Report

Published by:
Ministry of Local Government and Regional Development

Design: Sissel Sandve

Electronic voting – challenges and opportunities

NORWEGIAN MINISTRY OF LOCAL GOVERNMENT AND REGIONAL DEVELOPMENT

Preface

The Working Committee was appointed by The Norwegian Ministry of Local Government and Regional Development on 26 May 2004, with the task of assessing the potential and possibilities of introducing e-voting in Norwegian elections and, if recommended, to assess how such a system can be implemented.

The committee has been organized into four sub-committees according to the particular competence of its members: one group has been responsible for the technical aspects, a second group has been responsible for the economic and administrative aspects, a third group has worked on the democratic aspects and a fourth group has been responsible for the legal aspects. The committee as a whole has had 11 meetings. The sub-committees have had additional individual meetings. Although the sub-committees are responsible for their individual chapters, the committee as a whole has discussed and determined the content of the present report.

Members of the committee have made study tours to the UK, Switzerland, the US and Estonia, reports from which are found in chapter 4 and in appendix C. The committee members have also met with central bodies working in the fields of technical security, certification and control systems.

The working committee would like to thank all the people and the institutions who have contributed valuable knowledge and comments in fulfilling its mandate.

February 2006

Index

1 Mandate and Assembly

The Working Committee was appointed by the Norwegian Ministry of Local Government and Regional Development 26 May 2004 to elucidate the use of electronic means in casting a vote during national, regional and local government elections.

1.1 The Members

1. Bernt Aardal – chair, Institute for Social Research
2. Asbjørn Ausland – Oslo City Council
3. Cort A. Dreyer – The Norwegian Ministry of Trade and Industry
4. Are Vegard Haug – University of Oslo, Faculty of Law, section for IT and Administrative Systems
5. Einar Nødtvedt – Senit Rådgivning AS
6. Kristian Pinaas – Intentor Solutions AS
7. Bjørn Erik Rasch – University of Oslo, Department of Political Science
8. Marianne Riise – The Norwegian Ministry of Local Government and Regional Development
9. Gerhard Skagestein – University of Oslo, Department of Computer Science
10. Kristin Thorud Skorpen – the Municipality of Drammen
11. Kari Aarnes – the Municipality of Trondheim

Rune Karlsen – Secretary, Institute for Social Research
Guro Stavn – Secretary, Institute for Social Research

1.2 The Mandate

The mandate of the Working Committee:
”The Working Committee shall, on a principal basis, consider and decide *whether* the opportunity to cast a vote electronically is recommendable, and in case it is, *how* this opportunity can be made feasible. Furthermore, the committee shall consider and make recommendations as to regulations and requirements that pertain to systems for electronic voting. The mandate comprises the following tasks (which have been numbered for ease of reference):

1. Consider the importance of introducing an electronic system from a democratic perspective, including legitimacy and voter participation,
2. Give an overview of different systems by which a vote may be cast electronically through different channels (Internet, Touching screens, SMS text messages, digital TV, etc.),
3. Point out advantages and disadvantages of the different systems/channels,
4. Assess the different systems/channels with respect to user friendliness and security of the votes,
5. Discuss and assess the recommendation of e-voting by means of Internet technology in as well as outside the polling stations,
6. Consider solutions for proper identification and authentication of a voter ready to submit an electronic ballot (smart card, ID card, etc.),

7. Address and pay particular attention to the problem of undue influence related to voting in uncontrolled environments outside the polling station, cf. also the discussion pertaining to postal voting,
8. Consider the problems relating to the buying and selling of votes and to the identification of a voter casting a ballot outside the polling station,
9. Consider the introduction of verification solutions in the systems, and recommend possible ways to implement such solutions,
10. Consider the problems related to open source codes,
11. Consider the use of an electronic Population Registry, and its implications for an e-voting system,
12. Consider the advantages and disadvantages of e-voting compared with regular voting in a polling station,
13. Consider costs related to large scale e-voting, on a short term as well as a long term basis, including the short term and long term cost reduction potential,
14. Consider effects of changing control routines, from that of the layman to the professional expert, including effects on the voting system with respect to the audit and administration of the election and the competence of the administrators,
15. Consider the responsibilities related to electronic voting, from a local, regional and national perspective,
16. Consider how an approval of electronic voting systems should be conducted,
17. Summon reports and research done in this area,
18. Give an account of experience drawn on different types of voting system in other countries.

