting procedure . . . 14
4.2 Security requirements . . . 14
4.3 System . . . 15
4.3.1 Voter receives instructions . . . 15
4.3.2 Voter authentication . . . 16
4.3.3 List of candidates and parties . . . 17
4.3.4 Voter marks choices . . . 18
4.3.5 Receive and store vote . . . 19
4.3.6 Confirmation . . . 19
4.3.7 Voter anonymity . . . 20
4.3.8 Vote counting . . . 20
4.4 Security requirements summary . . . 21

5 Reflection **21**

6 References **23**

1 Introduction

1.1 Introduction

Modern cell phones are in the process of completely replacing home telephones, nowadays it is not rare that people entirely skip using a home telephone [1]. E-mail is replacing the traditional mail service [2]; even some important information from the government is sent by e-mail. The Internet has revolutionized the way people socialize, especially people born during the 1980's and later have adapted to a totally new ways of satisfying their social needs, for example Facebook. People are becoming more and more efficient (or lazy some would claim), today a certain amount of importance or urgency is required to make a phone call to your loved ones or friends; instead information, concern and affection is carried out using text messaging.

It would be quite natural to presume that these new modern ways of communicating and interacting with each other are restricted to the wealthy and industrialized countries of the west world - but this is not the case.

According to Time magazine, over 90,000 Chinese (0.0067 % of the population) are active Facebook users [3], even though the Chinese government has blocked access to the site, i.e. those users have chosen to break Chinese law by bypassing this blockade. In the same article one can read that Haiti has over 119.000 (1.224 % of the population) active users even though it is the poorest country in the Western Hemisphere.[4]

There is certainly no doubt that we live in a digitalized and Internet dependent world, where time is of the essence and where connectivity plays an essential role in people's every day life. Having said this let us draw attention to how other areas of society appears – on a technological and practical level – to be behind in comparison.

One of the most fundamental features of a democratic state is the right to vote. Although elections seldom occur more often than every third year they involve a large amount of bureaucratic work and resources. A vast quantity of papers has to be handled manually to be processed later on by some automatic counting systems (or manually, in some countries/elections [5]). Parts of the papers are being processed and counted centralized which means that resources have to be spent on logistics in order to ship votes between cities. Stating that it is a Sisyphean task to administer a whole election would maybe not be an exaggeration.

This essay will try to cover the possibilities of digitalizing and modernizing voting in order to (dramatically) decrease the effort and resources needed for an election.

1.2 Assignment

The assignment is to "pinpoint the weak points and the fortes of different possibilities and to recommend the ultimate net voting system.".[6]

A design of a theoretical net voting system will be presented. Each architectural design choice will be motivated. Existing net voting systems or suggestions for theoretical net voting systems will be used to help identify weaknesses in a design or to find inspiration for good design choices. Information found about other theoretical or implemented net voting systems will be analyzed.

1.3 Limitations

This essay is limited to a design – on a theoretical level – of a net voting system in Sweden, from a technical (an engineer's) point of view. Sweden meets prerequisites when it comes to penetration of some technical elements in society. Some of those are for example high speed internet connectivity (broadband) and electronical identification cards. The focus will be on such matters as identification, security and scalability; and not on the social impact this will have on society, politics or economy and such matters. Problems and questions raised concerning the usability will also be discussed, although it is hard to define and express limitations regarding this since it is not really a technical issue.

1.4 Terminology

Coercion refers to when someone is forced to cast a vote against their will. One could call it "vote theft".

Controlled voting is a term that signifies that the environment where the voting is taking place is a controlled place where the privacy and vote integrity of voters are secured. This is usually a polling station.

E-vote refers to a vote cast using an **E-voting** system.

E-voting is an abbreviation for *electronic voting.* E-voting means that the voting result is stored electronically (on some machine) and the result is computed from the electronically stored votes. The terms shed no light on how or if the votes are transported to be counted centrally. If the votes would be transmitted using the internet to a central server which counts all the partial results, then one could view E-voting as a slightly altered version of I-voting (or a hybrid of both terms) except that the voters have to vote from a certain kiosk rather from a remote place such as a home computer.

I-vote refers to a vote cast using an **I-voting** system.

I-voting (or sometimes **iVoting**) is an abbreviation for *internet voting.* This term is sometimes used as synonymous to *net voting* by some authors. Voters are allowed to cast votes from devices like ordinary PC's with internet connectivity, without being restricted to custom hardware or location.

Informal vote, also known as a spoilt, spoiled, void, null or stray vote, is a vote regarded by the election authorities to be invalid and thus not counted during vote counting.

Kiosk is the physical booth where the voters enter and cast their vote. In traditional ballot paper voting the voter chooses a candidate on a paper and typically puts that paper in an envelope (to hide their vote, so anonymity may be maintained) and then puts the envelop in the ballot bin.

Net voting could refer to two things. Either **I-voting** or **E-voting** where votes are sent over the internet from **kiosks**.

Paper trace refers to some kind of physical paper copy of each vote, presumably a paper roll which logs each vote. This makes storage of data redundant.

Uncontrolled voting signifies an uncontrolled environment where there are no guarantees of integrity or privacy. This could be the home of a voter or a public internet café.

2 Background

2.1 Why net voting?

The general discussion about whether society should use net voting or not is too extensive to be dealt with in this essay. But in order to understand the concept of net voting it is good to know some of the fundamental arguments for and against it.

2.1.1 Advantages

- Net voting could increase voting turnout.
- Net voting could minimize the risk of ambiguities as the voter makes his/her choice somehow electronically instead of physically marking his/her choice on paper (which could be undecipherable), thus minimizing the number of informal votes.
- Net voting could minimize the need for recounts as votes are counted electronically removing the human error factor.
- Net voting could provide possibility for faster calculation of results.
- The overall cost of an election would decrease since there would not be a need for personnel to count votes. The logistical cost would also decrease or disappear totally, since there would be no paper ballots to transport.
- Since voters can vote from anywhere in the world it is likely that the number of people voting would increase. Charles Stewart – a distinguished Professor of Political Science at Massachusetts Institute of Technology (MIT) – estimates that "1 million more ballots were counted in 2004 than in 2000 because electronic voting machines detected votes that paper-based machines would have missed" (in the US).[7] And in this case "electronic voting machines" refers to E-voting in kiosks.

2.1.2 Disadvantages

- It is hard to design a secure system, a system as safe as paper ballot voting. Although some people claim that net voting could be more secure than paper ballot voting.[8]
- Electronic failures might occur with such a system. This brings risks such as loss of data. Such risks result in a large requirement of redundancy of data. Could be solved with a paper trace (only works for E-voting though).
- It is more difficult for the voters to understand a net voting system as it places great reliance on technology. A limited part of the population has the necessary knowledge to understand it. This makes it harder for citizens to trust the system, this is a major big issue.
- Net voting brings a risk for coercion or forcing.
- Some election candidates may concentrate their PR-campaigns on the Internet voters at the expense of the attendance voters (would not be a problem if net voting was the only option).

- The initial cost of the net voting system would not be small. The system would probably also need some kind of support staff that voters could contact, which costs as well.

2.2 Implementation attempts

A handful of different E-voting and I-voting systems have been developed and some of them have even been used. But most of them have failed for various reasons mentioned below.

