KTH Computer Science
and Communication

Net Voting

Designing an Online Voting System.

Mattias Mikkola
mmikkola@kth.se
880703-0237
070-8673965

Månstorpsvägen 2
146 45 Tullinge

Joel Ahlgren
joelah@kth.se
870408-3214
070-4895526

Solbergsvägen 19
194 57 Upplands Väsby

Computer science and communications, Royal Institute of Technology, Sweden.
Degree Project in Computer Science, First Level (course DD143X)
Supervisor: Alexander Baltatzis (*alba@csc.kth.se*)

Abstract

We are currently in a time where old routines and ways are being converted to more easily accessible, digital ways. You can perform your bank errands and interact with authorities through the Internet. While many of our societies functions already have undergone this transformation, our elections are still very manual.

In our report we present what we think are the biggest obstacles to implementing a net voting system in Sweden, how to solve these issues and present a system which we feel would be a good start to designing The Ultimate Net Voting System.

We touch upon areas like authenticating voters, protecting their right to anonymous voting in sending and storing votes and ways to protect against attacks against this system. In the end, we present an abstract level of a system design which could begin to fulfill all requirements to make net voting a feasible solution.

Referat

Nätröstning – Design av ett Internet-baserat Röstningssystem.

Vi befinner oss i en tid där gamla traditioner håller på att bytas ut mot mer lättillgängliga, digitala sätt. Du kan utföra dina bankärenden och interagera med flera myndigheter via Internet. Medan många av våra samhällsfunktioner redan har genomgått denna förvandling, genomförs våra val fortfarande till stor del manuellt.

I vår rapport presenterar vi vad vi tror är de största hindren för att genomföra ett internetbaserat valsystem i Sverige, hur man kan lösa dessa frågor och presentera ett system som vi tycker skulle vara en bra början på Det Ultimata Nätröstningssystemet.

Vi berör områden som autentisiering av användare, rätten till valhemlighet vid sändning och lagring av röster och sätt att skydda mot angrepp mot systemet. Vår målsättning är med detta att få en abstrakt lösning till ett system som skulle tillgängligöra röstning via internet i Sverige.

Distribution of workload

Since this project is performed by two people we are required us to specify what parts of the project each of us have contributed to. The two following tables are rough indications to which one of us did the majority of the work on a certain area of the report. (Omitted areas are decided to be a common effort by both authors.)

Name	**Area**
Ahlgren, J	2.1, 2.3, 3.1
Mikkola, M	2.2, 3.2

Document History

Version	**Date**	**Changes**
1.0	2011-04-14	First hand-in

Contents

Chapter 1

Introduction

This report is the result of a few weeks of our research into various alternatives to the current voting mechanics used in Sweden. This work has been done as a Bachelor's Thesis in Computer Science, in the course DD143X.

1.1 Background

The election to parliament in Sweden is a massive undertaking which occurs every four years. It consumes large quantities of tax money, volunteers and other resources. A lot of these resources go to the printing and distribution of ballot papers and the administration of each polling station [16].

The turnout for the 2010 elections in Sweden was 84.63%. While this was an increase from the 81.99% of the 2006 elections [9], this still means almost every fifth swede does not vote. While you might argue that if someone can't be bothered to get themselves to a voting station they probably do not care enough to make an informed vote, a democracy still requires as high as possible participation during elections.

Aside from pure laziness there are other, legitimate, reasons for not going to a voting station. Handicap and illness are the more obvious examples, but some people might want to vote as anonymously as possible to avoid harassment or persecution.

But what about the 84.63% who actually did make their way to a polling station? Why would they want to vote in another way?

After the 2010 elections, "Valmyndigheten" received a lot complaints, substantially more than after earlier elections. [16]

1.2 Problem Statement

Facilitating voting over the Internet gives rise to critical security issues. Authentication needs to be very strong, in order to verify a users identity and make sure users can't vote more than once. Additionally, the system needs to be very resilient against Denial of Service attacks.

We want verifiability and validation of votes, but at the same time we want to protect the anonymity of the voters. This is a difficult process, and as we shall see the solutions are not always straightforward.

One method of securing identities today is a service called BankID [1], a collaborative effort between mayor banks of Sweden to create an online identification. It is currently being used by various governmental agencies, such as "The Swedish Tax Agency" (Skatteverket) and "The National Board of Student Aid" (CSN), which makes it possibly interesting for our purpose as well.

