KTH Computer Science
and Communication

Proposal for a Swedish remote electronic voting system

2012/05/20

VIKTOR COLLIN 880316-0277, VCOLLIN@KTH.SE,
HAMPUS OHLSSON 880328-0356, HAMOHL@KTH.SE

Bachelor's Thesis at CSC
Supervisor: Mikael Goldman
Examiner: Mårten Björkman/Mads Dam

This page is intentionally left blank.

Abstract

Electronic voting is an extensive topic related to many difficult issues. It is hard to fulfil all desired characteristics and security requirements, which is demonstrated by the lack of systems in use today. More and more services are moving online to the digital sphere, but the general election in Sweden is still a manual and costly process. With the growing demand and popularity of online services today, an electronic voting system might be a necessity to maintain voter turnout in the future. In this report we investigate how to model a reliable and trustworthy remote electronic voting system for use in Sweden, so that a vote is submitted in the safest manner possible while maintaining confidentiality and verifiability through the entire chain. It is based on the "Scratch, Click & Vote" scheme published by Kutylowski and Zagórski (2010), but with some modifications to better suit the Swedish electoral system. The system is built upon distribution of knowledge and responsibility between two different parts, a Proxy and an Election Authority (EA). It aims to fulfil all security requirements desirable from a remote electronic voting system while protecting the secrecy and integrity of the ballot.

Sammanfattning

Elektronisk röstning är ett utbrett ämne sammankopplat med en rad svårigheter och utmaningar. Det är svårt att uppfylla alla önskvärda egenskaper och säkerhetskrav, vilket kan demonstreras av bristen på elektroniska röstningssystem som används idag. Fler och fler tjänster har senaste tiden digitaliserats, men valprocessen i Sverige är fortfarande en manuell och kostsam procedur. Med den ökade efterfrågan och populariteten av digitala tjänster, är det möjligt att röstning över internet kommer vara nödvändigt för att bibehålla valdeltagandet i framtiden. I denna rapport undersöks hur ett tillförlitligt och trovärdigt nätbaserat röstningssystem kan utformas för användande i svenska val. En röst ska läggas på säkrast möjliga sätt samtidigt som integriteten bevaras och processen ska kunna verifieras genom hela kedjan. Resultatet är ett system baserat på "Scratch, Click & Vote"-systemet publicerat av Kutylowski and Zagórski (2010), men med modifikationer för att bättre passa det svensk systemet. Systemet bygger på fördelning av vetskap och ansvar mellan två olika parter, ett ombud och en Valmyndighet. Alla säkerhetskrav önskvärda av ett elektroniskt röstningssystem uppfylls av systemet, samtidigt som valhemligheten och integriteten bibehålls.

Statement of collaboration

Part	Viktor	Hampus
1. Introduction		x
2.1 The Swedish electoral system	x	
2.2 Features of a Net Voting System		x
2.3.1. I-Voting in Estonia	x	
2.3.2. Scratch, Click & Vote	x	x
3.1 Identifying require ments	x	
3.2 Review of literature	x	x
3.3 Benefits and concerns with SC&V	x	
3.4 Method criticism		x
4 System Design	x	x
5.1 Usability concerns	x	
5.2 Security concerns	x	x
5.3 Preventing double votes	x	
5.4 Conclusions		x

Table 1: Distribution of workload between the authors

Table of Contents

Chapter 1

Introduction

In today's technology-infused society, it is possible to press a "Like" button on virtually everyone and everything with a digital presence. More and more services are moving online to the digital sphere, but the general election in Sweden is still a manual and costly process (Bränström, 2010). With the current pace of services going digital and technological progress, realistically we also need to switch over to electronic voting at some point. In Sweden, approximately 88 % of the population has access to the Internet, out of which nine out of ten can access it at home. It is fair to state the Internet usage in Sweden is widely spread amongst all ages; of all individuals above the age of 75, one third states they occasionally use the Internet (Findah, 2011). A large majority of the population daily uses the Internet to perform security sensitive tasks such as financial transactions and similar services, and therefore it should be no great adjustment to also acclimatize to electronic voting. There are generally two main scenarios when it comes to electronic voting:

- Electronic voting at polling places, using Direct-Recording Electronic (DRE) voting machines or similar equipment. Representatives of governmental or independent electoral authorities physically supervise the procedure.

- Remote electronic voting via the Internet, is performed within the voter's sole influence and not physically supervised by any governmental representatives or restricted to any specific location or hardware.

This report will focus on the latter – remote electronic voting using the Internet. With the growing demand and popularity of online services, it might be an inevitable scenario and a possible necessity to maintain (or increase) voter turnout in the future.

1.1 Problem statement

The purpose of this report is to investigate how to model a reliable and trustworthy remote electronic voting system for use in Sweden, so that a vote is submitted in the safest manner possible while maintaining confidentiality and verifiability through the entire chain.

1.2 Limitations

The report will be constrained to theoretically presenting a design proposal for a remote electronic voting system, and how it could be integrated in the Swedish society. The following limitations are present:

- Only focus on *remote* electronic voting systems; the report will not cover electronic voting in polling stations.
- Propose a system that would be possible to use as a *complement* to the current Swedish electoral system.
- Scalability and performance of the system will not be covered.
- Assuming all eligible voters have a way of identifying themselves over the Internet, such as e-authentication.