2.2.1 Earlier attempts

2.2.1.1 NEDAP

One of the first countries to use E-voting in an election was Germany. In 2002, the German government used an E-voting machine called *NEDAP* or Groenendaal ES3B in the federal elections. The NEDAP voting machine was developed by the Dutch company NEDAP and belongs to the class Direct Recording Electronic (DRE) of voting computers. Over one million voters used this E-voting system. Three years later, in the federal election of 2005 an additional one million voters used the system. In the autumn of 2006, 90 percent of the votes in The Netherlands were cast on the NEDAP voting machine.[9] Slightly modified versions of the very same machine were used in Germany and France. In October 2006 the machine was hacked by the anti E-voting group *Wij vertrouwen stemcomputers niet* (We don't trust voting computers). In the paper *NEDAP/Groenendaal ES3B voting computer – a security analysis* – they explained how, after having hacked the machine, they managed to manipulate the election results without leaving any trace of intrusion in the software.

2.2.1.2 I-voting in Estonia

The first national election ever to use I-voting were the municipal elections in Estonia in 2005.[10] In a study of this election one can read that 1.85 percent of the voters used the I-voting system to vote over the internet.[11] A large proportion of I-voters, over 80 percent, declared that they wanted "to use I-voting in the future and for all types of elections in which it would be proposed as an alternative means of participation". In the same study the authors stated that they had found that I-voting was "completely neutral with respect to such crucial variables as gender, income, education and the type of settlement".

2.2.1.3 Diebold AccuVote

The American company Diebold has developed a series of voting machines. One model is called *Diebold AccuVote-TS* and its successor *Diebold AccuVote-TXs*. These machines are together the most widely deployed electronic voting platform in the United States. Over 10 percent of all voters in 2006 in American elections used these machines, according to a paper published by Princeton university [12]. The paper is entitled *Security Analysis of the Diebold AccuVote-TS Voting Machine* and presents major security issues with these machines. Two Princeton students report how they managed to install malicious software on the voting machine that "steals" (changes) a vote on candidate A to a vote on candidate B. To do so one needs to:

1. Transfer the malicious software to a memory card.

2. Open the memory card slot on the machine, behind a small side door with a lock. The key for the lock is a small key of standard type and there are hundreds of keys in circulation. Any of these keys can easily be copied at a hardware store/locksmith. The Princeton students also succeeded in picking the lock in under 5 seconds after some practice.
3. Wait one minute for the malicious software to auto-install after having rebooted the machine.

In other words, the Diebold machines are as insecure as the NEDAP. Not only was it possible to steal votes, but one could also spread the malicious software (virus) to other voting machines. This could occur when the machinist inserts a memory card in a "contaminated" machine when performing a firmware update, the virus could then spread to the memory card and contaminate other machines inserted with that same memory card.

2.2.2 Why they failed

Both the Diebold AccuVote and the NEDAP E-voting machines had major security flaws which hopefully were discovered before any binding election was tampered with.

Diebold failed not only because they programmed a hardware with major security glitches but also because they put minimum effort in construction of the machine. The key to the side door (that protected the memory card slot) lock is the same key used for mini bars at hotels (i.e. a key which is easy to acquire). [12] The company also posted a picture of the key on the company web page, in which the alphanumeric model code could be seen. Anyone could then, by referring to this code, purchase the very same key from any locksmith.

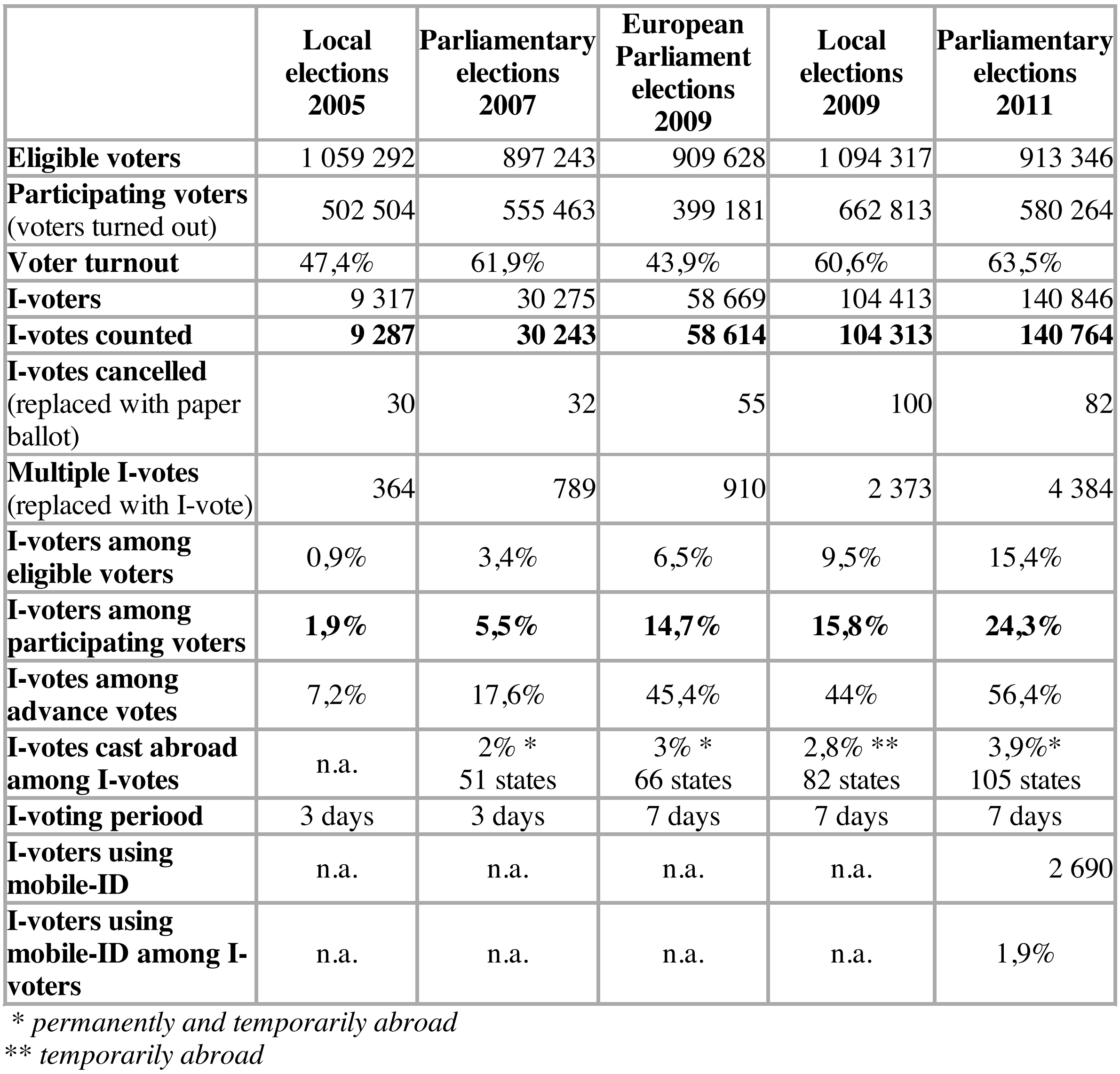
As a result of the poor design and construction of the Diebold machines they were banned in the State of California in 2004 and the State of Colorado in 2007. [13][14]

The NEDAP machine failed because of insecure software. A system of such great importance as voting must not contain such fundamental security glitches that permit stealing of votes.

