



Zentrum für sichere Informationstechnologie - Austria Secure Information Technology Center - Austria

A-1040 Wien, Weyringergasse 35
Tel.: ++43 1 - 503 19 63 - 0
Fax: ++43 1 - 503 19 63 - 66

A-8010 Graz, Inffeldgasse 16a
Tel.: ++43 316 - 873 5514
Fax: ++43 316 - 873 5520

e-Voting A Survey and Introduction

Dipl.-Ing. Thomas Rössler, A-SIT • eMail: thomas.roessler@a-sit.at

Abstract: Elections and referenda are the essential vehicles for citizens to participate in democratic processes. With the raise of e-governmental applications e-voting initiatives gain more and more interest. Thus, many countries are piloting with various e-voting models and systems in order to enable voting from abroad as well, for European Parliament elections for instance. International organizations develop standards and recommendations in this area.

This report is an introduction to e-voting systems. It is intended to be an entry point thus it gives an overview of common models, existing elections schemes and explains the usual terminology.

Contents

1 Introduction	3
1.1 Motivation and General Requirements	3
2 Concept of an e-Voting System	5
2.1 Pre-Voting Phase	6
2.1.1 Candidate Nomination Process	6
2.1.2 Voter Registration Process	6
2.2 Voting Phase	6
2.3 Post-Voting Phase	6
2.3.1 Counting	6
2.3.2 Result	7
2.4 Audit, Administration	7
2.5 Phase Models	7
2.5.1 One-Phase Model	7
2.5.2 Two- and n-Phase Models	7
3 Overview of e-Voting Schemes	8
3.1 EVS based on Homomorphic Encryption	8
3.2 EVS based on Mixing Nets	10
3.3 EVS based on Blind Signatures	11
4 Summary	12
References	13

1 Introduction

Electronic elections, e-voting respectively, gain more and more public interest. Some countries offer their citizens to participate in elections using electronic channels. The term e-voting stands for the possibility of voting electronically in general. Thus, e-voting includes voting by the use of telephones and electronic voting machines in voting booths as well. In this report, we are talking about e-voting in the sense of voting by the use of an ordinary computer via the Internet. This branch of e-voting is sometimes denoted as i-voting.

However, in this report we first give a motivation and we state the basic requirements and assets worth protecting in an election system. Thus, keeping the voter's decision represented by the voter's cast vote an inviolable secret is of paramount importance. In the next section, we give an overview over the election phases, the pre-voting phase, the voting phase and the post-voting phase respectively. In this course, we introduce the main actors used in e-voting scenarios. The next chapter describes the three common ways the technical core of e-voting can be implemented. The so called e-voting schemes represent a technical and mathematical model underlying every e-voting implementation. Most of the existing schemes can be divided into homomorphic schemes, mixing net schemes and blind signature schemes, which make use of cryptographic principles and mechanisms to meet the requirements of a democratic election. Finally, we summarize.

1.1 Motivation and General Requirements

In democracies, voting is the most important tool in democratic decision making. Therefore, elections and referenda should be accessible for as much people as possible. Especially when considering citizens living abroad, for these people it is sometimes difficult to participate in elections.

On the other hand, elections influence the democracy in a country directly. So it is highly important to ensure that elections carried out electronically are at least as secure and reliable as conventional elections are.

Many countries are experimenting with e-voting pilots or are using e-voting systems in real elections already. In Europe, noteworthy e-voting systems were used or were at least tested in:

- Switzerland (Geneva, Neuchâtel, Zurich) [1][2][3]
- United Kingdom (St.Albans, Sheffield, Liverpool) [4][5]
- The Netherlands.[6][7]

Recently, the Council of Europe has initiated an ad hoc group of specialists on legal, operational, and technical standards for e-enabled voting to develop recommendations for e-voting [8]. The recommendations developed by this group should be used in e-voting systems in order to guarantee the following major principles of democratic elections [9]:

- universal
- equal
- free
- secret
- direct suffrage.