1.3 Terminology

Blind signature A blind signature is a type of digital signature where the content is disguised before it is signed. A third party can later verify the signature and see that the content has not been changed.

Commitment scheme Commitment schemes are often important parts of cryptographic protocols, and allow one party to commit to a value while keeping it hidden. They can later reveal the committed value.

DRE DRE stands for Direct-Recording Electronic voting machine or voting system. In both cases, and as the name suggests, it is an electronic device where a person directly enters a vote through (usually) a touchscreen interface. The vote is then recorded electronically**.**

DDoS DDoS stands for Distributed Denial-of-Service, and is a common attack for bringing down systems, in particular web servers.

E2E verifiability End-to-end verifiability. An electronic voting system can be E2E verifiable, which certifies rigid security properties.

Electoral register The list of eligible voters used by the election officials at polling stations to mark the voters that have particiapted.

RSA RSA is a widely used algorithm for public/private-key encryption.

Chapter 2

Method

2.1 Identifying requirements

To be able to design an optimal remote electronic voting system, all system requirements had to be identified. To get a brief overview and introduction to the subject an interview was conducted with Douglas Wikström, Assistant Professor in cryptography at the Royal Institute of Technology, Sweden. He is currently researching cryptographic protocols, with a main interest in electronic elections. In the interview he stressed the importance of verifiability through the entire chain (E2E), and also described a flaw in the current paper-based system in Sweden. Furthermore an electronic voting system needs to follow the rules and prerequisites of the current Swedish electoral system. See section 3.2.1

2.2 Review of literature

The subject of electronic voting is very broad and a lot of previous research exists in the field. We came across the book "Towards Trustworthy Elections" that was published 2010, which is a collection of the most recent research available on electronic voting in the area of security and cryptography. The publications in the book has been of great value; it has been the main source of information and inspiration. Since it is a collection of scientific reports written and edited by many different researchers (R. Rivest among others) from all over the world, it is considered to be a reliable source.

The general attitude in all publications found, is that electronic voting and in particular remote electronic voting, is still associated with a lot of secrecy issues and concerns. Electronic voting is like a "black box"; no one can have any knowledge of the inner workings of the machinery, or at least not have control of all the information. Many attempts and system design proposals have been made, but no ultimate solution has been found.

2.3 Method criticism

The research done in the field of electronic voting is extensive, and it is definitely challenging to cover all aspect within the short timeframe of this course. Consequently we have been selective in our collection of data, and possibly overlooked important information and sources. Furthermore, we are novices on the topics of cryptography and elections, which may have impacted our results.

Chapter 3

Background

3.1 The Swedish electoral system

The general election in Sweden is an inefficient and costly procedure that is held every fourth year, with an approximate cost of 458 million SEK (Bränström, 2010). A significant proportion of this budget goes to keeping polling stations opened and staffed during the polling period, also printing ballot papers and putting them in place. In addition, there is a cost to print and distribute seven million voting cards to all eligible Swedish voters.

During the polling time frame, each eligible voter has to attend a polling station and mark his or her choice on a ballot paper. Their identity is confirmed by verification against a pre-printed list. There are three types of ballot cards – blank, party and party with candidates. As the ballot cards suggest, all eligible voters can vote for a specific party, but also vote for someone within that party. Sometimes the list of candidates consists of up to 76 names (Valmyndigheten, 2010a). If such a ballot is chosen, a voter must only vote for one candidate. The initial vote counting is completed the same night polling closes, and recounted the next day when the premature votes also are included.

A security flaw

In the current Swedish system there is a way for an attacker to examine that someone they coerced has voted in a certain way. For accessibility purposes, the system allows vote ballots with multiple chosen candidates. For example, if a voter due to misunderstanding, shaky hands or any other reason marks more than one candidate, none of the marks will be counted, but the vote is still a valid vote on the party. These votes will be separated in the tallying process and placed in a special pile Valmyndigheten (2010b).

Since the tallying process is open for public audience, this opens up the possibility for an attacker to coerce someone to mark a unique or uncommon pattern on the vote ballot. By monitoring that the pattern appears in the pile of vote ballots, the attacker can verify that the voter voted as expected.

This is a known system flaw, but the choice is made by the lawmakers to disregard it. To practice this on a large scale it would require a lot of manpower, and even in that case, the probability to change the overall result of the election is marginal.

3.2 Features of a Net Voting System

3.2.1 System requirements

In this section, the essential requirements that a proper electronic voting system should satisfy are briefly described:

- Only accept votes from eligible voters (proper user authentication).
- Prevent voters from casting multiple votes.
- Maintain secrecy of the ballot – there should be no way for any voter to prove how they voted.
- Maintain integrity of the ballot – including protection against malware and software threats.
- Not allow a placed vote to be changed, duplicated or deleted. The tally must be accurate.
- Be available for use during the entire election timeframe, including robust protection against DDoS-attacks and similar threats.
- The system should be auditable/verifiable through the entire chain, from placing a vote to election result.
- Easy to use with good accessibility for disabled voters.