The NEDAP machine was banned in the Netherlands in 2007 and in Germany in 2009. [15][16]

2.3 Systems in use

In Estonia I-voting was used in the parliamentary elections in March 2011. This is the fifth time that the country offered the voters the option to vote using home computers and internet. [17]



	Local elections 2005	**Parliamentary elections 2007**	**European Parliament elections 2009**	**Local elections 2009**	**Parliamentary elections 2011**
Eligible voters	1 059 292	897 243	909 628	1 094 317	913 346
Participating voters (voters turned out)	502 504	555 463	399 181	662 813	580 264
Voter turnout	47,4%	61,9%	43,9%	60,6%	63,5%
I-voters	9 317	30 275	58 669	104 413	140 846
I-votes counted	**9 287**	**30 243**	**58 614**	**104 313**	**140 764**
I-votes cancelled (replaced with paper ballot)	30	32	55	100	82
Multiple I-votes (replaced with I-vote)	364	789	910	2 373	4 384
I-voters among eligible voters	0,9%	3,4%	6,5%	9,5%	15,4%
I-voters among participating voters	**1,9%**	**5,5%**	**14,7%**	**15,8%**	**24,3%**
I-votes among advance votes	7,2%	17,6%	45,4%	44%	56,4%
I-votes cast abroad among I-votes	n.a.	2% * 51 states	3% * 66 states	2,8% ** 82 states	3,9%* 105 states
I-voting periood	3 days	3 days	7 days	7 days	7 days
I-voters using mobile-ID	n.a.	n.a.	n.a.	n.a.	2 690
I-voters using mobile-ID among I-voters	n.a.	n.a.	n.a.	n.a.	1,9%

* *permanently and temporarily abroad*
** *temporarily abroad*

Figure 1: This table, with I-voting statistics, was taken from the Estonian National Electoral Committee [18]

Please see the table in figure 1 with detailed statistics about the five elections in Estonia when the voters were presented with the option of I-voting. There has been a constant increase of confidence in I-voting from the voters in Estonia, the amount of votes cast by I-voting has increased from 1.9 percent to 24.3 percent in six years. As can be seen in the graph in figure 2, the increase rate has significantly accelerated. One could state that the increase rate is exponential. This means that the share of I-voters will reach the level of 50 percent long before the year 2015 if the increase rate does not dramatically decline.

One can also see that the voting turnout in Estonia has increased from 61.9 percent to 63.5 percent between the parliamentary election in 2007 and 2011. This growth could have something to do with I-voting. Professor Rüdiger Grimm (University of Koblenz, IT risk management) said the following in an interview about net voting's impact on the turnout: "With e-voting you can vote where ever you are, whenever you want - we don't have evidence but this must increase participation." [19]

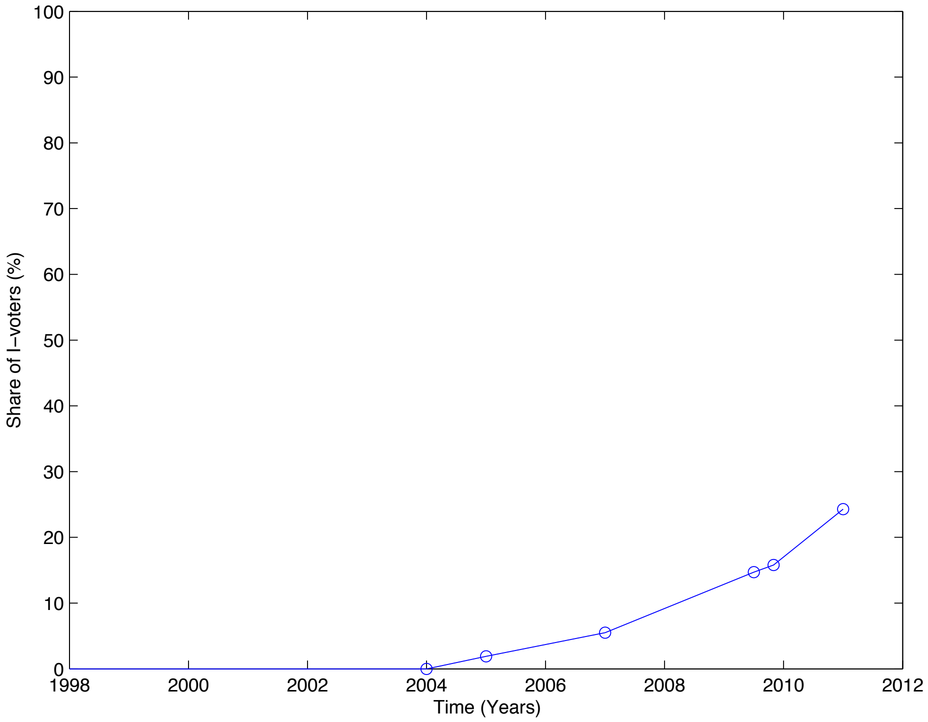


Figure 2: This graph shows the increasing popularity of I-voting in Estonia (plotted with Matlab).

But the success of I-voting could of course come to an end due to reports like the one the Estonian news agency *Eesti Rahvusringhääling* (Estonian Public Broadcasting) published in March 2011, four days after the Estonian parliamentary election. In the news report it was presented that the university student Paavo Pihelgas claimed to "have found a fatal flaw in the online election software that could make it possible for a virus to block certain candidates without the voter ever knowing that tampering had occurred".[8] Tarvi Martens, the head of the I-voting project in Estonia, replied that I-voting is "more secure than old-fashioned paper voting".

2.4 Design of the Estonian I-voting system

Some countries use a "double envelope" scheme for postal voting (see section 3.3.1), in order to guarantee secrecy of the vote. The Estonian system, in this section hence called *The System* tries to mimic this digitally.[20] People's votes are encrypted by a voting application (the election software) and then signed digitally. This is somewhat equal to sealing the vote into the "inner envelope" and then putting that envelope in the outer one with the personal details on it, please see figure 3.

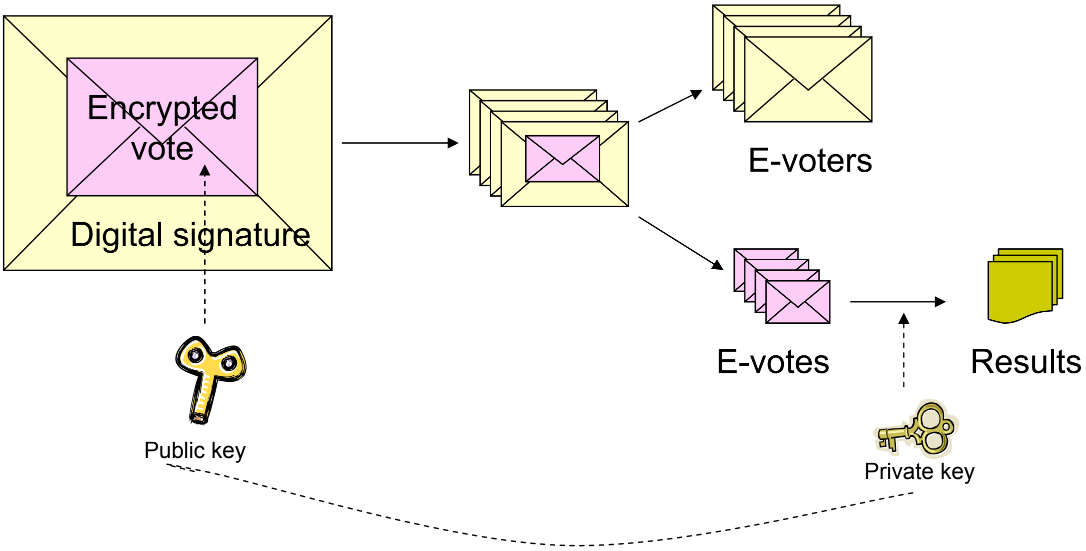


Figure 3: Picture that illustrates the double envelope scheme used in Estonia.[21]

When the vote has been encrypted and signed ("put in the outer envelope") by the voter it is sent to the servers for *The System* for checking and to ensure that only one vote per voter will be counted. *The System* utilizes public key cryptography, which consists of a pair of keys; a public and a private key. When the vote is encrypted with a public key, it cannot be decrypted with anything other than the corresponding private key. *The System* then decrypts the encrypted votes before counting using the private key. The counting procedure is done in the following way:

- The digital signature with the personal data is removed (the outer envelope is being discarded).
- The anonymous and encrypted votes are entered into the counting system.
- The votes are decrypted using the private key.
- All votes are counted.