The question we've asked ourselves is, is it possible to design a system for net voting for the Swedish electoral system? Can it be done without compromising the integrity of the voters?

1.3 Limitations

Describing a system like this could encompass a massive amount of work, discussing programming language(s?) of choice, security issues, availability issues and so forth. We've decided to limit our report to the following parts:

- We will only focus on the Swedish electoral system.
- We will not do an implementation of our system.
- Our system design will be described in a very abstract way.

1.4 Glossary

A list of words, abbreviations and terms that may be unknown or unfamiliar to the reader or used by us in ambiguous ways.

Term	Definition
Certificate	A Digital Certificate binds a public key to an identity. It is a way to assert that a key belongs to a certain individual or organization, as long as the Certificate Authority that issued the Certificate can be trusted.
County council	The Swedish "Landsting", ranks between parliament and municipalities.
(Distributed-)Denial-of-Service attack	An attack where one or many computers continuously send requests to a server in order to make it inaccessible.
eID	An abbreviation for Electronic Identification, meaning a ways of confirming a persons identity digitally.
Election	In this report mostly used to denote an occasion where citizens can cast a legally binding vote.
Election Authority	An organization separate from the government, charged with administering elections in Sweden, to allow a degree of transparency in the democratic process. In Swedish: "Valmyndigheten".
Electoral register	A list of people who are eligible to cast a vote in a specified election.
eVoting	A shortened version of "Electronic Voting", can mean either voting via the Internet or just an election where ballot papers to some extent are replaced with electronic voting systems.
HTTPS & SSL	HTTPS refers to the secure HTTP protocol, which is regular HTTP over a connection secured by SSL or TSL
Key	Used in this report to denote a digital key, used in cryptographic operations.
Man-in-the-middle attack	An attack where the attacker places himself between to victim and the victim's intended target in order to intercept information.
Polling station	A facility in which voters can cast their vote.
Signature	A Signature refers to a digital signature. It is a method of validating authenticity of data. By encrypting a hash of the data we want to transmit with our private key, anyone can match the decrypted hash to their own hash of the data. This assumes we trust the public key.

Chapter 2

Research

One of the two big aspects of our work is to find information to base our assumptions and discussion on. We looked into three areas: "The Swedish Electoral System", "Aspects of a Net Voting System Design" and "Previous and Current Implementations".

2.1 The Swedish Electoral System

The first thing we needed to find out was how the Swedish electoral system works, in order to determine the prerequisites for our solution.

The Swedish elections are governed by the Swedish electoral law [10]. It states when elections are to be held, who is qualified to vote (electoral register), what forms of voting is available and much more.

All elections in Sweden are to be held on a Sunday, where parliament elections, county council elections and municipal council elections are to be held on the second Sunday of September every fourth year.

Each municipality is divided into election districts of between 1000–2000 voters each. Each municipality is obligated to ensure there is at least one polling station per district, according to the Swedish electoral law chapter 4, §20.

2.1.1 Methods of voting

While the elections occur on the second Sunday of September, it is possible to cast your vote in advance [6]. This is possible from 18 days before the election day up to the election day, at certain polling stations selected by each municipality.

Another possibility is to vote by courier [7], but this is reserved for people with special needs and disabilities. The vote can be prepared at earliest 24 days before the election day and handed in at latest on the election day.

It is also possible to vote from abroad, either from a Swedish embassy or consulate [3] earliest from 24 days before election day up until a date set by that embassy

(to make sure votes get to Sweden in time) or by mail [5] (which can be sent no earlier than 45 days before and must arrive at latest the day after the election day).

2.1.2 Voting in practice

There is a certain procedure when casting your vote in a polling station, either voting in advance or on the election day), stated in the Swedish electoral law [10], chapters 9 and 10.

Upon entering the polling station, the voter picks up a number of ballot papers and one to three envelopes, depending on which elections (parliament, county and/or municipal) they wish to participate in. They then take these behind a screen and put their selected ballot papers in the envelopes and seal them. After discarding any left over ballot papers, they present the envelopes, their voting card and ID to the vote collectors, who check them off in the voting registry and deposit the envelopes in sealed boxes, to be collected and counted later.