3.2.2 User authentication

Participating in elections is regarded as one of the most effective methods for individuals to express their opinion, and one of the reasons why the right to vote is a cornerstone of democracy. To make sure each participating voter in an election only places one vote, identity verification is very important.

In the current paper-based elections in Sweden, the officials in the polling station mark each voter's name off a list when they cast their vote. In the case of voting by mail in advance, a voter can replace his or her vote if another vote is placed at the polling station during the Election Day. In remote electronic voting systems this introduces a concern: a voter has to verify their identity and be able to replace their votes, but a vote cast must never be linkable to a specific person.

In Sweden there are a couple of ways of electronically verifying the identity of a person, which will be described below.

E-authentication

In Sweden there are three e-authentication system distributors, BankID (a collaboration between several large banks), Telia (through SEB and ICA Banken) and Nordea. Both SEB and Nordea are starting to migrate towards BankID. The three distributors have agreed to follow a framework set by the Swedish Administrative Services Agency. According to Logica (2011), in October 2011 4.4 million people, or almost 60 % of the population over 18 had access to a valid e-authentication system, and the numbers have been steadily increasing over the last years.

Other solutions

All major banks in Sweden have some solution for customers to use Internet to do financial transactions (online banking) it often includes login with the help of a authentication token device. First quarter of 2011 78 % of the population between 16 and 74 used online banking (SCB, 2011).

3.2.3 Challenges

While electronic voting is great in certain aspects such as convenience and possibly increased voter turnout, it is also associated with a lot of issues.

End-to-end (E2E) verifiability

It is of great importance for an electronic voting system to be end-to-end verifiable, since such a system certifies important security features. By just ensuring two key properties, voter auditing and universal verifiability, the entire path from voting attempt to election totals is covered. Voter auditing implies that any voter should be able to verify that their vote is correctly included in the ballot. With universal verifiability any voter may determine that all of the votes have been correctly counted.

Secrecy of the ballot

One of the major problems with electronic voting is maintaining the election integrity and the secrecy of the vote; no voter should be able to demonstrate how he or she voted to any third party to prevent vote selling and similar activities. Another challenge lies in guaranteeing that someone in a position of power over the voter isn’t watching over their shoulder, with a gun (figuratively or even literally) to make sure they vote the “right” way. Making sure that a voter’s vote is private and personal is one of the key things accomplished with polling places; nobody watches anybody else while voting. For obvious reasons, this is hard to achieve in a remote environment.

Integrity of the ballot (the secure platform problem)

The secure platform problem is a fundamental problem one must face when trying to design a remote electronic voting system, which essentially is that client platforms are vulnerable to malicious software (viruses, Trojan horses, etc. . .) and thus cannot be trusted. Ronald Rivest, recognized cryptographer and the “R” in “RSA”, states that cryptography is not the problem when it comes to remote electronic voting. In fact, many solid cryptographic voting protocols have been proposed, but the main problem is presenting the cryptography to the voter (Rivest, 2001b).

To better illustrate the secure platform problem, Rivest talks about the “Alice abstraction” (Rivest, 2001a). Almost all suggested cryptographic voting protocols assume that a voter (Alice) has a secure platform (e.g. a computer), which reliably and correctly will perform its part of the protocol. Furthermore, Alice can generate a secret key SK_A that she uses as her electronic identity and her way of identifying herself. As far as the cryptographic voting protocols are concerned, the platform is Alice.

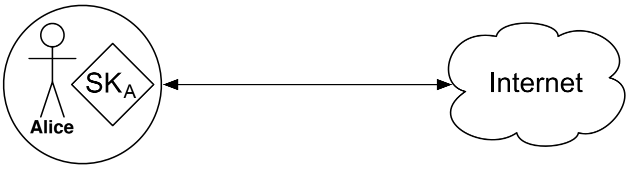


Figure 3.1: Cryptography in theory

The problem is that Alice is not a computer. Alice needs a computer to store her secret key SK_A and trust that the platform faithfully and correctly will perform computations on her behalf. In the case of voting, Alice needs to be 100 % sure that her computer displays the intended vote, and then submits it correctly and cryptographically according to the protocol in use. Unfortunately it is hard to accomplish this in the real world.

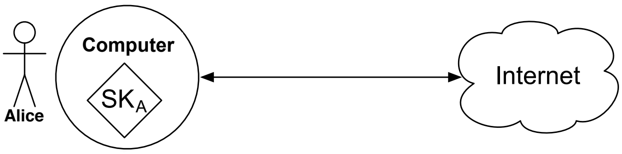


Figure 3.2: Cryptography in practise

In reality, most computers today are far too vulnerable to viruses and other forms of malicious software. If an operating system allows a third-party program to run, it can theoretically also run a virus. A mischievous attacker could easily make a virus that would cause a voter’s computer to display one candidate while actually voting for another. If a substantial amount of computers would be infected with similar malware, an election could be rigged – which is an unacceptable risk (Rivest, 2001b).

3.3 Current implementations and system proposals

During the last few years there have been many proposals of different E2E voting systems, some of the most recognized include Prêt à Voter, Punchscan and ThreeBallot (Kutylowski and Zagórski, 2010). These present some interesting ideas, but are dedicated to electronic elections in polling places and will therefore not be discussed any further in this report. Up until recently no voting schemes proposed by the academic community have fulfilled all the security requirements of remote voting. In particular, almost all schemes ignore the secure platform problem described above.