Please see the figure 4 below for a schematics over the design of the Estonian I-voting system.

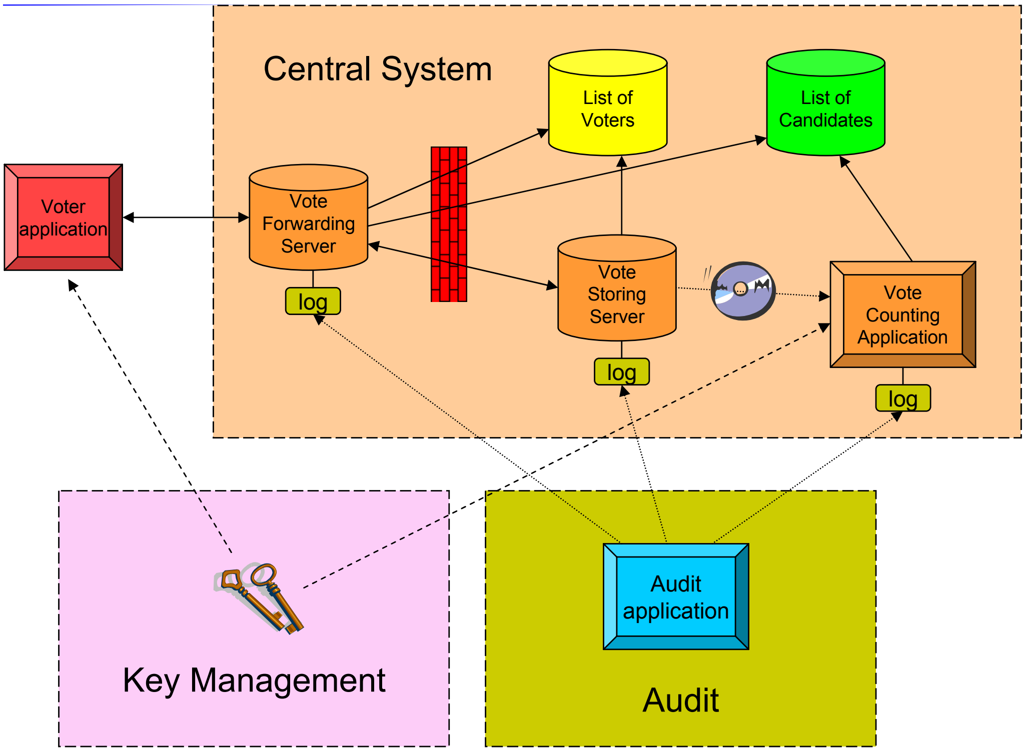


Figure 4: Picture illustrating the architecture of the Estonian I-voting system.[21]

The specification below over *The System* is taken from a paper released by The Estonian National Electoral Committee.[22] In the same paper one can read the following explanation of the parts of *The System*:

- **Voter** - e-voter[1] with his/her PC. Creates an encrypted and digitally signed vote and sends it to the Central System.

- **Central System** - System component that is under the responsibility of the National Electioral [*sic*] Commmittee. Receives and processes the votes until the composite results of e-voting[2] are output.

- **Key Management** - Generates and manages the key pair(s) of the system. The public key (keys) are integrated into Voter's applications, private key(s) are delivered to Vote Counting Application.

- **Auditing** - solves disputes and complaints, using logged information from the Central System.

[1] referred to as I-voter by the terminology in this essay.

[2] referred to as I-voting by the terminology in this essay.

2.4.1 Main principles

The System follows all major principles of paper-voting:

- The I-voting is allowed during a certain period before Election Day.
- The user utilizes an ID-card with a chip on it, and a personal pin code.
  - *The System* authenticates the user.
  - The voter confirms her choice with a digital signature (the pin code).
- Repeated I-voting is allowed, only the last I-vote is counted.
- Manual re-voting is allowed, if vote is cast using paper ballot system during the Election Day, the I-vote will be revoked.

2.4.2 Voter registration

- All citizens (residents) register their home address in a central population register.
- Only voters with registered addresses are eligible.
- The governmental population register is used.

2.4.3 I-voting prerequisites

- Voter needs an Estonian ID card with valid certificates and PIN-codes.
- Voter needs a computer with:
  - Reader for the ID-card.
  - ID-card drivers.
  - One of the following operating systems: Microsoft Windows, Linux or Mac OS X.

2.4.4 Security procedures

- All security-critical procedures are logged, audited & observed and videotaped.
- Network-monitoring 24/7 to ensure protection against DDoS[3] or trojans.
- Two independent parties are responsible for guarding the server room.
- Strict requirements for entering the server premises.
- All hardware is sealed and protected.

[3] internet attack when many computers simultaneously and collectively overload a server

3 Problems

3.1 General analysis

The problem with the current ballot voting system is that it is inefficient.[23] Every voter has to go to the polling station and mark their vote on a ballot. Their identity is then confirmed by checking the ID of the person voting and comparing it with a pre-printed list of eligible voters. The ballot is then placed in the ballot bin and the person voting is marked as *has voted*. After the polling station has closed the votes are counted manually or scanned. After the initial counting the ballot papers are sent to a central location for storage in case a recounting of the votes is requested.

The problem consists of designing a net voting system that has no serious drawbacks when compared to the traditional ballot voting system but improves on the drawbacks of the traditional ballot voting system. It should shorten the handling time, reduce the cost and lower the time required to perform a nation-wide election. A digital replacement of ballot voting is not trivial to design and implement.

3.2 Security issues

3.2.1 Identification issues

Before a vote is cast, the voter has to be identified as eligible to vote. This applies to any net voting system as well as the traditional ballot voting system. In the Swedish ballot voting system a national ID card is required or a voter's identity can be attested by a person with ID card.[24]

To identify users electronically some kind of electronic identity for each voter is needed. To create electronic identities to facilitate net voting alone is probably not necessary however, since electronic identities are commonly used as means of identification when using electronic resources in Sweden (such as internet banks or governmental institutions).[25] The same identities could be used to identify voters, where every voter would need an electronic identity to participate. Countries without any standard electronic identities will need to create such a system before it is possible to identify voters electronically.

3.2.2 Integrity and privacy issues

There are several ways in which the integrity and privacy of a voter can be violated. When voting is taking place in an uncontrolled environment, which as earlier defined is called uncontrolled voting, the voter can be influenced, coerced or forced by other means to vote in a certain way or display their vote to others. This is a big issue when uncontrolled voting is used.

3.2.3 Trust in the system

One of the elements playing a central role in the success of a net voting system is trust. A system, even though not perfectly secure, could still function as a successor to the traditional voting methods provided that the citizens trust it. The matter of trust goes both ways of course, if a perfectly secure system is not trusted by the citizens, then it will fail to become a standard.