2.1.3 Counting the votes

When the polling stations close at the end of the election day, the counting of the received votes begins. Each individual voting district counts their received votes and then report their results to the Electoral Authority.

The allocation of mandates in parliament from the number of votes each party receives is out of the scope of this report and will not be looked into further.

2.2 Aspects of a Net Voting System Design

2.2.1 Requirements

Any voting system requires at least the same level of security as the current implementation. The aspects of the current Swedish voting systems that need to be considered are:

- How do we confirm the identity of the person voting?
- How do we make sure the vote is cast correctly?
- How do we provide anonymity for the voter?
- How do we prevent ballot rigging?

All of these are addressed in some way in the current system in use by Swedish authorities, we confirm identity by requiring the votee to present identification papers of some kind, a visual inspection of the envelope containing the ballot is made possible through a small slit, anonymity is secured since the ballot is turned in separately from the identification check, and the storing of ballots until the election is finalized assures we can always recount the ballots.

2.2.2 Asserting Identity

Because there is no physical identity check, the system needs to assert whether or not the user voting can be identified as the owner of that vote.

Currently Available Systems

BankID BankID is the most popular way of asserting identity online in Sweden today[8]. BankID uses a Public Key Infrastructure (PKI), and BankID itself acts as the Certificate Authority (CA). The Banks which offer BankID to their customers acts as a Registration Authority, creating a users identify certificate. BankID then signs this key with their own CA key, effectively vouching for the identity of that user. A service provider that then wants to verify the identity of a user then installs a module provided by BankID, which verifies that the user's identity certificate was indeed signed by BankID.[2]

Other Electronic ID Services The Swedish bank Nordea, as well as the telephone company Telia, also offer a service similar to BankID. They use PKI as well, but the same organization is both the CA and the RA.

Open Solutions OpenPGP is a public-key cryptography standard, implemented in various software such as PGP from PGP inc and GnuPG from the GNU project. It has gained widespread use for email encryption, and uses a model similar to BankID and Nordea e-leg. PGP relies on a web of trust. This means that, if I trust Bob's identity certificate, then I can trust other people who's identity certificates have been signed by Bob. So if we just trust certificates signed by a trusted CA, we effectively have a PKI with PGP encryption.

2.2.3 Sending and Storing Information

The subject of storing information is a sensitive one. We need to know who has voted, and what party they voted for, without being able to link the two together. This becomes particularly tricky when it comes to how the information is sent, because we need to send both the identity of the voter, and what party / candidate they voted for. There is no solution here that does not require a level of trust from the voter.

Avoiding eavesdropping

The HTTPS protocol ensures reasonable protection against eavesdropping and man-in-the-middle attacks. The underlying SSL protocol effectively negates eavesdropping by the use of Diffie-Hellman Key Exchange.[14] The exchange is secured from man-in-the-middle attacks by the usage of certificate identities. As long as the user can trust the CA for the certificate, a reliable connection can be made.

2.2.4 Possible Attack Vectors

An attacker looking to exploit the system would have one of several motives. A simple example would be to manipulate the voting process, giving a party more votes than it actually received. Coercion is also a factor, a group of people might threaten other individuals to vote in a certain way. They could also try to get them to sell their votes. Or the attackers might simply want a list of people who voted for a certain party for intelligence reasons (similiarily to how Informationsbyrån kept records of members of extremist organisations in the 70's).

Protecting individual votes

For individual voters, the most pressing issue might be securing the secrecy of their vote. This is indeed absolutely required in a democratic system, since it eliminates threats against voters (There is no way to verify Bob voted for Party A, so why threaten him to vote for Party A?).

As previously discussed, this is a challenge with a remote voting system. If we need to assert the identity of the voter remotely, as well as his choice of vote, how can we possibly guarantee that his vote will remain anonymous? We can make the system secure from outside manipulation, but voting remotely by any means will always require a certain degree of trust in the system.