3.3.1 I-Voting in Estonia

There are however some systems in use, even though they do not satisfy all requirements. As world wide pioneers, Estonia started to use a system called I-Vote in 2005 for use in their general elections. Since then it has been used a total of five times. With the use of digital envelopes, the system mimics the physical dual envelope system used e.g. in Sweden for the premature postal votes. Firstly, the system encrypts the actual vote which is similar to sealing the inner envelope. Then the vote is digitally signed and put in an outer envelope containing the personal information about the voter. When the votes are counted, the outer envelope is discarded and only the vote information remains with no information about the voter. Votes can be placed multiple times during a certain timeframe until a couple of days before the Election Day, when the system closes and only the last registered vote will be used. If the voter also votes at a polling station, the digital vote will be discarded.

In 2005 I-Vote system was used for local elections in Estonia and made up for 1.9 % of the votes counted. In the parliamentary election 2011 the corresponding number was 24.3 %. The overall turnout in the local election increased from 47.4 % in 2005 to 60.6 % in 2007. For the parliamentary election the turnout was 61.9 % in 2007 and 63.5 % in 2011 (VVK, 2011).

3.3.2 Scratch, Click & Vote

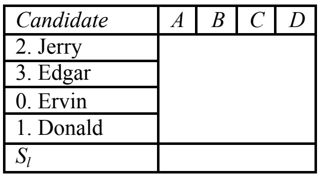
Recently, a scheme for remote electronic voting called "Scratch, Click & Vote" (referenced as SC&V below) was published by Kutylowski and Zagórski (2010). The SC&V system is based on Prêt à Voter, Punchscan and ThreeBallot, and claims to be E2E verifiable, as well as providing guaranteed security against malicious hardware and software used by a voter. The system is built upon distribution of knowledge and responsibility between two different parts, a *Proxy* and an *Election Authority (EA)*. There can simultaneously exist multiple independent *Proxies*, but only one *EA*. The *Proxy* is used by the voter and will know **who** voted, but not on what candidate or party. *EA* recieves the votes from *Proxy* and will know **what** has been voted on, but not who voted. After the election closes, all SC&V votes are published and can therefore be audited; a voter can detect that their vote has been included in the tally and not modified. Furthermore, to fulfill the E2E requirements, the system also has universal verifiability; anyone can recount the tally if they like.

In order to vote, the voter needs to obtain two paper-based cards in advance, a *ballot card* and a *coding card*.

Ballot Card

EA is responsible for preparing the paper ballots, which consist of the following information covered by a scratch surface (in the style of a lottery ticket). The purpose of the scratch surface is to prevent anybody from knowing who gets which ballot while they are distributed.

- List of candidates, permuted with a random permutation
- A unique ballot serial number S_l
- Four confirmation tokens A, B, C, D – one per column



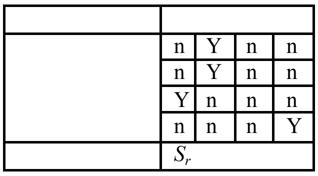
Candidate	*A*	*B*	*C*	*D*
2. Jerry				
3. Edgar				
0. Ervin				
1. Donald				
S_l				

Figure 3.1: Ballot Card

Coding Card

A *Proxy* prepares the coding card which consists of:

- Four columns, with exactly one Y (Yes) and three n (No) on each row
- Coding card serial number S_r



	n	Y	n	n
	n	Y	n	n
	Y	n	n	n
	n	n	n	Y
	S_r			

Figure 3.2: Coding Card

A coding card is **not** covered with a scratch surface, and can easily be accessed from e.g. the *Proxy* website in a suitable format so that voters can print them.

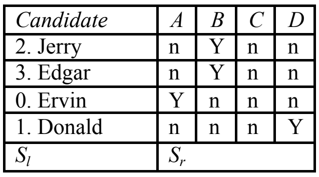
Serial numbers

The main purpose of the serial numbers S_l and S_r is to be internal identifiers for *EA* and *Proxy*, so they know which permutation of candidates and Yes/No-pattern is used by the voter.

Voting procedure

For a voter (e.g. Alice) to vote using the SC&V system, she first has to obtain the two cards described above.

Step 1 Alice lays the ballot and coding card side by side and obtains a complete ballot:



Candidate	*A*	*B*	*C*	*D*
2. Jerry	n	Y	n	n
3. Edgar	n	Y	n	n
0. Ervin	Y	n	n	n
1. Donald	n	n	n	Y
S_l	S_r			

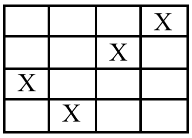
Figure 3.3: Complete ballot

Step 2 Alice finds a *Proxy* she trusts and authenticates herself on their election webpage.

Step 3 An empty 4-column matrix is shown on the screen (without any candidates or n/Y marks), and Alice marks her choices according to the following concept:

- On the row corresponding to the candidate she votes for, she marks the position of the Y according to her complete ballot.
- On each of the remaining rows, she puts a mark in one of the columns with an n according to her complete ballot.