On behalf of the European Council a common legal and technical framework for e-voting (including a computer language standard EML) is being developed. Norway takes part in this development. It is expected that the EC recommendation will be considered by the end of 2004. It is within the working committee's mandate to consider what practical consequences the provisions of the recommendation will have for Norway.

The working committee is free to take up any questions related to the use of electronic voting means beyond the tasks specified in the mandate above.

Considerations made by the working committee shall be worked out in a report to be delivered to the Ministry by 31 December 2005."

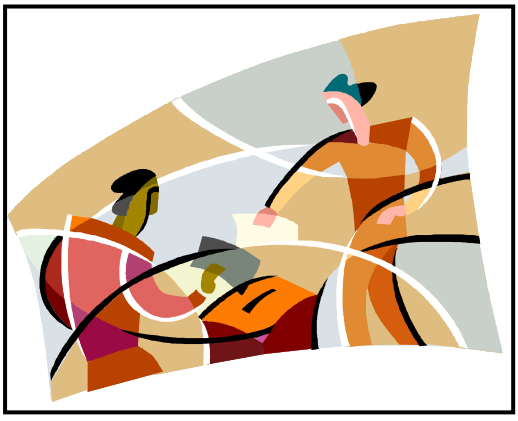
2 Recommendations from the working committee

2.1 Introduction

The present report considers questions concerning electronic voting in Norway; to what extent e-voting is recommendable, and, if it is recommended, how it can be implemented. The questions have been considered from democratic, legal, technical and administrative points of view. The discussion that follows has been structured according to three central dimensions relating to how voters cast their votes:

1. One major distinction is made between the act of physically inserting a paper ballot in a ballot box on the one hand and casting an electronic ballot on the other.
2. Another distinction is made between the act of casting a vote in a polling station under the supervision of an election official (called *controlled* environments) and casting a vote outside the polling station (called *uncontrolled* environments).
3. A third distinction is related to the time of voting. We make a distinction between the submission of advance votes (called *phase 1* in the present report), and the submission of votes on Election Day (called *phase 2* in the present report). A more precise overview of the possible combinations of the three dimensions is given in tables 3.1 and 3.2 in chapter 3.

The overall objective of the working committee's recommendations is to facilitate the exercise of a voter's democratic rights and reduce the costs related to this exercise. To reach this objective, one strategy is to allow e-voting in uncontrolled environments for all voters. The introduction of an e-voting system will increase the availability and in the long run reduce the costs related to running an election, and ensure a faster and more accurate counting of the votes. One objection is that e-voting may reduce the formal atmosphere associated with the act of voting in a traditional polling station. The working committee would like to emphasize that e-voting is only recommended as *a supplement* to traditional voting procedures. Traditional voting in polling stations will be maintained in the foreseeable future**.** This means that voters unacquainted with or unfamiliar with e-voting technology will have the right to cast their votes according to traditional practice. It is worth mentioning, though, that the extensive practice of submitting advance votes over the last years has already contributed to changing traditional voting practice[1]. Whichever way the election procedure is run, it is always of vital importance that the voters have confidence in the system and the process.



One possible consequence of introducing the opportunity to vote in uncontrolled environments – whether the vote is cast electronically or manually (for example by post) – is that the right to secret suffrage may be threatened. The voter may be under undue influence (as in for example *family voting*) and the buying and selling of votes may not be precluded. By admitting multiple submissions of

[1] In the last three Parliamentary elections in Norway approx. 20% of the votes have been submitted in advance. See fig 5.1, ch.5.

advance votes, as well as the right to cast a vote again in controlled environments at a polling station, the negative consequences will be reduced significantly, although not avoided completely.

The following sections in the present chapter summarize the main points in the working committee's recommendations:

2.2 Democratic principles and legitimacy (see chapter 5)

Voting outside the polling station – whether e-voting or voting by post – makes the principle of secret suffrage particularly vulnerable. Permitting e-voting in uncontrolled environments on Election Day (phase 2) is in direct conflict with the democratic principle of secret suffrage. To assess satisfactory technical solutions, the working committee therefore assumes that the following conditions are met:

1. Two phases should be maintained in the election: one phase for the submission of advance votes, and one for casting a vote at a polling station on Election Day;
2. E-voting in uncontrolled environments should only be introduced in the advance voting phase.