There is a good analogy to this, and that is the postal vote. Swedes who are abroad and otherwise can not make it to a Swedish embassy or consulate have the option to vote by mail. When doing this a set of 4 envelopes and three ballot papers are ordered from a embassy or consulate in advance. When voting, the voter writes down his choices on the ballot paper and puts each ballot inside a envelope, just like at the polling station. These three envelopes are then put into a larger envelope, which is signed by the voter and two witnesses. The envelope is then sent off to the voters polling station, where it is received, the voter is ticked off in the electoral register and the smaller envelopes are put into the ballot box with all the local votes. Even this postal system requires a degree of trust by the voter, since there is no way for him to confirm that his vote has actually been cast. A corrupt official at the ballot station could check the ballot, then replace them with new ballot papers and envelopes.

There are additional security issues here. Because the propsed system allows users to vote from any computer, it is impossible for us to guarantee that those computers are secured. It remains to the user to confirm that no malicious software is present on the system being used to cast the vote. For example, an attacker could have remotely installed software that allows him to view the screen of that system, this way it is possible to see what the user will vote, if the attacker is viewing the screen at that particular moment.

Ballot Rigging

The most critical part of the voting system is the counting of the votes. If the results are tampered with, the entire election is rendered invalid. There are many ways to tackle this threat. It would seem a combination of preventive protective measures and some sort of validity check afterwards would be the best approach.

Preventive The first defense should be to hinder the tampering from being made in the first place. Limiting the access to the server(s) recording votes and voters to only accept incoming votes from the interface specified by the design. The administration of these servers should be heavily monitored, and only accessible from one specified terminal placed in a protected and controlled environment.

The servers in the Estonian implementation of net voting are placed in a locked room which is controlled by two separate organizations. Whenever anyone accesses these servers, their interaction is recorded and videotaped to ensure nothing is tampered with. The votes are stored in an encrypted format and are decrypted just before being sent for counting, using a secure hardware module, accessible only with several physical keys held by various members of the Estonian National Election Committee.[11]

Validity The absolutely simplest way to check if the results have been tampered with is to check that the number of cast votes matches to the number of registered voters.

A more in-depth solution would be to implement an audit function of some sort, without sacrificing voter anonymity.

The Estonian voting system implements some sort of auditing system but we've so far been unable to find any information about their inner workings, only general descriptions[4].

Denial of Service

It is important that the system is protected against Denial of Service attacks, or users will not be able to vote at all. Most of the system should be in a secure network, only the servers requiring direct communication with the user should allow incoming connections from outside the secured network. So any DoS attacks will most likely be directed at this/these servers, and as much as possible should be done to try and prevent possible attacks. Server configurations should be checked thourougly, and communications should only be allowed on necessary ports.

2.3 Previous and Current Implementations

The concept of net voting or electronic voting is not new. There are countries which have tried to implement a net voting system and failed, there are those who have implemented systems that are currently in use and there are countries that have

gone halfway and exchanged ballot papers for electronic voting machines. Here we present some of these, which we feel have important lessons for us in implementing our system.

2.3.1 eVoting at polling stations

This is a fairly common occurrence India, Brazil, Venezuela and USA where you exchange the ballot papers and envelopes with a specialized voting machine. This system still requires the voter to visit a polling station, but alleviates much of the work associated with collecting and counting the cast votes.

It has also been used in the Netherlands, but after a group of concerned citizens calling themselves "Wij vertrouwen stemcomputers niet" ("We do not trust voting computers") exposed critical security flaws in the voting machines[15], the government decided to go back to the old system of ballot papers.[17]

2.3.2 Remote eVoting

Taking the concept of eVoting to it's full potential, there are countries which have implemented and used electronic voting over the Internet. These have been used in elections of varying sizes, from referendums to parliamentary elections.

Estonia

One of the more successful systems is the one used in Estonia. The legal groundwork for allowing voting over the Internet in Estonia was made in 2002, and even though some required amendments where protested by the president, the first legally binding, national election with Internet voting was held in October 2005. It was estimated that 80% of the eligible voters had all prerequisites to vote via the Internet, and that roughly 1% (around 9.200) used it.[13;18]

While this might seem like a fairly small amount of votes, it is important to remember that introducing new ways to vote will be met with some resistance at first, before the method becomes generally trusted.

The system is still in use, and was last used in the 2011 parliamentary elections, where 145.230 votes were cast via Internet (of which 96% were cast from voters within Estonia and the other 4% by citizens abroad).[19]

This seems to indicate that people will gradually accept and trust a new way of voting.