A vote for candidate Ervin could look like this on the screen:



			X
		X	
X			
	X		

Figure 3.4: Choice matrix displayed on screen

Step 4 *Proxy* commits to the clicks Alice has made, and sends the commitments to *EA* through a commitment scheme. This step is required to prevent *Proxy* from modifying the content. Alice will also be able to print the choices out if she like.

Step 5 Alice enters the coding card serial number S_r.

Step 6 *Proxy* verifies S_r, and converts the choices into a 4-column ballot matrix by putting an x on each n that was not marked.

X		X	
X			X
	X	X	X
X		X	

Figure 3.5: Ballot matrix

Step 7 *Proxy* obtains a blind signature from *EA* under each ballot matrix column. This step is required to prevent *EA* from modifying the content.

Step 8 Alice enters the ballot serial number S_l.

Step 9 *Proxy* sends S_l together with the ballot columns to *EA*.

Step 10 *EA* stores the obtained ballot columns into its database. When the election closes, *EA* publishes the commitments to the ballot columns previously obtained from *Proxy*.

Step 11 Alice selects which column she want as receipt. The receipt consists of three parts.

- $T \in \{A, B, C, D\}$ confirmation token value
- y - ballot column
- t such that $T = sign_{EA}(t, S_l)$

$$C, \begin{array}{|c|}\hline \text{X} \\ \hline \\ \hline \text{X} \\ \hline \text{X} \\ \hline \end{array}, c$$

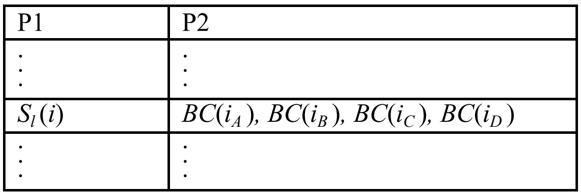
Figure 3.6: Receipt for column C

EA database

In this section we describe a simplified overview of the database structure *EA* uses, to make it easier to comprehend the overall system. For a more detailed technical description, we refer to the original publication by Kutylowski and Zagórski (2010).

When the ballot columns are received from *Proxy*, *EA* stores them in its database. The database has two tables, P and R.

Table P Each row of P is dedicated to a single ballot matrix (e.g. a vote). Column $P1$ corresponds to the ballot serial number S_l. Column $P2$ contains reference pointers to each of the four ballot columns (BC). The contents of each ballot column are stored in table R.



P1	P2
⋮	⋮
$S_l(i)$	$BC(i_A)$, $BC(i_B)$, $BC(i_C)$, $BC(i_D)$
⋮	⋮

Figure 3.7: Structure of table P

Table R Each ballot column of some ballot has a dedicated row in R. There are three columns, which are used to store permutation data calculations so that *EA* can obtain the correct choice made by the voter. We will not go into detail of how *EA*'s database tables calculates the permutations, but it is constructed in such a way that all steps in the voting chain can be verified by an external entity.

Chapter 4

System Design

4.1 A modification of SC&V

While reviewing the collected information and data, it became evident that the SC&V system took an approach which had a lot of advantages. SC&V fulfils all crucial security requirements needed for a remote electronic voting system, including E2E verifiability as well as the secure platform problem.

However, a concern when trying to apply SC&V to the Swedish electoral system, is that the system is built to allow voting for candidates in elections where the number of candidates is relatively small. Sweden has eight large parties, and each party can register up to 76 candidates to be printed on the paper ballot used at the polling station (Valmyndigheten, 2010a). If SC&V was applied directly on the Swedish system, the choice matrix would potentially consist of 600+ rows. In practise this would be almost impossible from a usability perspective. Users would have to actively mark one column on each row, which would be very time consuming with a high risk of misunderstanding and misplaced votes.

The design of the resulting system is based on SC&V since it has many appealing features, but to make it work with the current Swedish electoral system some adjustments had to be made.

4.1.1 Color coding

When looking at a big matrix filled with Y's and n's, it can be hard to distinguish them from each other. Therefore we have replaced the letters with colour codes (dark colour for Y, light for n), which makes it easier to follow (see Figure 4.2).

4.1.2 Managing parties & candidates

As previously described, an eligible voter has to be able to vote for a party, but also a candidate within the party if they like. To make this possible using the SC&V system, we renamed the table that is currently labelled “Candidate” to “Parties”. It will be permutated and calculated in the exact same way as in the original SC&V

system, but contain names of the different parties instead of candidates. This allows the voter to place a vote on a specific party. We also include a row for a blank vote.

To be able to also vote for a candidate, we introduce a new table labelled "Candidates", which contains a permutated list of numbers ranging from $1 - n$, where n is the maximum number of candidates any of the different parties have registered. Similar to the list with parties, we include a row representing a blank vote. The permutation is calculated in the same way as the list with parties.

To know which candidate to vote for, *EA* have to publicly advertise a list of all candidates, where they are associated with a certain number. The voter then has to select a candidate and mark their choice, in the same manner as for choosing a party (marking the position of the dark field).