Voters may of course be exposed to undue influence even if the casting of the vote in uncontrolled environments takes place in the first phase of the election. Buying and selling votes are similarly not precluded. To counter problems of this sort, a *cancellation right* is recommended for those who cast their votes electronically in the first phase. Traditional polling stations are maintained, warranting the possibility of casting a secret vote even if the voter has already submitted a vote electronically once or several times before.
In the second phase a voter can cast his vote only once by physically inserting a paper ballot in the ballot box. A voter who has already cast his or her vote electronically in the first phase, may cast his or her (new) vote again in an approved polling station, either in the first or the second phase. Only the last vote cast is counted.

Given a voting procedure as presented above, there is reason to believe that every voter is given ample opportunity to cast a secret vote without being exposed to any undue influence, even within a system which admits e-voting in uncontrolled environments. Similarly, the buying and selling of votes is precluded: a potential buyer can never ascertain that an e-vote will actually count.

2.3 Legal matters (see chapter 6)

This report includes considerations of national as well as international jurisdiction pertaining to e-voting, including matters related to the specification of provisions for e-voting. Of particular importance are the recommendations of the European Council pertaining to standards for e-voting. According to current Norwegian legislation e-voting is not permitted. The Elections Act (Norway) and its provisions are based on traditional voting procedures by which the voters insert a paper ballot in the ballot box. If e-voting is introduced as an option, the jurisdiction pertaining to elections must be altered. Until such amendments have been formulated, however, opportunity should be given to run pilot projects regulated by provisional legislation.

Although the democratic principle of secret suffrage is not fully consistent with e-voting, legal opinions vary with respect to how the principles should be interpreted in view of Article 3 of The European Convention on Human Rights. The Venice Commission considers e-voting to be in compliance with the European Convention on Human Rights, provided certain provisional measures are taken. In the last instance this question must be answered by national or international legal jurisdiction. Since the legal status remains unclear on this point, in a potential case for the Courts great importance must be attached to experience and practice.

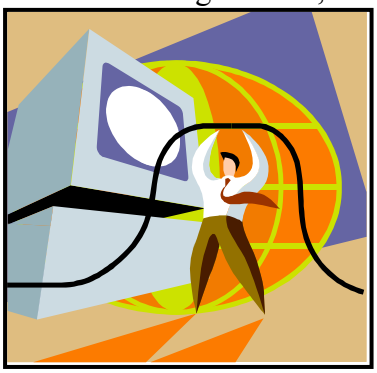
2.4 Economic and Administrative Considerations (see chapter 7)

Considerable economic and administrative resources are required for running elections in Norway. The introduction of modern technology will be of greater interest to the municipality if it reduces rather than increases economic and administrative costs. E-voting will have considerable administrative advantages in so far as the exactness of the results is improved and the final results are quickly arrived at. E-voting will also contribute to the reduction of a number of expensive manual procedures and audit routines. Compared with traditional voting procedures, e-voting in *controlled environments* will require new investments to cover the acquisition of new computer technology, rigging, and a number of new booths, possibly also new premises, which will result in an increased number of staff**.**

E-voting in *uncontrolled environments*, on the other hand, is considered by the working committee to reduce costs on a long term basis.
Pilot project activities, however, will involve a more complex administration and higher costs since electronic solutions are offered in addition to traditional voting procedures. The working committee therefore recommends pilot activities to be not only administered, but also financed, by the state.

2.5 Technological challenges and possible solutions (see chapter 8)

From a technological perspective e-voting in *uncontrolled environments* faces two substantive challenges: one is to know who the voter is (identification and authentication), the other involves the registration, transmission and counting of the voters' electronic ballots with a hundred per cent accuracy. Voter identification and authentication can be obtained with the help of something the voter *owns* (e.g. a smart card), *knows* (a PIN-code, for example) or *is* (a physical property which may be read off, such as for example the voter's finger print or retinal pattern). The working committee is of the opinion that e-voting specific identification procedures should be avoided. At present PKI solutions have been chosen at security level "Person High" for electronic communication with the public sector.