In addition to these cardinal principles, Lorrie Cranor gives in [10] and [11] some definitions of requirements for e-voting systems. She states the following "characteristics of a good electronic voting system":

- Accuracy

- Democracy
- Privacy
- Verifiability
- Convenience
- Flexibility
- Mobility

At first sight, the most important characteristics are accuracy, democracy, privacy and verifiability. Cranor and Cytron define them in [11] as follows:

Accuracy: A system is accurate if

1. it is not possible for a vote to be altered,
2. it is not possible for a validated vote to be eliminated from the final tally, and
3. it is not possible for an invalid vote to be counted in the final tally.

In the most accurate systems the final vote tally must be perfect, either because no inaccuracies can be introduced or because all inaccuracies introduced can be detected and corrected. Partially accurate systems can detect but not necessarily correct inaccuracies. Accuracy can be measured in terms of the margin of error, the probability of error, or the number of points at which error can be introduced.[11]

Democracy: A system is democratic if

1. it permits only eligible voters to vote,
2. it ensures that each eligible voter can vote only once.[11]

Privacy: A system is private if

1. neither election authorities nor anyone else can link any ballot to the voter who cast it, and
2. no voter can prove that he or she voted in a particular way.

The second privacy factor is important for the prevention of vote buying and extortion. Voters can only sell their votes if they are able to prove to the buyer that they actually voted according to the buyer's wishes. Likewise, those who use extortion to force voters to vote in a particular way cannot succeed unless they can demand that voters prove that they voted as requested.[11]

Verifiability: A system is verifiable if voters can independently verify that their votes have been counted correctly.

The most verifiable systems allow all voters to verify their votes and correct any mistakes they might find without sacrificing privacy. Less verifiable systems might allow mistakes to be pointed out, but not corrected or might allow verification of the process by party representatives but not by individual voters.[11]

Based on these definitions and thoughts, we can define the assets of an election system. All e-voting systems, and of course common election models as well, have to take efforts to protect their assets. For example, the most important assets can be given as:

Authentication Data is the information used to prove the claimed identity of a user, the candidate or the voter in particular.

Cast Vote represents the voter's choice (the voter's decision) transferred to the electronic ballot box. The integrity, confidentiality and availability of cast votes have to be ensured until the counting process and

even beyond, for recounting for instance. The voter's decision is the most important asset in elections. Especially in e-voting systems, ensuring that the voter's decision remains an inviolable secret is one of the main design requirements.

Summing up, the very most important asset thus a requirement of e-voting system is to keep the voter's decision an inviolable secret. Therefore, the protection of cast votes is essential. On the one hand, it must be ensured that no cast vote carrying the voter's decision can be mapped with the voter's identity. On the other hand, for elections voters have to be uniquely identified and authenticated. These two requirements seems to be contradictory but both have to be satisfied. This is the reason why electronic election systems are so challenging to design.

2 Concept of an e-Voting System

From a conceptual perspective, e-voting can be split up into three phases:

- Pre-Voting Phase
- Voting Phase
- Post-Voting Phase

Considering e-voting systems this way follows the high level models of election systems given by the Organization for the Advancement of Structured Information Standards (OASIS). The OASIS consortium specifies a so called Election Markup Language (EML) [12] specially for the exchange of data within e-voting processes. Therefore, OASIS drafts a high level overview and a high level model dealing with the human view and a high level model dealing with the technical view. In this report, mainly the human view is taken as a basis for talking about e-voting systems from the conceptual point of view. These models should be the initial point of creating e-voting concepts. EML is in particular useful for interoperability reasons.