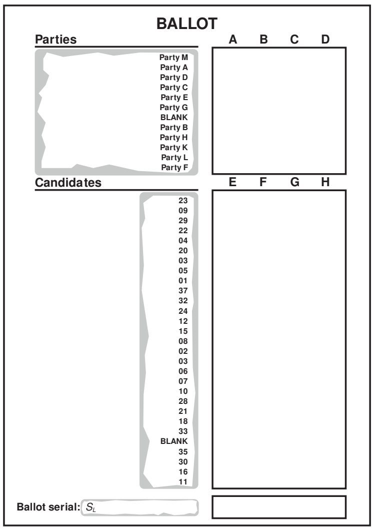


Figure 4.1: Ballot card with scratch surfaces and cut-out "windows" for coding card.

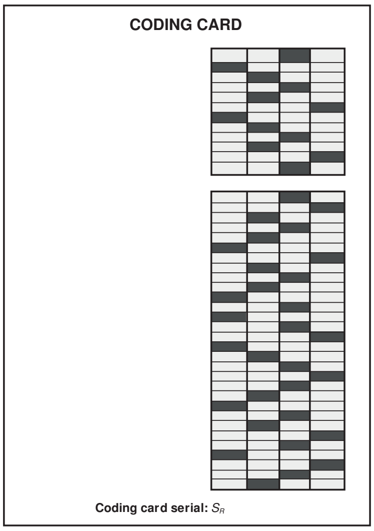


Figure 4.2: Coding card. Dark boxes represents Y and light boxes n.

4.1.3 Proxy modifications

Instead of just generating one ballot matrix, *Proxy* generates two different ballot matrices – one representing Parties, and one representing Candidates. Basically the process is the same, but duplicated. E.g. *Proxy* obtains blind signatures for 8 columns instead of 4, and sends two ballot matrices to *EA* instead of just one.

4.1.4 Election Authority modifications

Introducing column P3 and table S For *EA* to handle one more matrix, we introduce a new column *P3* in *EA*'s database table *P*. For simplicity, we rename the ballot column pointers in *P2* from *BC* to *PC* (Party Column). In *P3* we name the column pointer *CC* (Candiadte Column). Table *R* contains the column data from the Parties ballot matrix received from *Proxy*. We duplicate the structure of table *R* into a new table *S*, to hold the column data from the Candidate ballot matrix.

P1	P2	P3
⋮	⋮	⋮
$S_l(i)$	$PC(i_A)$, $PC(i_B)$, $PC(i_C)$, $PC(i_D)$	$CC(i_E)$, $CC(i_F)$, $CC(i_G)$, $CC(i_H)$
⋮	⋮	⋮

Figure 4.3: Structure of modified table P

Finding the candidate *EA* will perform the same calculations as in the original SC&V system, to obtain the party voted for. Since both the parties and the candidates share the ballot serial number S_l, it will be possible to fetch the number of the candidate voted for. Once the party has been determined, it will be easy to cross reference the candidate number with the actual candidate of that party.

4.2 Integration of system in society

If an electronic voting system was introduced in Sweden, it would have to co-exist with the current system for a long period of time. Our proposal does not completely support all features available in the Swedish general elections, such as voting for an alternative unregistered party or nominating an unlisted candidate.

4.2.1 Registering as a Proxy

The *EA* would also have to enable third-party entities to register as a *Proxy*, and providing them with access to an API that would be used for communication between the two, as well as requirements of the coding cards (number of parties/candidates). To be able to register as a *Proxy*, a certain security standard is required, in particular sufficient user authentication.

4.2.2 Opt in for electronic voting

To make sure voters can place only one vote (and not both paper-based and electronic) we let them opt-in by registering for electronic voting during a certain timeframe before the election period. This could perhaps be done from the election authority website. They would then receive a ballot according to our system, instead of a regular poll card used for paper-based voting. In Sweden it is possible to vote without a poll card on the actual Election Day only using personal identification. To prevent multiple votes, this scenario must be prohibited for all voters who have registered for electronic voting.

4.2.3 Multiple votes

In order to avoid the extreme scenario of someone literally forcing someone to vote in a specific way (or those who change their minds), just like the Estonian system, our system allows for replacing previous votes during the election period. Since the same ballot card serial number S_l is used, this is possible. All previous ballot columns with the same S_l would be overwritten in the *EA* database.

4.3 Voting procedure

In this section the voting procedure is described from the voter's perspective.

Preparation A voter (e.g. Alice) opts in by registering for electronic voting at the Election Authority website (identification using e-authentication) a couple of weeks before the election.

Step 1 Alice obtains her unique ballot card, perhaps by postal mail to her national registration address.

Step 2 Alice chooses a Proxy that she trusts. Either she can print a coding card from its website, or fetch it physically if made available by the Proxy.

Step 3 Alice peels off the scratch surface of the ballot card and combines it with the coding card to get a complete ballot.