The working committee is of the opinion that the technology currently used in uncontrolled environments does not provide a sufficient level of security with respect to registration and the transmission of cast votes. However, there is good reason to believe that better solutions will be available on the market in due course.

The working committee suggests that a voter should have the right to withdraw a ballot that has been cast electronically in an uncontrolled environment. A cast ballot may be cancelled either by the submission of a new electronic ballot, or by the submission of a vote by traditional procedure in a polling station on Election Day. In order to make this feasible, each electronic ballot must be linked to the voter's identity and the link must be maintained until the vote can no longer be cancelled, but the content of the vote must be sealed (this may be achieved using encryption). This places special security requirements on the routines related to the handling of e-votes, to be elaborated on in chapter 8.

2.6 Control and approval (see chapter 9)

To secure safe technical solutions in a remote e-voting system, and to ensure the voters' confidence in the system, the working committee recommends an independent body, appointed by the electoral authorities, to assess the system's operability and the system providers' compliance with appropriate security standards.
This means that any *person* or *body* appointed to certify and approve system providers and technical solutions on behalf of the electoral authorities (accredited certification bodies) should be subject to certification. Furthermore, any *procedures* or *routines* to be followed by the providers of e-voting solutions should be subject to accreditation by accredited certification bodies. The electoral authorities can *only* choose accredited providers whose technical solutions for e-voting have been accredited/certified with respect to the critical parts. *Technical equipment* and *technical solutions* should also be subject to certification. As a rule, no piece of non-certified equipment should be used in the system. Critical parts of the technical solutions *must* be certified.

The solutions recommended here will imply a change from a layman approval to a professional approval of our election system. This will affect the election system as a whole, with respect to its administration and audit procedures as well as to the competence required. The recommended solution requires the formulation of requirement specifications for e-voting in Norway. Before a *de facto* standard for e-election is provided or a law and legal provisions are set forth, specifications must build on the legal, operational and technical specifications provided in the Recommendation of the European Council, including the amendments provided in chapter 8 of this report.

The working committee bases its recommendations on the assumption that current, established routines for audit and approval are maintained during the pilot project period. An essential task for the new project group recommended in chapter 10 will be to work out new routines (cf. discussion in chapter 10). A provisional solution is to have this project group take the responsibility of approving the technical solutions.

2.7 Long term goals and offensive investment

For e-voting in uncontrolled environments to be feasible, it is all important that strict security measures are taken that do not negatively affect the voters' confidence in the system. Current technology does not warrant this level of security. For this reason, the working committee does not at present recommend the introduction of full-scale e-voting. The committee's recommendation should be seen as the beginning of a long-term objective.

Notwithstanding, it is not inconceivable that there will be a considerable pressure to introduce remote e-voting in uncontrolled environments. This may take place as the result of a constantly growing use of information and communication technology in society as a whole, or because e-voting is introduced in other countries, or because there's a drastic fall in voter turnout. The working committee is of the opinion that e-voting in uncontrolled environments should *not* be made generally available without thorough prior testing, and the committee therefore wants to emphasize the need for an aggressive government initiative to carry out a number of pilot projects and tests. Well-planned test projects and systematic evaluation should be carried out as soon as possible, the aim of which should be twofold:
In part to test various technical solutions, in part to enhance the voters' confidence in voting by electronic means.

2.8 Step-by-Step Introduction (see chapter 10)

The working committee recommends a step-by-step process in which e-voting is tested systematically. Testing does not have to be performed in connection with regular elections. Rather, controlled experiments may be carried out on selected, pre-defined groups of voters. One type of test will be related to user interfaces. Other tests may be more suitable in conjunction with local referendums. The choice of testing ground should primarily be guided by considerations such as easy handling and potential efficiency gain. Tests conducted in conjunction with real elections should be performed in three steps:

2.8.1 Step 1

The first step relates to e-voting in controlled environments. Step 1 may be performed in controlled environments with secure networks and computers provided with security logs. The voter submits his or her ballot with the help of a computer in an approved polling station controlled by election officials. The security log ensures that the votes are stored and not lost in the event of a breakdown or an error affecting the e-voting system. Given that the computer used by the voter can be secured (for example by using a separate CD-ROM to start the computer) tests may also comprise voting in uncontrolled environments, in which case the pilot should be restricted to non-binding elections, such as local, consultative referendums. The objective of these pilots is to test user interfaces, technical solutions and the voters' confidence in using the various solutions.