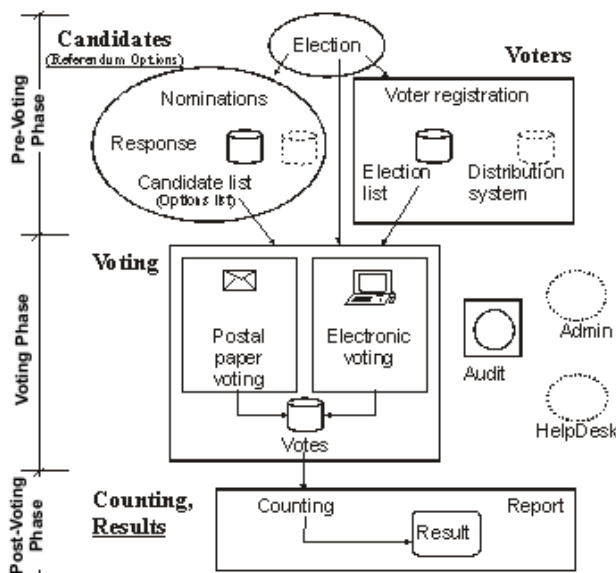


Figure 1: The human model stated by EML

Separating the process into these phases gives a good abstraction of an election process. Moreover, these models provide a common terminology and a conceptual perspective.

2.1 Pre-Voting Phase

As depicted in the human view of the OASIS high level model (see figure 1), the major tasks provided within this phase are:

1. Candidate Nomination Process
 - Candidate Nomination
 - Candidate Response
 - Generation of the Candidates List
2. Voter Registration Process
 - Voter Registration
 - Generation of the Election List

2.1.1 Candidate Nomination Process

There might be various ways to become nominated as a candidate to be elected depending on the national legislative. A candidate has to meet some legal restrictions, e.g. she must be old enough, etc. The candidate suggested might have to accept her nomination. She has to decide whether to accept or decline her nomination. Finally, a nomination process results in a list containing all candidates, the so called candidate list.

The EML model considers referenda as well. Thus, the model includes the referendum options nomination process in parallel to the candidate nomination process. In principle, they are quite similar beside the different legislative restrictions. Even the options nomination process leads to a resulting options list. In this paper we limit our scope only to elections.

2.1.2 Voter Registration Process

Depending on the local laws, voters have to register for voting explicitly. On the other hand, in many countries citizens are registered for voting automatically. However, the result of this process is an election list containing all persons allowed to vote.

2.2 Voting Phase

Based on the results of the pre-voting phase, the voting phase enables all eligible voters to make their decisions and cast their votes. Thus, by the use of the election list the voter has to authenticate herself as an eligible voter and she has to cast her individual vote. Figure 1 does not limit voting on electronic voting only. It is the voter's decision which channel she prefers to cast her vote. However, the main scope in this paper is the Internet as electronic voting channel. Since the voter should have an alternative to e-voting and since conventional voting with paper ballots must be provided in parallel, the model has to consider multiple possibilities. Especially the interfaces and cutting edges between electronic and conventional elections have to be considered in the conceptual design.

2.3 Post-Voting Phase

The post-voting phase deals with the juicy bites of the e-voting process. This phase covers counting and result reporting mainly.

2.3.1 Counting

Counting is one of the most critical steps. Here, the possibility of recounting must be considered as well. Therefore, counting has to be re-runnable and the input needed, such as the cast votes in particular, have to be archived.

2.3.2 Result

Close to the counting mechanisms, an analysis system is needed. Such a system provides the auditing team and the election officials with various reports. One of the most important reports is of course the final result of the counting. The form and the precise schema of such reports is out of scope of the model provided by EML.

2.4 Audit, Administration

Beside the phases and roles given above, there are some other important actors and elements in the model. Very important are the audit mechanisms needed along all phases of an election. On the one hand, it is important to have possibilities to prove the correctness of the process as such. On the other hand, it is crucial to do not violate the main principles and security requirements, keeping a vote an inviolable secret in particular. However, audit is necessary to prove the authenticity of the result of the election. Thus, a special set of persons, e.g. election officials and candidate's representatives, should be allowed to gain access to auditing information.

System administration is critical as well, since administrators are allowed to access the system. Nevertheless, administration is necessary and therefore the security concept of the e-voting system has to protect critical data and components, the secrecy of the ballots especially. This effects the organizational aspects of the security concept either. Not only technical security mechanisms can guarantee this. The administrative staff has to be elected in respect to reliability as well.