Something worth noting is that Estonia has a very extensive saturation of eID in the population, as the national ID card contains a chip which enables digital identity assurance.[18] This has enabled their net voting system to be integrated into their electoral system without too much friction.

Chapter 3

Design

3.1 Front-end

We won't immerse ourselves too much with the front-end solution of this system, other than state what our back-end system will require from the front-end.

We see two different front-ends required: one for the completely remote voting and one for those who don't want or have the ability to acquire the required authentication to use the remote voting interface.

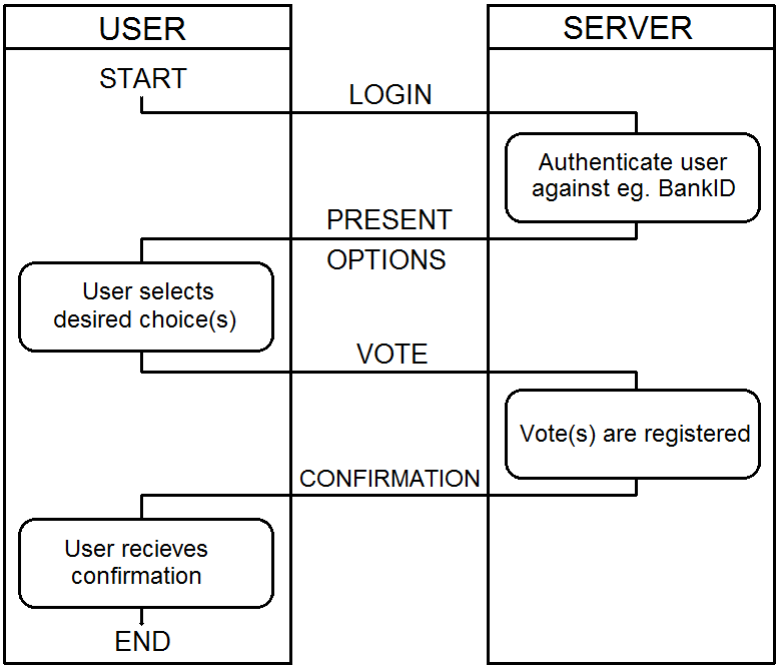

Figure 3.1. Example flow of events during a vote, from the users point of view.

Remote voting

The primary interface for our system would ideally be the one accessible from anywhere in the world. Other available authority services utilize web based interfaces, and it would make it easier to guarantee maximized platform support. The general flow of this interaction is depicted in figure 3.1.

This interface would utilize an eID service to authorize voters and provide them with the interface to cast their vote(s).

Net Voting at the Polling Station

For those who for some reason don't have an eID, a computer in the polling station would provide them with the possibility to cast a net vote anyway.

This interface would need an alternate way of authenticating a voter, provided by the staff at the polling station. Some kind of generated code which allows them to vote once, and have them checked in the voting registry.

We leave this part outside of our design, as it is of little relevance to our work at this time.

3.2 Back-end

We designed our back-end to counter-act the security and secrecy issues discovered in Chapter 2. This section will discuss a simple implementation of a system designed with these issues in mind.

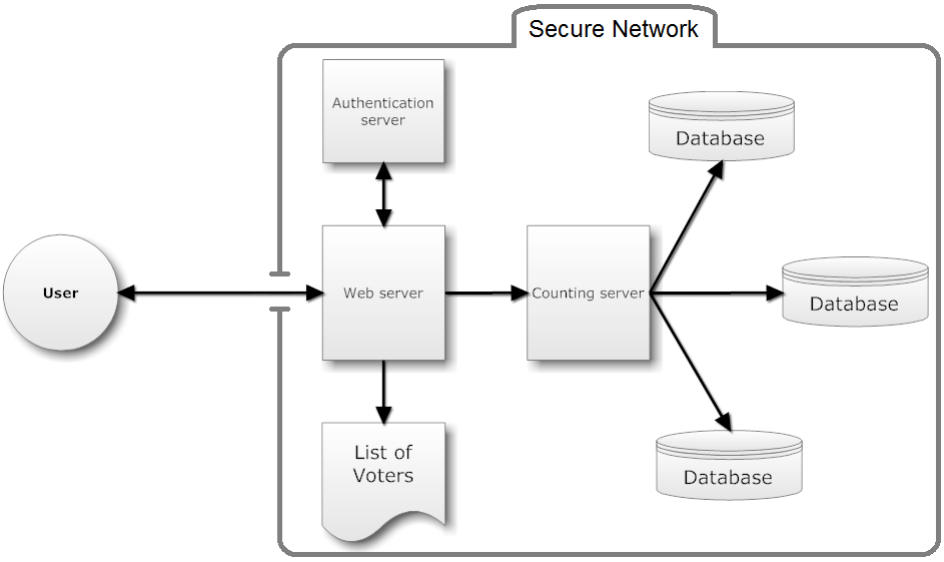

Figure 3.2. A general overview of the system. The various parts are described in the following subsections.