2.8.2 Step 2

After systematic assessment of the experience gained from step 1, the next natural step is to test small-scale e-voting in uncontrolled environments for special groups of voters (citizens residing or staying abroad, voters with disabilities or voters in a single municipality). In step 2 experiments with controlled computers in uncontrolled environments may be conducted also for legally binding ballots. Testing related to uncontrolled computers in uncontrolled environments should be restricted to non-binding elections (see also chapter 10).

2.8.3 Step 3

Provided the test results in step 2 have been found satisfactory, the next step is to gradually expand the pilots to include e-voting in uncontrolled environments using uncontrolled computers for legally binding elections, and to make this option available to a steadily larger group of voters.

2.9 Central control and audit arrangements

Before e-voting pilots are conducted, a project group should be appointed to have the overall responsibility for planning, conducting and evaluating the pilots. Furthermore, an accredited certification authority should be established to approve requirement specifications, including audit, control and operation. This relates to the accreditation of certification authorities, the approval of system and service providers' procedures and routines, and the approval of technical equipment and technical solutions.

If e-voting is introduced as an alternative during regular election proceedings, the working committee would like to emphasize that some of the project group's tasks will be of a long-term and enduring nature. This may suggest the establishment of an electoral commission whose responsibilities may include election planning and proceedings. Considerations of this kind may await further experience gained by the project group.

3 Elections – a complex affair

3.1 Introduction

This chapter considers electronic voting in a larger setting, and is intended to demonstrate the complexity of the election process in all its phases. Furthermore, advantages and disadvantages of e-voting will be seen in the perspective of three major dimensions in which election processes may be analysed.

Free, equal and secret suffrage is fundamental for a democratic political system. But these privileges are not sufficient conditions for a democracy. Examples abound of non-democratic regimes that run elections to strengthen the support of their own population and the international public opinion[2]. This demonstrates how important democratic elections are to obtain the people's confidence in their political system and for the people to support their political leaders.

Political elections are run at different geographical levels. Norway has four different political elections: election for the National Parliament, (the Storting), for the County Councils (regional), for the Municipal Councils (local) and for the Sami Assembly. Elections are strictly regulated by law, pertaining to who is entitled to vote, who is eligible as a candidate, how a vote is submitted, how the polling districts are divided, how many representatives can be elected and how the seats are allocated relative to the votes cast for the individual candidate lists. The principle of "one voter – one vote" is fundamental, but the additional principle of "one value" i.e. that each vote has the same value, is not equally fundamental. The distribution of seats relative to the number of voters in each polling district may not be fully proportional (Aardal1997). This is the case in Norway. Furthermore, there are special rules laid down in separate provisions for the Sami Assembly elections, regarding voters' register, voting procedures and the counting of votes. However, many of the problems we touch upon in the present report are relevant for all types of election.

3.2 The voting process

A voter will probably associate an election with what goes on in the polling station, but an election does in fact consist of a chain of procedures. Simplified, the procedure may be divided into three stages: 1) the pre-voting stage (preparation), 2) the voting stage (the casting of the votes) and 3) the post-voting stage (counting, auditing and reporting). Each stage may be further sub-divided into several phases. In order for the analysis not to be too detailed, the phases presented below may suffice to give an impression of the complexity of the process:

[1] Although elections run by non-democratic regimes may observe the principle of secret suffrage, they always break the principles of equal and free suffrage.