2.5 Phase Models

Election systems can be categorized according to the number of rounds a voter has to pass casting a vote. Most of the existing e-voting models can be classified into one-phase and two-phase models. Since a few models require some more phases, those models are called n -phase models.

Each phase represents a certain action required at a certain time. Thus, the phases are in a special order. The phases considered here are not necessarily the same that are defined within EML. Some of them can be similar, although a phase in the model view may cover several EML phases as well and vice versa. For example, a voting model may require a user to register and to vote in two distinct steps. Talking in EML, the pre-voting phase (voter-registration) is similar to phase one. The voting phase itself is phase two from the model's perspective. Post-electoral tasks as defined in EML are not considered here since they are not a part of the voters' business. This categorization bases on the voter's view.

2.5.1 One-Phase Model

One-Phase models are quite rare. Here, for the voter casting a vote can be done in a one-stop manner. This means, that the voter is not required to register for voting in advance. Thus, from the voter's perspective the voting process takes places in one phase.

2.5.2 Two- and n -Phase Models

The most of the e-voting models available are so called two-phase models (fig.2). Commonly, in the first phase the voter has to register for voting and she receives some kind of authentication credentials in exchange. By the use of these credentials, the voter is permitted to take part at the voting process in phase two (main phase).

On and of, between the first phase and the main phase a system may require some more steps. In a so called n -phase model, the voter is repeatedly asked to register for voting in two or more distinct steps at multiple authorities. In this case, from the voter's perspective the pre-voting phase defined by EML is broken up into n phases.

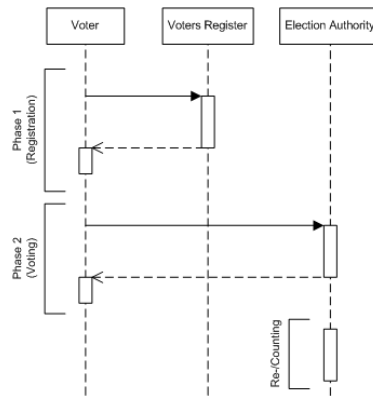


Figure 2: Sequence of a 2-phase voting model

3 Overview of e-Voting Schemes

E-voting systems consist of a conceptual design and an underlying so-called e-voting scheme. Thus, e-voting systems are based on e-voting schemes (EVS). A scheme is the core of the system ensuring that requirements are met. Most of them use cryptographic mechanisms and principles. This chapter gives an overview and a survey of the most important classes of schemes used today. They can be grouped as follows:

- EVS based on Homomorphic Encryption [13][14][15][16]
- EVS based on Mixing Nets [17][18][19]
- EVS based on Blind Signatures [17][20][21][22][23][24]

Of course, there exist other schemes as well and the grouping can be done based on other objectives. However, here the most common approach was chosen.

The following sections do not describe the schemes in all details. The aim of this introduction is to provide the main ideas and principles only. Further introducing descriptions can be found in [25] and in the referenced documents for instance.

3.1 EVS based on Homomorphic Encryption

These schemes are based on the homomorphic properties of the encryption methods used. In context of e-voting, in such a scheme all encrypted votes are collected and summed up. At last the sum of all encrypted votes is decrypted thus the result can be reconstructed. This works because of homomorphism.

To give a mathematical definition of homomorphism:

A mapping $f : A \mapsto B$ is called a homomorphism of A into B if f preserves operations of A . That is, if \circ is an operation of A and \star , an operation of B , then $\forall x, y \in A$ we have $f(x \circ y) = f(x) \star f(y)$. [26]

For instance, the ElGamal public key encryption is homomorph. Using this for encrypting votes would be a basis for a homomorphic voting scheme.

A scheme of this kind is the scheme proposed by Josh Benaloh [14]. Beside other cryptographic mechanisms, such as threshold cryptography, this scheme bases on homomorphic encryption. In order to give an idea of the principles behind homomorphic encryption, we give an example based on a simple yes-no decision where 0 or 1 represent the available options.