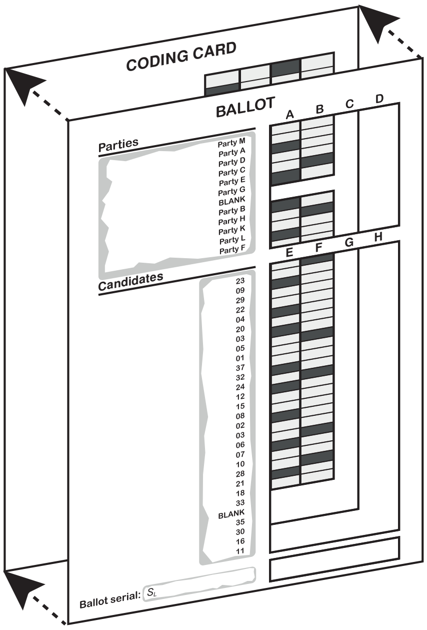


Figure 4.1: Ballot Card + Coding Card

Step 4 Alice authorizes herself on the Proxy website.

Step 5 Alice locates the Party she wants to vote for, and marks her choices in the empty matrix labelled Parties represented on the screen.

Step 6 Alice identifies the candidate she wants to vote for, by looking at the public candidate list provided by EA. She locates the corresponding number in the permutated list "Candidates" on the ballot, and marks her choices in the empty matrix labelled Candidates represented on the screen.

Step 7 Alice enters coding card serial number S_r.

Step 8 Alice enters coding card serial number S_l.

Step 9 Alice selects which column from each table she wants as a receipt.

Step 10 The receipts are presented on the screen, and Alice can print or save them if she likes.

4.3.1 System Protocol

Figure 4.2 displays a graphical representation of the system protocol used for voting.

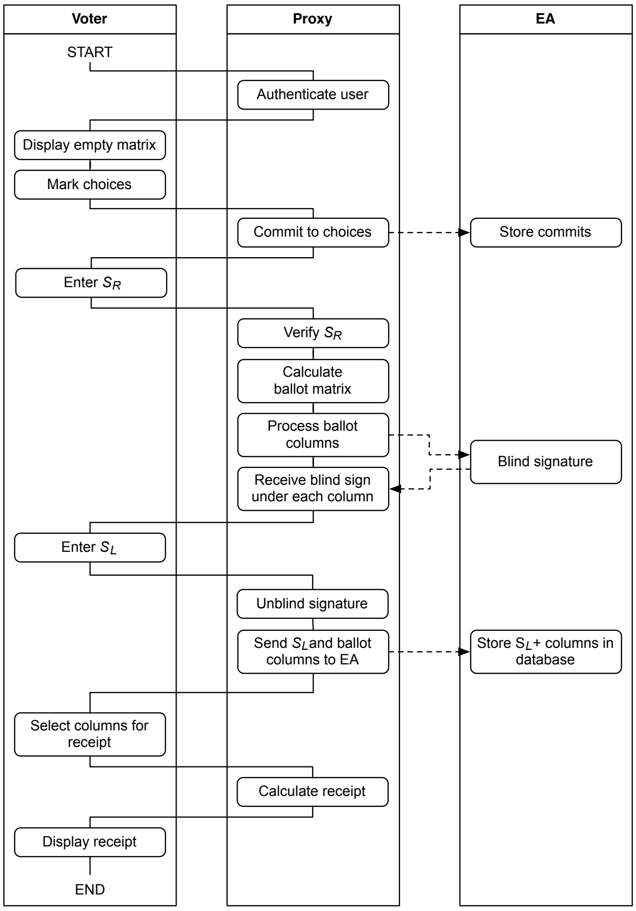


Figure 4.2: System protocol

Chapter 5

Discussion & Conclusion

When voting in Sweden today, all eligible voters have the choice to write the name of any party on a blank ballot to place a vote on them. It is also possible to nominate candidates not present on the paper ballot. Our system does not support these features – for a party to be available for electronic voting using our system, they would first have to be registered with the Election Authorities, who then would add them to the ballot and coding card.

5.1 Usability concerns

One of the major drawbacks we see with our proposed system is usability. A lot of clicks have to be made in a correct pattern – in the worst case more than 100 clicks. The matrix system used ensures the security of the system, but it is arguable that it is too complicated for voters to understand how to fill in the matrices. Also, the probability of misplaced votes or misunderstanding might outweigh the convenience of remote voting.

5.2 Security concerns

5.2.1 Malicious behaviour of voter's PC

Assumption: *Voter's (Alice) PC behaves in a dishonest way (infected by malicious software), but reliable Proxy and EA.*

Even if the PC sends all information it knows to an attacker, it is impossible to find out (1) which row that is marked with *Yes*, and (2) which row that corresponds to a certain party or candidate number.

For the PC to successfully change Alice's vote into a random party, it first has to guess which row corresponds to a *Yes* with a probability of $\frac{1}{k}$ (where k is the number of rows in the Parties list), and then change it to a *no.* Then choose one of the remaining rows, and guess which field corresponds to a *Yes* on that particular row according to the coding card, with a probability of $\frac{1}{3}$. Consequently, there is only a $\frac{1}{3k}$ probability for the PC to successfully change Alice's vote into a random one. Alice can still detect the fraudulent behaviour through her receipt, but there is still a risk that the receipt column she chose is unmodified by the changes. The probability of a successful and undetectable vote change is $\frac{1}{4k}$.