The Estonian National Electoral Committee released a pamphlet with information about the elections and internet voting system in Estonia.[21] In that document there is a heading with the title “What it takes” – only displaying the following picture:

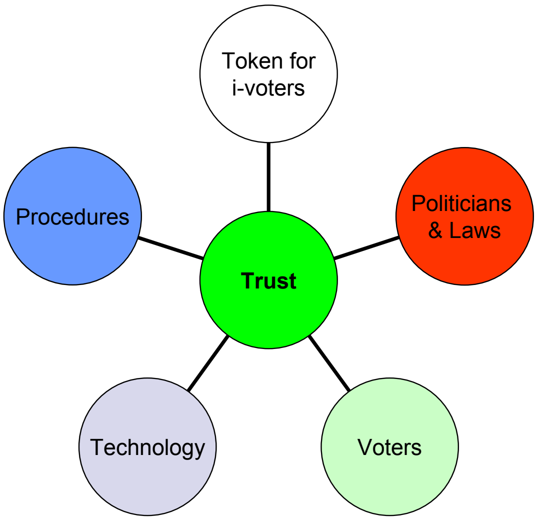


Figure 5: This is “What it takes” to make a net voting system successful according to the Estonian National Electoral Committee.[21]

This is interesting because it reveals that the organization responsible for the development, maintenance and administration of the elections in Estonia thinks that trust is the single most important element when it comes to the success of the system.

3.3 Usability issues

3.3.1 Voting methods

A voting system has to be usable by everyone and one system only might not be sufficient to provide voting capability. In Sweden there are five ways for a voter to cast their vote; voting in a polling office on election day, advance voting in a polling office before election day, vote via letter, vote via embassy or vote via proxy.[26] These different possibilities exist to enable as many Swedish eligible voters as possible to register their votes.

The advanced voting and voting on election day in a polling office is necessary since an electronic voting system cannot rely on all voters having access to the required hardware. An electronic voting system of any sort will require some hardware and connectivity such as computers, smart phones or specially crafted hardware plus access to internet or other network. That hardware and connectivity must be provided to the voters since they cannot be expected to posses it. Polling offices (kiosks) are a suitable place for this since they are regionally distributed and recognized by voters.

The vote via embassy can be solved by equipping the embassies with the same voting system with which the polling offices are equipped. There is then no need to introduce a separate mechanism for voting via embassy. This simplifies the voting system in general when there is no difference between votes cast at a polling office or votes cast at an embassy. This solution does, however, introduce an extra requirement on the electronic voting system: it needs to function outside the country. The usability requirements do not change since voting at an embassy is essentially the same as voting at a polling office. If voters are limited to using the electronic voting system at embassies voters will have to acquire the electronic identities needed.

One other alternative is to handle the embassy votes as before, with each voter's ballot being sent to the voter's polling station, where a polling office worker will submit the votes into the system. This creates the requirement that the electronic voting system must be able to receive votes from authorized polling office workers.

Can the proxy vote be performed when an electronic voting system is used? In Sweden, vote by proxy is a rather complicated process. The voter is required to pre-order proxy voting material, such as a custom election envelope and envelopes for the ballots. The voter is also required to acquire the ballots, which can be found at any polling station. The voter puts the ballots in the correct envelopes in the presence of the proxy and a witness. The proxy and witness fill in details on the envelope. The proxy then brings the vote envelope to the voter's polling station and the polling station workers place the votes in the ballot box.[26] This creates a need for polling station workers to be able to enter voting data manually. However, in order not to disclose the voter's identity and vote, the entering of a proxy vote has either to conceal the identity of the voter or the particular vote from the polling station worker who enters the vote.

Can an electronic voting solution replace all of these five ways of voting? It can as proven by earlier electronic voting systems[23], replace two of them, the voting on election day and the advanced voting before election day. Proxy voting and embassy voting are issues that need to be solved by other means.

3.3.2 Accessibility

The user interface for the electronic voting systems must be adapted for the users' needs. It has to be accessible for all eligible voters. This requirement is not only set on the voters' interaction with the system but also on the polling station workers' interaction and the central organization reading the results.

This places requirements on the graphical design of the applications used when voting. The interface must be user friendly and easily understood by all voters. This is an imprecise requirement since user interfaces, in general, are difficult to verify.

Voters must get a certain feedback after having voted, they must have the feeling that their vote is registred. Margaret McGaley – spokesperson on ICTE[4] (Irish Citizens for Trustworthy Evoting) – said the following after the Dutch E-voting machine NEDAP was hacked:
"Any system which lacks a means for the voter to verify that their vote has been correctly recorded is fundamentally and irreparably flawed"

[4] See for info on their webpage: `http://evoting.cs.may.ie/`

3.4 Performance requirements

The performance requirements are not a key feature. However, the system must be scalable. This means that our solution must not depend on any single component that is not scalable. Simply put, the voting system must be able to increase its voter capacity by increasing the allocated hardware and bandwidth.

In Sweden there were 6 028 682 votes cast in the national election [27], while 2 377 639 of these were carried out in the advance voting period [28]. In this election there were 7 441 398 eligible voters which means that 81 percent participated in the election.[29] The advance voting period is 19 days long and starts 18 days before election day. This means that 3 651 043 votes were cast on election day. On Election Day, polling stations are open for 12 hours between 8.00 am and 8.00 pm. This gives a peak rate of roughly 300 000 votes an hour. Since distribution is not necessarily uniform however, the peak could be higher.

4 Design

Now that earlier net voting systems have been investigated, explained and design problems have been defined and studied, a new system can be presented. Since the Estonian system is trusted and used by 24.3 percent of the voters it will be used as inspiration. The system should be transparent and even though not all voters have the necessary technological knowledge to understand the information they will still be able to access such information. This could help citizens place their trust in the system.

4.1 Voting procedure

A voting procedure can now be described. First, the voter has to connect with the system. The voter has to identify him- or herself to the voting system in order to return the correct party and candidate list, since these differ regionally. The party and candidate list is then sent out to the voter. When the voter has finished marking his or her choices the choices are sent into the system. The system responds with a confirmation to the voter that the choices were received. See figure 6 for a graphical representation.

4.2 Security requirements

The security requirements for net voting systems are as listed in the table below. The requirements are composed from standard ballot voting requirements combined with additional limitations to counter weaknesses due to voting through a net voting system.[30]

- Accuracy - all valid votes are counted, all votes counted are valid and no cast vote cast can be altered.
- Only eligible voters - only votes from eligible voters should be received.
- No duplicate votes - only one vote should be counted for each voter.
- Voter privacy - it must not be possible to link a voter's identity with its vote.
- Coercion-resistant - it should not be possible to coerce a voter to vote in a certain way.

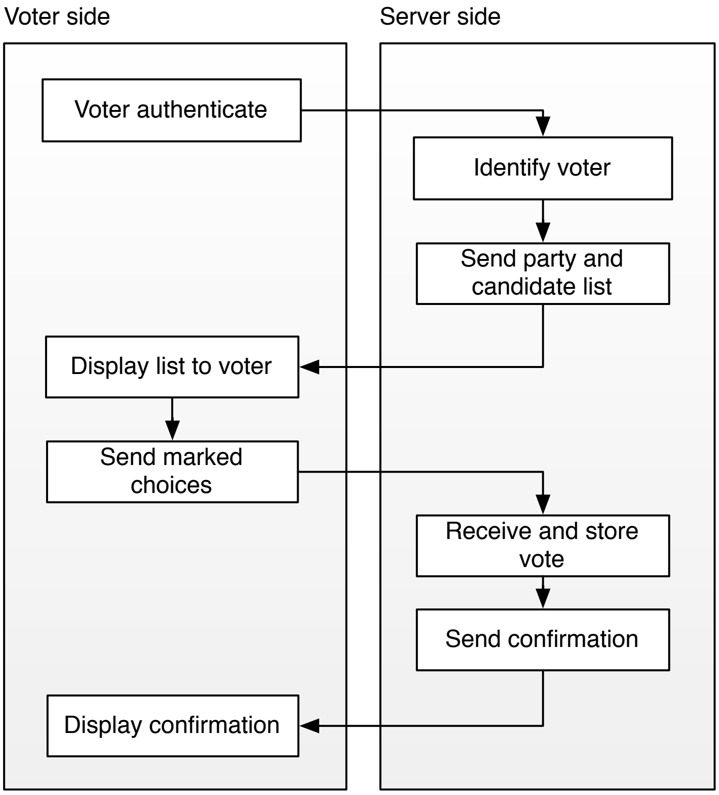


Figure 6: Basic flow chart of vote procedure

- No interference - no person or third party should be able to disrupt the voting.
- No premature disclosure of votes - keep vote counts secret until election is over. The system must keep the vote tally secret until the election is over.