The e-voting environment consists of M -authorities, A_1 to A_M . Each of them owns a public key pair. Authorities are tight to each other by threshold cryptography requiring that at least t authorities are used to decrypt the result of the election. The number of all voters is given by N , whereby every voter has got her very own public key pair.

To cast a vote, the voter has to split it up into M parts, each for one authority.

$$v_i \rightarrow s_{i,1}, \dots, s_{i,j}, \dots, s_{i,M} \quad (1)$$

Next, every part of the decomposed vote becomes encrypted with the public key of the authority for which the part of the vote is intended for. One of those shares of a voter's vote dedicated to an authority A_j look like this:

$$(g^{r_{i,j}}, \gamma_j^{r_{i,j}} g^{s_{i,j}}) \quad (2)$$

The notation used is quite common, but for this introduction it is not necessary to know all its details. Here, the tuple $(g^r, \gamma^r x)$ stands for the ElGamal encryption algorithm, where g denotes the generator function and r represents a random number. The random number is characteristic for the ElGamal encryption. This is why it is denoted as a randomized encryption algorithm. In consequence of this, by the variation of this random factor the encrypted messages will vary even if the plain text is the same. This is very important for this kind of e-voting scheme. Otherwise the voter's decision could be revealed by the form of the encrypted vote since there would only exist two different types of encrypted votes.

After the election is over, every authority collects the valid votes received and calculates the component-wise product of all of them without decrypting the particular votes. Due to the use of threshold cryptography, this is anyhow impossible.

Assuming authority A_j receives N shares of votes, whereby all of them are proved for correctness, uniqueness and whether the voter is authorized to cast a vote.

$$(g^{r_{1,j}}, \gamma_j^{r_{1,j}} g^{s_{1,j}}), \dots, (g^{r_{i,j}}, \gamma_j^{r_{i,j}} g^{s_{i,j}}), \dots, (g^{r_{N,j}}, \gamma_j^{r_{N,j}} g^{s_{N,j}}) \quad (3)$$

Building the component-wise product of these encrypted shares leads to the following result:

$$(g^{\sum_i r_{i,j}}, \gamma_j^{\sum_i r_{i,j}} g^{\sum_i s_{i,j}}) \quad (4)$$

The component $S_j = g^{\sum_i s_{i,j}}$ is important. This component contains the resulting sum of all votes cast. Thus, by decrypting the result, authority A_j gains this component thus the sum of the shares dedicated for it respectively, namely $g^{\sum_i s_{i,j}}$. Because of the use of threshold encryption, at least the components of t authorities are necessary to reconstruct the resulting sum according to all votes cast. Therefore, the overall result can be calculated by the so called *Lagrange-Interpolation* used within threshold cryptography systems:

$$\prod_j (g^{S_{i,j}})^{\alpha_j} = g^{\sum_j S_{i,j} \alpha_j} = g^S \quad (5)$$

Due to the infeasibility of computing discrete logarithms, gaining S would be infeasible. Since the number of votes is limited by N , it is effortful to calculate all results possible, such as $g^0 \dots g^N$ reflecting $S = 0 \dots S = N$. By comparing the result with these preprocessed values, the voters decision can be easily determined.

The major principle in this scheme is, that it is not necessary to decrypt each ballot and to construct the result by the use of the encrypted votes. By using the homomorphic property of the encryption algorithm used it is possible to compute a result by using the encrypted ballots and the homomorphic function adequate to addition. Threshold encryption used within this scheme brings an additional advantage to face malicious

authorities, but it is not needed from the point of view of homomorphism. Reducing the number of authorities to one will lead to a scheme pointing the principle of homomorphic e-voting schemes best.