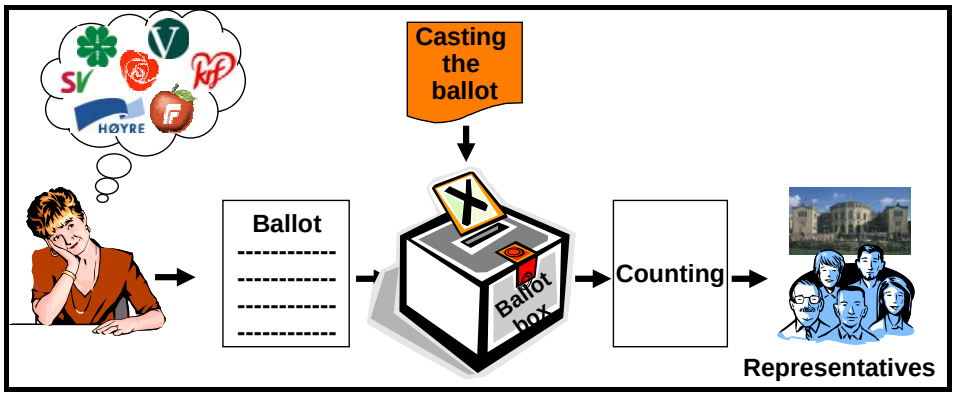


Figure 3.1: Stages in the voting process

3.2.1 Producing and maintaining a voters' register

All entitled voters in Norway are registered in the voters' register of the municipality in which they hold residence as of 31 May of the election year.[3] The municipalities own the registers and collect information from the Population Registry. The municipal authorities may decide to have a computer company provide an electronic register to be used during the pre-voting stage. Norwegian citizens who have resided abroad for more than ten years must apply for inclusion in the voters' register to be entitled to vote. Based on circumstances laid down in the provisions relating to elections, the voters' register may be amended up until the polling stations open on Election Day. When a person is registered in the voters' register, he or she is entitled to submit a vote either as an advance vote or as a vote cast in the ballot box in a polling station on Election Day. Electronically updated registers form the basis for the paper printed registers used on Election Day, in which all the advance votes submitted are crossed off. The paper copy of the voters' register is printed after the advance voting period has been closed.

3.2.2 Checking candidate lists

The voters' register and the Population Registry are used by the Electorate Committee when they approve the lists of candidates presented by the political parties. Candidate lists from parties and groups standing for election are to be handed in to the electoral authorities who take the responsibility for approving the lists in compliance with chapter 6 of the Norwegian Elections Act. Among other things the candidates must be eligible and the lists presented must be signed in accordance with the provisions. The number of signatures needed depends on whether the list comes from a political party already receiving a certain amount of support from the voters or whether it comes from some other group or party. In the first case the list must be signed by two persons, while in the latter case it must be signed by 500 persons in order to be an approved list for a parliamentary election at the national level or a County election at the regional level. In the case of elections to the Municipal Council (local level) two per cent of the entitled voters in the municipality must have signed the list in order for it to be approved by the authorities.

Parties included in the Register of Political Parties may send in electronic signatures, given that digital communication with the municipal authorities or the county authorities is available. Signatures collected from groups or parties with a certain amount of support from the voters are to be handed in on paper, cf. provisions laid down in the Elections Regulations,

[3] A voter for the Sami Assembly must personally register in the Sami voters register before his or her first participation in an election for the Sami Assembly

Article 13. In accordance with the provisions these groups do not have the opportunity to collect signatures electronically. The provisions also state that these signatures are under secrecy, and are not to be made public. To have signed a proposed list of candidates is a piece of information about "a person's privacy", which means that secrecy must be observed, cf. the Administration Act, article 13 (1). The electoral authorities check the list of candidates against the voters' registers and the Population Registry for control and approval of the proposed lists. All approved lists are printed as ballot papers for the election in question.

3.2.3 Preparing the polling stations

Some of the preparations that are not really visible to the individual voter relate to setting up and organizing polling stations for advance voting as well as for voting on Election Day. Furthermore, election officials must be recruited and trained for their jobs. These preparations require considerable manpower and financial resources.

3.2.4 Voter identification

The Elections Act in Norway enables a voter to submit his or her ballot before Election Day, i.e. the voter is entitled to cast an advance vote. During the time period set for advance voting the municipalities receive votes from different voting channels. The municipal authority establishes premises on which advance voting may take place. Advance voting is also organized in health institutions and social institutions, and provisions are made for so-called ambulatory voting (voters who cannot cast a ballot at any of the assigned premises may apply for permission to vote where they are). Some counties also provide the opportunity for advance voting in secondary schools, colleges and universities. Advance votes are also received by post from other municipalities, from Svalbard and the Island of Jan Mayen, as well as from abroad. Under special conditions a vote may be submitted in a letter sent from abroad (voting by post). As the advance votes are coming in, the Electoral Committee checks them for approval and crosses them off in the voters' register. On Election Day a voter must cast his or her vote in the municipality in which he or she is registered. The voter may, however, cast his or her vote in *any* polling station in the municipality of residence. Particular routine requirements are placed on the authorities to keep records of cast votes. The voters' register is used to keep records of advance votes as well as votes submitted on Election Day. A separate paper copy of the voters' register is produced for each polling district. This register contains a list of the names and birth dates of the voters who are entitled to vote in that district only.