4.3 System

4.3.1 Voter receives instructions

The voter will be informed on how to vote and what needs to be done in order to become an eligible I-voter. When ballot voting is used there are poll cards sent out in advance to every eligible voter. This system will also need instructions sent out in advance. The instructions are expected to be combined with the ordinary poll card sendouts and will therefore not cause additional letters to be sent out, although the sent out papers will increase. The increase in sent out paper is motivated and explained in section 4.3.6.

4.3.2 Voter authentication

The voter authenticates via an electronic identity authority. There are several electronic identity providers. *BankID* is the most commonly used electronic identity in Sweden and will therefore be used.[31] However, since many electronic identities are similar it would be easy to replace or extend the authentication mechanism to support other types of electronic identities.

In order to get a BankID in Sweden the users have to complete a process similar to the following:

- The user signs up for internet banking services.
- A package containing a credit card reader is sent to the user's home address.
- The user logs on to the internet bank by using this:
  - The user opens a web browser and navigates to the internet bank log-in site and enters his social security number.
  - The user inserts his credit card into the credit card reader and enters a control code displayed on the web page.
  - The card reader prompts the user for authentication by entering the pin code for the credit card.
  - The card reader displays a confirmation code, uniquely paired with the control code entered. The user enters this confirmation code on the internet bank log in page and is now logged in.
- The user downloads his/her BankID (the digital authentication certificate file) and chooses a password that permanently links to that BankID.
- The user also needs to download the BankID software that reads the BankID file.

A large part (40 percent) of the population in Sweden already has access to BankID, so not all of Sweden's 7 441 398 eligible voters [5] will need to follow the procedure above, in order to acquire BankID).[32][33] When the user has access to BankID (s)he needs to complete some additional preparations before (s)he can cast his/her vote:

- The voter navigates to the voting portal using an arbitrary web browser and downloads the voting software.
- After having installed the software the program prompts for login credentials, the BankID software starts and asks the user to enter the password linked to the BankID.
- The user is now logged in and can mark their choice in order to cast their vote.
- The user is then again prompted for authentication to confirm their choice.

The choice of using voting software instead of letting the users vote directly on the web page is in order to achieve maximum compatibility with the voter's computer. The software has to be developed so that it runs on the most common platforms.

[5] This was the value in September 2010, the actual number is slightly higher

4.3.3 List of candidates and parties

There are security issues in displaying the list of candidates and parties in clear text. Malicious software on the voter's device or computer could listen to the data and interpret it, and try to interfere when certain votes are cast. Even if the transmission of the list and choices were encrypted, a malicious piece of software on the voter's computer could visually distinguish marks and then choose to interfere upon seeing certain choices. To solve these problems the parties' and candidates' lists must be obfuscated so that no malicious software on the vote computer can determine what the voter is about to vote on. This was one weakness in the Estonian voting system that was not accounted for. If the list is obfuscated, the voter has to be provided with the true values for each choice. This list of true values could be distributed on a vote card that is sent out in advance. It could also be provided through mobile phones. However, since there are already vote cards sent out in Sweden, voters are well accustomed to receiving instructions via postal mail and this is the channel which the true values will be distributed via. If this second channel is compromised then this solution will not provide any extra security. It will, however, be harder to launch large scale attacks since each letter would need to be intercepted.

Obfuscation of the codes could be carried out in several different ways. One approach is simply to match parties and candidates to number codes. The vote card would then contain information as in figure 7. The voter would vote by looking up the code for the desired party and candidate on his vote card and then mark those numbers as his choice on the screen. These cards are randomly generated for each voter and therefore likely unique. The codes are then sent to the server which has stored the match. Another approach is to use images instead of number codes. The possible advantage is that images could be less prone to errors from the voter. The images used need to be neutral. The voting card would in that case contain the same list as in figure 7 but with images instead of number codes.

Party 1	431
Party 2	131
Party 3	145
⋮	⋮
Candidate 1	683
Candidate 2	242
⋮	⋮

Figure 7: Example vote card with number codes

In both cases security depends on the security of the second channel through which the vote cards are distributed. If the second channel is compromised, then the codes or images for each voter could become known, and malicious software could interfere with the voting, as mentioned earlier. On the server side, the system has to store mappings between voter, images and party or candidate as visualized in figure 8.

However, while images might be easier to remember and recognize than numbers, it is difficult to arrange and display images in a natural order. So if there are a lot of parties and candidates images would probably become more confusing than helpful. It is also difficult to generate a vast number of images that are neutral and easily identified by the voters. Therefore, the number list will be used. The number list will also allow for using error correcting codes, so that one wrongly

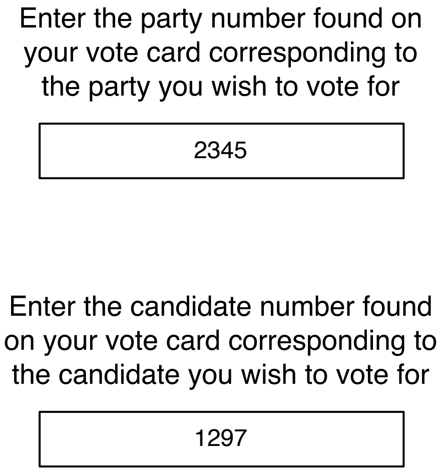
Voter	**Image**	**Party or candidate**
Voter 1	♣	Party 1
Voter 1	♢	Party 2
⋮	⋮	⋮
Voter 1	♠	Candidate 1
⋮	⋮	⋮
Voter 2	△	Party 1
⋮	⋮	⋮

Figure 8: Server keeps a match of voters, images and party or candidates

typed digit can be detected and the voter alerted. The server has to keep a match between voter, code and party/candidate.

4.3.4 Voter marks choices

The voter application will display an interface to the voter indicating that the choices should be filled in as illustrated in figure 9. The voter chooses by looking up what number the selected party and candidate has on the received vote card, as seen in figure 10, and then enters those numbers. After the voter has entered their choices they can press “Next” to see a summary before choosing to send the vote. The voter will be asked to sign their vote using their BankID. This first packages the codes into votes, then encrypts the votes using the public key of the server and then signs the package. This corresponds to the double envelope scheme as earlier described in section 2.4.