This idea of this scheme is widely used. Many other existing schemes are built on this principle, [16] for instance. Once again, the big advantage is that no vote has to be decrypted, which is very effortable to keep the voters choice an inviolable secret. Thus, no authority is able to conclude about the vote of a single person. The voter is authenticated by the use of some credentials and her public key pair respectively. On the other hand, the encrypted vote given by a voter, which is in the case of a threshold cryptographic system a share of her original vote only, will be never decrypted. So, the voter's secret remains untouched.

A mentionable drawback of schemes of this class is that the complexity of the scheme grows extraordinary with the number of electable options. Most elections have more than only two options, thus election schemes based on homomorphic encryption might be hard to implement due to complexity reasons.

3.2 EVS based on Mixing Nets

The basic idea in this class of schemes is the use of mixing devices. A mixing device, a mixing net for instance, takes some input and scrambles it, and vice versa. Thus, the output corresponds to some permutation of the input. This mechanism can be used to scramble incoming votes in order to decouple the voter from her vote. On the other hand, mixing devices can be used to scramble all possible votes a voter can cast among the voter has to select. As a result, the voter's choice becomes hidden and a secret. Various schemes use both principles.

David Chaum [17] introduces the idea of mixing nets the very first time. He proposes to use a cascade of several mixing devices. Each of these devices takes its input and produces an output corresponding to an arbitrary permutation of the input. Moreover, the mixing device knows the relationship between the input and the output only. However, in a cascade built of n mixing devices, since at least 1 of n mixing devices keeps the relationship between input and output a secret, the result of the whole mixing cascade remains a secret and will be unpredictable. This is one of the main advantages in context with mixing nets as proposed by David Chaum. On the other hand, this may be an disadvantage at the same time. For instance, if at least 1 device fails the whole mixing cascade is failing.

The voting scheme proposed by Martin Hirth and Kazue Sako described in their paper [19] uses this principle beside other cryptographic mechanisms such as the homomorphic property of encryption. However, the main primitive aimed in their work is the use of mixing nets in order to decouple the voter and her vote. The basic workflow is the following:

At first, assuming that for each vote possible, denoted by $v_i \in V$, there exists an encrypted counterpart using standard encryption, denoted by $e_i^{(0)} \in E$. The encryption of all valid votes possible have to be announced publicly, e.g. by the use of a bulleting board of some kind. Based on this assumption, the sequence of initial encoded votes $(e_1^{(0)} \dots e_L^{(0)})$ is taken as the input for the first mixing authority A_1 . This authority takes this input, scrambles it and feeds it to the next authority A_2 as input sequence $e_1^{(1)} \dots e_L^{(1)}$. The relation between $e_1^{(0)} \dots e_L^{(0)}$ and $e_1^{(1)} \dots e_L^{(1)}$ produced by the randomness of authority A_1 is communicated to the voter via an untappable channel. In other words, the permutation π_M used to produce the output of the input sequence is known by the voter only. This untappable channel is of absolute importance in this scheme, which ensures that the voter only is knowing which element of the output corresponds to which element of the input. By cascading all the M -authorities stepwise to a sequence, whereby the output of the preceding authority is used as the input for the succeeding authority, the resulting sequence of encoded votes $e_1^{(M)} \dots e_L^{(M)}$ is totally mixed. Because that the voter becomes informed about the relation between the input and the output sequence of every authority, she is the only one who can map an arbitrary element of the initial sequence to the according element of the final sequence. Therefore, it is essential in this situation to guarantee that the communication between every or at least one authority and the voter is kept secret and untappable. However, the voting process as such is that the voter points to the element of the resulting sequence which corresponds to the initial encrypted vote she wants to cast.

Mixing nets are very often used in e-voting systems. Very often, mixing nets are used to send a sender-untracable email. Therefore, messages are sent into a mixing net in order to lose the relation between the message and the sender. This mechanism is often used in e-voting systems in combination with

other principles, blind signatures for instance. An example for an e-voting schemes following this approach is the collision free secret ballot protocol proposed by Juang and Lei [18].