3.2.1 Web Server

The web server will provide the service to the user, it acts as the only point of communication between the user and the system. When a user logs on, he will authenticate himself and be presented with a list of options of how to vote. The user will then use a system analogous to the postal vote system discussed in 2.2.3. The user first chooses his vote on the ballot. The ballot is then encrypted using the counting servers' public key, this ensures that the web server will not be able to see the ballot. This package is then encrypted again, with the web server's public key, and then signed with the users private key from BankID or a similar system. This layered encryption scheme is why we refer to the system as an onion.

The server then receives this package, checks the signature to assert the identity of the user, then decrypts the package, revealing the inner encrypted ballot. The voter's identity is then sent off to the voter list server, and the encrypted ballot is sent off to the counting server.

3.2.2 Voter list

The voter list server is a simple list of all eligible voters, and once a user has voted his name is ticked on the list. This is to make sure that a user can not vote twice.

3.2.3 Authentication Server

The Authentication Server verifies the identity by checking that the signature on the package is legit. It does not serve any other purpose and several authentication servers will need to be used if the system is going to support more authentication methods like Nordea E-legitimation.

3.2.4 Counting Server

The counting server has access to a private key that decrypts the ballots. It receives a ballot, with no information about the voter, decrypts it, checks the vote and adds it to a number of database servers. The counting server should log votes it has received.

3.2.5 Database servers

The databases simply store the number of votes. They need to be physically secure, as well as not allow any communication with hosts other than the Counting Server. Certificate Identities should be used to ensure that the Counting Server has not been swapped for a malicious host. Logging should be enforced on all database servers.

3.2.6 Tallying the results

When voting has ended the system stops all communication with the Internet completely. The Database servers are checked for consistency (They should all have the same results), and the number of votes are checked towards the Counting Server log and the voter list (The number of votes should not differ).

3.3 Assumptions

Our design makes a number of assumptions:

Assumption	**Motivation**
All server-to-server communication is on a secure network.	Communication with Internet is unnecessary.
User is not able to make an invalid vote.	This should not happen with normal usage of a web application.

Chapter 4

Discussion and Conclusion

4.1 Discussion

From the design described in chapter 3, there are still some concerns we'd like to emphasize.

4.1.1 Ethical and Social Limitations

This is where the biggest concerns lie. The most important obstacle to implement a net voting system is to get the citizens of the democracy to accept it as a viable and trustworthy alternative to the current systems in place.

4.1.2 Technical Limitations

The net voting system cannot be implemented as a replacement for the current system, as there is no guarantee that 100% of the population has access to a computer with Internet and has an eID.

The real balance act of this system is to provide sufficient levels of auditing (verify that each vote was cast by an eligible person and that the vote recorded is the same as the voter cast) and to protect the voters right of voting confidentiality.

Our system does not validate votes outside of checking that the voter is eligible to vote. This is because the ballot in itself is anonymous and encrypted, and once we decrypt it to validate it we have lost the information about whose vote it is. To get around this problem one would need to use a Zero-Knowledge Proof, that is to somehow validate the vote without actually opening up the encrypted package. Such a system was described by Md. Abdul Based and Stig Fr. Mjølsnes in 2009. [12]

We feel that the system we've described in chapter 3 makes a good weigh-off for both aspects, but it is also an unsolvable problem to fully satisfy both sides. It works as long as the user trusts the system and the organization behind it, but the same is true for any voting system.

4.1.3 Transparency of the System

To gain the biggest trust possible, and to ensure that the system is as flawless as possible, we'd like the implementer of to consider the idea of releasing parts of or the whole source code to the public, to allow people to understand the inner workings of the system and find flaws missed by the developers.