5.2.2 Malicious behaviour of Proxy

Assumption: *Proxy behaves in a dishonest way, but reliable PC and EA.*

Since Proxy commits to Alice's choices before the coding card serial is known, it cannot change the ballot without *EA* noticing. After Alice has entered the coding card serial *Proxy* knows which row is marked with *Yes*. However, it do not know the permutation of parties or candidates, and cannot therefore change the vote to a specific outcome. *Proxy* has the possibility to change the vote into a random one before committing Alice's choices to *EA*, but this would generate mismatching receipts that would be detected by Alice.

5.2.3 Malicious behaviour of EA

Assumption: *EA behaves in a dishonest way, but reliable PC and Proxy.*

The only chance for *EA* to change a vote is when the columns are inserted into the database. Since the voter gets a receipt of a column signed by *EA*, the mismatch can be detected.

5.2.4 Malicious behaviour of external part

One unavoidable possibility with remote electronic voting is that another person could be physically present, forcing Alice to vote in a certain way. Since our system allows for replacing votes, it would have to be done in a very short timeframe just before the electronic voting closes. This could arguably be compared to the flaws of the current Swedish system described in section 3.1.

In a larger perspective, there is a potential risk that a foreign/external power could bring down the voting services, e.g. through a DDoS attack. This threat alone is perhaps enough to justify the continuance of paper-based systems.

5.3 Preventing double votes

In order to prevent a voter from placing both an electronic and a physical paper-based vote, we have two different possible approaches.

The first and simplest solution is to prohibit all voters that have registered for electronic voting from placing a vote in a polling station. This can be done by marking all registerd "e-voters" on the pre-printed electoral register. Using this approach, all *Proxies* can be available during the Election Day. The major disadvantage with this approach is that if a voter initially registered for electronic voting, but misplaced their ballot card (or in some other way has failed to vote electronically) they cannot vote at all.

A possibly better solution is that the remote electronic voting system closes some time before the Election Day. The Proxies would then send information about witch voters that have voted to *EA*, which is responsible for printing the electoral register. Only these voters would then be prohibited from placing a vote in a polling station. To maximize the timeframe *Proxies* are open before the Election Day, it might be possible to introduce an electronic electoral register (printing and distribution of electoral registers is time consuming). However, the possibility to do so has not been investigated.

5.4 Conclusion

Electronic voting is an extensive topic related with many difficult issues. It is hard to fulfil all desired characteristics and security requirements, which is demonstrated by the lack of systems in use today. All forms of voting have their vulnerabilities, whether by paper or electronic. There are weaknesses in the current paper-based system today, but to this date no electronic voting system has been satisfactory enough to completely replace it. However, the "Scratch, Click & Vote" scheme takes an interesting approach on how to satisfy almost all of the important requirements.

In the technology-based society today, the topic of electronic voting will only become more and more appealing. Estonia among others has already implemented a remote electronic voting system that co-exists with traditional voting. The turnout has increased since they started, but we can only speculate that this is due to the introduction of remote voting. It is also evident that the general trust in the system has increased significantly during the last years.

The research in the field is moving forward, and we would not be surprised if electronic voting is introduced on a larger scale in the future. Nevertheless, to completely replace paper-based systems will take a long time. Voting is a cornerstone of democracy; the security, confidentiality and privacy requirements of a proper electronic voting system have to be waterproof.

References

Sara L Bränström. 2010. Valet kostar halv miljard. *SvD Näringliv*. URL http://www.svd.se/naringsliv/valet-kostar-halv-miljard_5361623.svd, visited on 2012-02-12.

Olle Findah. 2011. Svenskarna och internet 2011. DanagårdsLiTHO, Ödeshög. ISBN 978-91-979411-2-9.

Miroslaw Kutylowski and Filip Zagórski. 2010. Scratch, click & vote: E2e voting over the internet. In David Chaum, Markus Jakobsson, Ronald L. Rivest, Peter Y. A. Ryan, Josh Benaloh, Miroslaw Kutylowski, and Ben Adida, editors, *Towards Trustworthy Elections*, volume 6000 of *Lecture Notes in Computer Science*, pages 343–356. Springer. ISBN 978-3-642-12979-7.

Logica. 2011. Användning och spridning av e-legitimation i sverige. URL http://eid.primeportal.com/eid/Sidor/Statistikochanv%C3%A4ndning.aspx, visited on 2012-04-09.

Ronald L. Rivest. 2001a. Issues in cryptography. Short luncheon talk given March 7, 2001 at Computers, Freedom, and Privacy 2001 Conference.

Ronald L. Rivest. 2001b. Electronic voting. Talk given for Cambridge Club at Harvard Faculty Club, March 5, 2001.

SCB. 2011. Privatpersoners användning av datorer och internet 2011. URL http://www.scb.se/statistik/_publikationer/LE0108_2011A02_BR_IT01BR1201.pdf, visited on 2012-04-10.

Valmyndigheten. 2010a. Regler för valsedelslayout. URL http://www.val.se/det_svenska_valsystemet/partier/bestalla_valsedlar/manual_regler_for_valsedelslayout2010.pdf, visited on 2012-04-11.

Valmyndigheten. 2010b. Rösta på parti och person. URL http://www.val.se/det_svenska_valsystemet/valsedlar_och_personrostning/personrosta/index.html, visited on 2012-02-12.

VVK. 2011. Statistics about internet voting in estonia. URL http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics, visited on 2012-04-10.

List of Figures