3.3 EVS based on Blind Signatures

The third major approach for realizing e-voting uses so called blind signatures. The idea of blind signatures was introduced by David Chaum in [17][20]. Blind signatures initially were intended to be used within electronic cash systems (e-cash) to ensure the anonymity of its owner. Because in e-voting schemes the motivation to keep the voter anonymous is the same, this technique can be applied as well. The key technique of blind signatures allows a signer to sign a document without seeing it. This can be compared with giving a hand written signature on to a document wrapped in a flimsy paper. The wrapped document gets signed without beeing seen.

The following paragraph describes the mathematical principle used by blind signatures.

The authority's key is given as:

$$\begin{aligned} \text{public} &: (n, e) \\ \text{private} &: (n, d) \end{aligned}$$

The voter wants the authority to sign the vote v without learning it (blind signature). Thus, the voter generates a random value r satisfying:

$$\gcd(n, r) = 1 \quad (6)$$

By using this random value r and authority's public key component e , the voter blinds her vote and creates a *blinded vote* x :

$$x = (r^e v) \bmod n \quad (7)$$

Now, the authority cannot derive any useful information from this message x . Therefore, the voter asks the authority to sign it by using its private key:

$$t = x^d \bmod n \quad (8)$$

The authority returns the signed "vote" t to the voter.

$$t = x^d \bmod n \quad (9)$$

$$= (r^e v)^d \bmod n \quad (10)$$

$$= (r^{ed} v^d) \bmod n \quad (11)$$

$$= r \cdot v^d \bmod n \quad (12)$$

Since the voter knows the random vale r used for blinding, she can remove it from the signed vote to receive:

$$s = r^{-1} t \quad (13)$$

$$= v^d \bmod n \quad (14)$$

Finally, s is the vote v signed by the use of the authority's private key preventing the authority to learn the signed vote v .

In e-voting schemes, this principle is used in several occurrences. However, common to all of these occurrences is, that a vote can be signed by an authority without reading the content, the voter's decision respectively.

For example, prior to the voting process, a voter has to identify himself at the registration authority. After having been authenticated successfully, the voter sends her blinded vote carrying her decision to the registration authority to become signed. In consequence, the voter's vote is signed by the authority by the use of a blind signature technology in order to assert that the voter is legitimated to vote. Due to the blind signature, the content of the vote will not be revealed to the registration authority. After the vote has been cast an election authority can prove every cast vote by verifying the blind signature. Thus, the election authority is able to decide whether a voter was eligible to cast a vote or not. On the one hand, the registration authority cannot learn the voter's decision during signing. On the other hand, the election authority cannot learn which voter a vote belongs to. The voter's identity remains a secret. However, the blind signature is used to prove that the voter is authenticated and authorized to cast a vote. So, the voter is authorized without revealing her identity.

In such a scheme, additional mechanisms should be implemented to ensure, that every voter can cast one valid vote only. This can be achieved by including some unique random sequence on each vote. Such a sequence should be generated in a way, that the authority cannot learn which sequence is used by a particular voter. Anyway, this could be ensured by preparing ballots in an anonymous process or by the voter himself locally.

4 Summary

In this report, we gave a short introduction on aspects of e-voting systems. Therefore, we introduced the basic requirements and the most important assets of electronic elections. To keep the voter's decision an inviolable secret during the election and beyond it was identified as the most important asset. Next, we introduced the several phases an election process can be separated to, the pre-voting phase, the voting phase and the post-voting phase respectively. In this course, the Election Markup Language (EML) and the human model given within its definition was presented. Additionally to the phases defined by EML, we categorized existing e-voting schemes according to their number of rounds, phases respectively, from the voter's point of view. Thus, we discussed one-phase models, two- and n -phase models.

After this theoretical views, we discussed the three main principles existing e-voting schemes follow. These are based homomorphic encryption, mixing nets and blind signatures. We provided a short and very simply description of the core ideas behind. Most of the existing schemes makes use of these principles and some of them combine them as well.