We understand that this also presents a possible danger in itself, if someone finds a security flaw and takes advantage of it instead of reporting it. We do however believe that enough skilled people will be interested in scrutinizing the code that for every evil-doer there's at least two people with honest intentions. A monetary reward for finding a flaw could also be considered.

4.1.4 Vulnerability

The most vulnerable point in the system is the counting server, both the private key to decrypt votes and the software within it are a critical point in the system. Someone with access to the server could potentially make changes to the software to replace votes. We can verify that the right number of votes exist due to the log from the authentication server, but we cannot verify that a vote was not manipulated in the counting server.

4.2 Conclusion

In the end, we feel that from a purely technical standpoint, the only thing stopping Sweden from implementing a net voting system today is the lack of a standardized national eID (like Estonia does).

The biggest obstacle is the lack of trust from the general population. While many Swedes claim to want the possibility to vote over the Internet, in the end, many still don't trust it to the same extent that they trust the tested and true voting system with paper ballots and polling stations.

Bibliography

[1] Bankid. Website. URL http://www.bankid.com/.

[2] Bankid: Delivering bank-common trust for web-based transactions. Website. URL http://www.infosec.co.uk/ExhibitorLibrary/168/Cybertrust_CS_BBS_1.pdf.

[3] Rösta på ambassad eller konsulat. Website. URL http://www.val.se/det_svenska_valsystemet/rostning/rosta_ambassad/index.html.

[4] E-voting system – general overview. Technical report. URL http://www.vvk.ee/public/dok/General_Description_E-Voting_2010.pdf.

[5] Brevrösta från utlandet. Website. URL http://www.val.se/det_svenska_valsystemet/rostning/brevrosta/index.html.

[6] Förtidsrösta i sverige. Website. URL http://www.val.se/det_svenska_valsystemet/rostning/fortidsrosta/index.html.

[7] Rösta med bud. Website. URL http://www.val.se/det_svenska_valsystemet/rostning/budrosta/index.html.

[8] Bankid är den lösning som används av flest. Website. URL http://www.bankid.com/Documents/wwwbankidcom/Diagram%20nr%201.pdf.

[9] 2010 allmänna val – sammanfattning. Website, . URL http://www.val.se/tidigare_val/val2010/index.html.

[10] Vallag (2005:837). Website, . URL http://www.notisum.se/rnp/sls/lag/20050837.htm.

[11] R. Michael Alvarez, Thad E. Hall, and Alexander H. Trechsel. Internet voting in comparative perspective: The case of estonia. *PS: Political Science & Politics*, 42(03):497–505, 2009. doi: 10.1017/S1049096509090787. URL http://dx.doi.org/10.1017/S1049096509090787.

[12] Md. Abdul Based and Stig Fr. Mjølsnes. A non-interactive zero knowledge proof protocol in an internet voting scheme. In *The Norwegian Information Security Conference (NISK) 2009*, 2009.

[13] Anne Borache. Estona pulls off nationwide net voting. *CNET News*. URL http://news.cnet.com/Estonia-pulls-off-nationwide-Net-voting/2100-1028_3-5898115.html.

[14] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246 (Proposed Standard), August 2008. URL http://www.ietf.org/rfc/rfc5246.txt. Updated by RFCs 5746, 5878, 6176.

[15] Rop Gonggrijp, Willem-Jan Hengevald, Andreas Bogk, Dirk Engling, Hannes Mehnert, Frank Rieger, Pascal Scheffers, and Barry Wels. Nedap/groenendaal es3b voting computer – a security analysis. Technical report. URL http://www.wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf.

[16] Kristina Lemon. Erfaranheter från valen den 19 september 2010. Technical report, Valmyndigheten, 2011.

[17] Jan Libbenga. Dutch pull the plug on e-voting. *The Register*, October 2007. URL http://www.theregister.co.uk/2007/10/01/dutch_pull_plug_on_evoting/.

[18] Tarvi Martens. Internet voting in estonia. Technical report. URL http://porvoo9.gov.si/pdf/THU_11c_1415_Country_update_Estonia_EVoting_Porvoo9.pdf.

[19] Martin Šmutov. E-valijaid oli 106st välisriigist. *Postimees*. URL http://poliitika.postimees.ee/?id=396780.