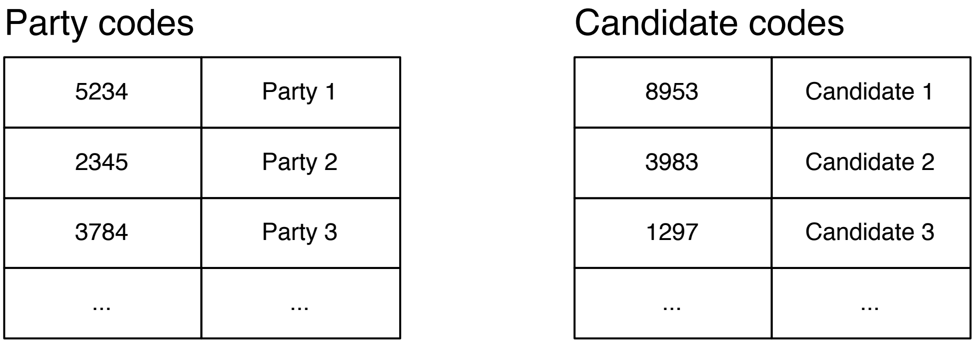
Enter the party number found on your vote card corresponding to the party you wish to vote for

2345

Enter the candidate number found on your vote card corresponding to the candidate you wish to vote for

1297

Figure 9: An example interface for marking votes



Party codes

5234	Party 1
2345	Party 2
3784	Party 3
...	...

Candidate codes

8953	Candidate 1
3983	Candidate 2
1297	Candidate 3
...	...

Figure 10: An example vote card for a voter

4.3.5 Receive and store vote

Each vote is sent to the voting system encrypted and signed (with BankID) using the double envelope scheme (please see previous section 2.4 for details). The inner envelope is encrypted with the public key of the vote system. The system utilizes a public-private keypair for encryption of the inner envelopes. The public key of the system is distributed and used for encryption while the private key is kept secret in an isolated part of the system and used for decryption. To be able to vote several times, the votes must be stored and it must be possible to link each vote with a voter, so that the old vote for a certain voter can be replaced by a new one when that voter re-casts his or her vote. The digitally signed votes are stored on the system as long as the election lasts.

After the system has received a vote it must send a confirmation code back to the user. Please see next section 4.3.6 for details about the confirmation code.

4.3.6 Confirmation

The voter should have feedback from the voting system when their vote has been received. After the user's vote has been cast and sent to the system, the user should receive some kind of confirmation that the system registered the same vote as the voter cast. The same code system mentioned in section 4.3.3 could be used, but with other codes. So for example, if the voter cast her vote on the party with code 131, namely *Party 2*, she receives a message telling her that she has voted for the party with code 932. The user can then in a table sent to the voter by mail (that matches parties and candidates to confirmation codes) look up which party corresponds to the code 932 and verify that code 932 equals *Party 2* and thus verify that the system registered the correct vote.

The whole idea of using confirmation codes is that a trojan, virus or any kind of malicious software must not be able to hijack the voting application and furtively manipulate the vote. The malicious software might try to show a fake confirmation message to the user. The voting system server sends the correct confirmation code corresponding to the vote it **registered**, regardless if that vote was modified by malicious software. This means that the server must, based on the vote, determine and look up the corresponding confirmation code in the table of individual codes and then send the confirmation code back to the voter. This prevents malicious software from intercepting the vote and displaying a false confirmation code to the user.

The confirmation code can be generated in several different ways. The first and obvious solution is that when a vote is received into the system the receiver strips the outer envelope, decrypts the inner envelope (which then gives the obfuscated codes), looks up the codes in the voter – code – party – candidate match and returns appropiate confirmation codes. However, the decryption of the inner envelope would require the private key. This is suboptimal because the private key should be locked down and restricted for usage only in isolated parts of the system. The receiver should therefore not have access to the private key, which means it is not allowed to "peek" into the inner envelopes. A solution to this is instead to precompute hash values[6] for the inner envelopes. This is a rather large precomputation since it involves precomputing all possible vote values for each voter. The procedure for precomputation is as follows: for each voter, assemble all possible inner envelopes and for each possible envelope, encrypt it, calculate the hash value and store the hash value. This results in building a complete table that maps voter – hash value – party – candidate.

The procedure for receiving and sending confirmation is then easily summarized: verify the voter signature, temporarily remove the voter signature, calculate the hash value of the inner envelopes and return confirmation codes.

4.3.7 Voter anonymity

Voter anonymity will be preserved using the slightly modified double envelope scheme which the Estonian System also uses. Please see previous section 2.4 for details about the original double envelope scheme and section 4.3.6 for the modifications performed.

4.3.8 Vote counting

When the voting period is over and counting is to commence, each of the uncounted envelopes is identified and with that identification linked to a vote code match table that allows deobfuscation of the codes into the actual parties or candidates. For each identified party or candidate, increase its counter with one. When a vote has been counted it is saved as an anonymized vote before the original double envelope is deleted. It is not possible to link an anonymous vote to a voter since the original votes with signatures are deleted. The anonymous votes will, however, contain information from which county they were cast (enabling relevant statistics).

This system will, like the current Swedish election system, save all votes until next election (at least).[34] This is done to offer a complete overview of the election result. Anyone will be able to see statistics about the election. This helps avoiding scenarios where people accuse the net voting system of being faulty and thus helps ensuring the citizens' trust in the system.

The system must not allow counting of the votes to start before the election period is over. Premature disclosure of vote results could influence voters decision.

[6] A hash value is a representation similar to a checksum. For more info see `http://www.cgisecurity.com/owasp/html/ch13s05.html`

4.4 Security requirements summary

A short summary of solutions to requirements is presented now. See section 4.2 for the original requirements.

- All votes are verified as valid before storage and all of the stored votes are counted. No cast vote can be altered since they are signed with each voter's identity.
- Only eligible voters are allowed to vote since they are identified and can be verified to be eligible before their vote is stored.
- No duplicate votes are stored. This is confirmed upon receipt of a vote.
- Voter privacy is ensured by storing the votes. Although the signatures are stored with the votes, the votes can only be read by decrypting with the private key. The private key must not be compromised.
- Coercion-resistant by allowing voters to cast a vote multiple times. This minimizes the risk of coercion affecting the election results.
- No interference should be possible, the scheme used allows for verification of votes being properly received. However, ordinary DDoS attacks could still pose a problem. How to handle DDoS attacks is in this case implementation specific and will not be covered.
- Keeping the vote count secret until the election has closed is performed by not initiating a count until the election period has ended.

5 Reflection

Net voting is a topical subject and there is a vast quantity of essays, papers and reports on the subject. Many countries have tried electronic voting systems but chosen to abandon them due to lack of security. One can conclude from this essay that it is a serious non-trivial mission to design the *perfect* net voting system. The design mentioned here has taken inspiration from several earlier attempts and fulfilled requirements which they did not. However, it is hard to say if this system could succeed in becoming a standard, because it is crucial for citizens to trust it, which is virtually impossible to determine. When the older generation is replaced by the younger and more tech-savvy ones, it is possible that the prospects for net voting looks even better than it does right now.

One of the disadvantages presented in section 2.1.2 was the risk of coercion that I-voting brought. It is not possible to prevent a voter from being forced into voting against her will in uncontrolled environments (such as a voter's resident). The net voting system presented in this essay handles this issue. The solution is that a voter can vote unlimited times until the election closes. This means that if a voter is coerced to vote in a certain way they can always re-cast their vote at a later time. However, a small number of voters could still be coerced to cast a vote just before the election closes. This is acceptable, since there is no clear solution to this scenario.

Problems with identification has been solved using *BankID* which is already used by a large part of the population, this will hopefully help building up the citizen's trust in the system, since they would be using an identification system they already are used to.

The drawback of this system is that the Swedish government has to create and mail out a table with confirmation codes to every eligible voter, a table which contains hundreds of codes and thus requires several pages of paper. In comparison with todays system this is not a problem however, since every eligible voter already receives a letter with papers needed for voting. The postal service will not become especially more expensive if the envelope contains more papers. Another important aspect to take into consideration is that less ballot paper votes needs to be transported and counted which most likely will result in a smaller price tag of the election all together.