References

- [1] N.Braun. E-voting in der schweiz. In A.Prosser, editor, *collection of working papers of the e-Democracy/e-Voting-workshop at IRIS2003*, 2003.
- [2] R.Opplinger. *Addressing the Secure Platform Problem for Remote Internet Voting in Geneva*. eSECURITY Technologies, May 2002.
- [3] Schweizer Bundesblatt Nr. 5. *Bericht über den Vote électronique vom 9. Januar 2002: Chancen, Risiken und Machbarkeit elektronischer Ausübung politischer Rechte*, Februar 2002.
- [4] Local Government Organisation (LGA). *The Implementation of electronic voting in the UK-Research Summary*, May 2002.
- [5] The Crown. *E-Voting Security Study-Issue 1.2*, July 2002.
- [6] The Chairmen of the House of Representatives of the States General (Netherlands). *Remote Voting Project*, March 2002.
- [7] Invitation to Tender (Netherlands). *Remote Electronic Voting and Voting by Telephone Experiment*, November 2002.
- [8] Council of Europe. *Multidisciplinary Ad Hoc Group of Specialists on legal, operational and technical standards for e-enabled voting (IP1-S-EE)*, 2003.
- [9] Council of Europe, Venice Commission. *Code of good practice in electoral matters*, 2003.
- [10] L.Cranor. *Electronic Voting - Computerized polls may save money, protect privacy*. ACM Crossroads Student Magazine, 1996.
- [11] R.Cytron L.Cranor. *Design and Implementation of a Practical Security-Conscious Electronic Polling System*. Department of Computer Science, Washington University, June 1996.
- [12] Organization for the Advancement of Structured Information Standards (OASIS). *Election Markup Language (EML) 4.0a*, July 2003.
- [13] Josh Cohen and Michael Fischer. A robust and verifiable cryptographically secure election scheme. In *Proceedings of the 26th IEEE Symposium on the Foundations of Computer Science (FOCS)*, page 372 to 382. IEEE, 1985.
- [14] Josh Benaloh. *Verifiable Secret-Ballot Elections*. PhD thesis, Yale University, New Haven, 1987.
- [15] Josh Cohen and Moti Yung. Distributing the power of government to enhance the privacy of voters. In *Proceedings of 5th ACM Symposium on Principles of Distributed Computing (PODC)*, page 52 to 62. ACM, 1986.
- [16] Ronald Cramer, Rosario Gennaro, and Berry Shoenmakers. A secure and optimally efficient multi-authority election scheme. In *Advances in Cryptology - Eurocrypt 97*, page 103 to 118. Springer Verlag, LNCS, 1997.
- [17] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–86, 1981.
- [18] Wen-Sheng Juang and Chin-Laung Lei. A collision free secret ballot protocol for computerized general elections. *Computers and Security*, 15(4):339–348, 1996.
- [19] Martin Hirt and Kazue Sako. Efficient receipt-free voting based on homomorphic encryption. In *Proceedings of the Eurocrypt 2000*, 2000.
- [20] David Chaum. Blind signatures for untraceable payments. In *Proceedings of Crypto 82*, page 199 to 203. Plenum Press, New York, 1983.

- [21] Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta. A practical secret voting scheme for large scale elections. In *Advances in Cryptology - Auscrypt 92*, page 244 to 251, 1992.
- [22] Kazue Sako. Electronic voting schemes allowing open objection to the tally. In *Transactions of IEICE*, vol. E77-A No.1, 1994.
- [23] Tatsuaki Okamoto. Receipt free electronic voting schemes for large scale elections. In *Proceedings of Workshop on Security Protocols 97*, page 25 to 35. Springer Verlag, LNCS, 1997.
- [24] A.Prosser and R.Müller-Török. Electronic voting via the internet. In *Proceedings of 3rd International Conference on Enterprise Information Systems (ICEIS)*, Setubal, Portugal, page 1061 to 1066, 2001.
- [25] O.Mürk. *Electronic Voting Schemes*. Institute of Computer Science, Tartu University, June 2000.
- [26] Wenbo Mao. *Modern Cryptography - Theory and Practice*. Hewlett-Packard Books, 2004.