The benefits of net voting are numerous, hopefully will it not only dramatically reduce the costs of elections but also minimize (or completely remove) the risk of computational mistakes. However, these factors are merely bonus benefits; the single most important one is the possibility of an increase in voting turnouts. Net voting makes voting easy accessible and minimizes the effort required by the voter, and it seems to appeal the younger generation.

In a society where we perform our banking businesses, check-in for flights, order food to the residence and declare income taxes over the internet, would it not be natural to vote over the internet as well? The system mentioned in this essay addresses issues associated with net voting. The fate of the system now lies in the hands of the citizens.

6 References

[1] M. Wallström, "Kaos när mobiler ersätter fast telefon." http://www.idg.se/2.1085/1.210444/kaos-nar-mobiler-ersatter-fast-telefon, 2009. [Online; accessed 29-January-2011].

[2] G. stad, "Bättre service och miljö med digitala remisser." http://www.goteborg.se/wps/wcm/connect/goteborg.se/goteborg_se/invanare/bygga_bo/stadsplanering/detaljplaner/art_n300_bb_stadsplanering_digitalaremisser, 2009. [Online; accessed 29-January-2011].

[3] L. Grossman, "Person of the year 2010." http://www.time.com/time/specials/packages/article/0,28804,2036683_2037183_2037185,00.html, 2010. [Online; accessed 29-January-2011].

[4] Central Intelligence Agency (CIA), "The world factbook." https://www.cia.gov/library/publications/the-world-factbook/geos/ha.html, 2011. [Online; accessed 31-March-2011].

[5] People's Daily Online, "Votes to be counted manually in cote d'ivoire's presidential elections." http://english.peopledaily.com.cn/90001/90777/90855/7174700.html, 2010. [Online; accessed 29-January-2011].

[6] Royal institute of technology (KTH), "Essay project proposals." http://www.csc.kth.se/utbildning/kth/kurser/DD143X/dkand11/ProjectIdeas/, 2011. [Online; accessed 31-March-2011].

[7] Wikipedia, "Electronic voting — wikipedia, the free encyclopedia." http://en.wikipedia.org/wiki/Electronic_voting, 2011. [Online; accessed 9-April-2011].

[8] K. Rikken, "Student finds flaw in e-voting, seeks nullification of result." http://news.err.ee/Sci-Tech/ed695579-af05-48ab-8cc0-3085e5f0c56c, 2011. [Online; accessed 27-March-2011].

[9] W.-J. H. Rop Gonggrijp, "Nedap/groenendaal es3b voting computer a security analysis." http://biobug.org/had-mirror/Es3b-en.pdf, 2006. [Online; accessed 25-March-2011].

[10] Wikipedia, "Electronic voting in estonia — wikipedia, the free encyclopedia." http://en.wikipedia.org/wiki/Electronic_voting_in_Estonia, 2011. [Online; accessed 29-January-2011].

[11] Fabian Breuer, Alexander H. Trechsel, "E-voting in the 2005 local elections in estonia." http://www.coe.int/t/dgap/democracy/activities/ggis/e-voting/evoting_documentation/PDF-FinalReportCOE_EvotingEstonia2005.pdf, 2006. [Online; accessed 29-January-2011].

[12] Ariel J.Feldman, J. Alex Halderman, Edward W. Felten, "Security analysis of the diebold accuvote-ts voting machine." http://citp.princeton.edu/pub/ts06EVT.pdf, 2006. [Online; accessed 25-March-2011].

[13] D. Frosch, "Colorado decertifies machines for voting." http://www.nytimes.com/2007/12/19/us/politics/19voting.html, 2007. [Online; accessed 26-March-2011].

[14] K. Zetter, "California bans e-vote machines." http://www.wired.com/politics/security/news/2004/04/63298, 2004. [Online; accessed 26-March-2011].

[15] E. D. R. (EDRI), "No e-voting in germany." http://www.edri.org/edri-gram/number7.5/no-evoting-germany, 2009. [Online; accessed 26-March-2011].

[16] E. D. R. (EDRI), "Electronic voting machines eliminated in the netherlands." http://www.edri.org/edrigram/number5.20/e-voting-machines-netherlands, 2007. [Online; accessed 26-March-2011].

[17] Estonian National Electoral Committee, "Internet voting in estonia." http://www.vvk.ee/voting-methods-in-estonia/engindex, 2011. [Online; accessed 26-March-2011].

[18] Estonian National Electoral Committee, "Statistics about internet voting in estonia." http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics, 2011. [Online; accessed 26-March-2011].

[19] European parliament, "Can e-voting increase electoral participation?." http://www.europarl.europa.eu/en/headlines/content/20110321STO15986/html/Can-e-voting-increase-electoral-participation, 2011. [Online; accessed 13-April-2011].

[20] Estonian National Electoral Committee, "Internet voting in estonia." http://www.vvk.ee/public/dok/Internet_Voting_in_Estonia.pdf, 2007. [Online; accessed 5-April-2011].

[21] Estonian National Electoral Committee, "Internet voting in estonia." http://porvoo9.gov.si/pdf/THU_11c_1415_Country_update_Estonia_EVoting_Porvoo9.pdf, 2006. [Online; accessed 5-April-2011].

[22] Estonian National Electoral Committee, "E-Voting System - General Overview." http://www.vvk.ee/public/dok/General_Description_E-Voting_2010.pdf, 2010. [Online; accessed 13-April-2011].

[23] Wikipedia, "Electronic voting — wikipedia, the free encyclopedia." http://en.wikipedia.org/wiki/Electronic_voting, 2011. [Online; accessed 29-January-2011].

[24] Valmyndigheten, "Röstning." http://www.val.se/det_svenska_valsystemet/rostning/index.html, 2010. [Online; accessed 26-March-2011].

[25] Kommunikationsmyndigheten PTS, "Konsumenters förhållande till internetsäkerhet." http://www.pts.se/sv/Dokument/Rapporter/Internet/2009/Konsumenters-forhallande-till-Internetsakerhet---PTS-ER-200918/, 2010. [Online; accessed 25-March-2011.

[26] Valmyndigheten, "Röstning." http://www.val.se/det_svenska_valsystemet/rostning/index.html, 2010. [Online; accessed 25-March-2011].

[27] Wikipedia, "Resultat i riksdagsvalet i sverige 2010 — wikipedia, the free encyclopedia." http://sv.wikipedia.org/wiki/Resultat_i_riksdagsvalet_i_Sverige_2010, 2010. [Online; accessed 27-March-2011].

[28] Valmyndigheten, "Förtidsrösta - val 2010." http://www.val.se/val/val2010/rostmottagning/fortidsrostning/rike/index.html, 2010. [Online; accessed 27-March-2011].

[29] S. Centralbyrån, "Antalet förstagångsväljare fortsätter att öka." http://www.scb.se/Pages/PressRelease____285869.aspx, 2010. [Online; accessed 10-April-2011].

[30] B. L. Langer, "Privacy and verifiability in electronic voting," 2010.

[31] Finansiell ID-Teknik BID AB, “Detta är bankid.” http://www.bankid.com/sv/Vad-ar-BankID/, 2011. [Online; accessed 8-April-2011].

[32] M. Jerräng, “Bankernas e-leg utmanar statens.” http://computersweden.idg.se/2.2683/1.368003/bankernas-e-leg-utmanar-statens, 2011. [Online; accessed 10-April-2011].

[33] S. Centralbyrån, “Befolkningsstatistik.” http://www.scb.se/Pages/Product____25785.aspx, 2010. [Online; accessed 10-April-2011].

[34] Valmyndigheten, “Rösterna räknas två gånger.” http://www.val.se/lattlast/Omval_2011/rosterna_raknas_tva_ganger/, 2011. [Online; accessed 13-April-2011].