The election official receiving the vote may demand that the voter identify himself/herself before he or she inserts the ballot in the ballot box. The voter is crossed off in the register as the voting is approved. Register records are kept to prevent a voter from casting multiple votes. Voters who have submitted an advance vote may not vote again on Election Day, according to Norwegian law. Votes from voters, who choose to vote in a polling station outside his or her assigned polling area, require special treatment. The voter personally inserts the ballot of his or her choice in a ballot paper envelope, which is then put in a cover envelope with the voter's name on it. The paper copy of the register in which this voter is listed, is in a different polling station, and to prevent multiple voting, this vote must be kept separate. After the polling stations are closed, these votes are controlled against the register in the voter's polling district. Only when it is clear that the voter has not been already crossed off in the register, can the ballot be approved.

3.2.5 Casting a vote

As already mentioned a voter may submit an advance vote in his or her home district or at some other address assigned for this purpose. In accordance with current legal provisions a voter may not make a second opinion, i.e. withdraw the ballot already cast and vote again, unless formal errors have been detected. When advance votes are submitted, they are inserted in a ballot paper envelope. This envelope is placed in a cover envelope along with the voter's polling card. Advance votes are opened and counted on Election Day before the polling stations are closed. When votes are cast in the polling stations on Election Day, the ballots are inserted in the ballot box directly, without any envelope, unless the voter submits his or her ballot in a polling station outside his or her assigned polling area in the municipality.

3.2.6 Maintenance and transportation of cast votes

Advance votes and votes submitted on Election Day must be stored in a secure place until they can be transported safely to the counting station. The duration of storage and transportation may vary, but must be taken care of in a safe and secure manner. Regulations to this effect are laid down in the Elections Regulations, Articles 33 and 34.

3.2.7 Counting and audit

The process of settling the voting results may be divided into three phases: counting (provisional and final), seat allocation and the returning of members. Today most countries make a provisional count at the polling stations immediately after the voting period is closed. The provisional counting of the advance votes is administered by the Electoral Committee. Final counting of advance votes and votes cast during the voting period normally takes place centrally in the municipality, under the supervision of the Electoral Committee. At elections for the Municipal Council the calculation of seat distribution and the returning of members are performed by the Electoral Committee. At Parliamentary elections and elections for the County Council the votes are collected from each municipality for control and a final counting by an Electoral Committee for the County. The members of this Electoral Committee are responsible for calculating the seat allocation and the returning of members for the County Council. Approval of the election results takes place in the County Council. The Electoral Committee of the county is also responsible for calculating the seat allocation for district representatives to the Storting. As for calculating the allocation of seats at large, this is done by the national Electoral Committee. Parliamentary elections are approved by the Storting. The tasks of settling the results of the election, including final counting, seat allocation calculation and the returning of members are automated in many municipalities, as optical counting systems and terminal-based registration have been available.

3.2.8 Reporting voting results

The last stage in the election process consists in reporting the voting results in the form of statistical reports on the number of votes, the calculated mandates, representatives and vice-representatives nominated etc.

Looking back on the simple three-stage model presented in the introduction of this chapter, the reader will see that subsections 1-3 above relate to the pre-voting stage, subsections 4-5 to the voting stage and subsections 6-8 to the post-voting stage. However, it should also have become evident that the different activities often cross over into more than one stage.

3.3 The ICT society

Traditionally, running an election has been a manual and work intensive operation. In recent years, however, computer terminals as well as optical readers have been put to extensive use for voter registration and the counting of votes. Information and Communication Technology (ICT) has also been introduced for voter registration, for seat allocation calculation and for statistical reports (minute books). Up until the present, modern technology has been used by the electoral authorities, not by the voters. Using modern ICT to simplify the administration and to increase cost efficiency is a non-controversial issue, and will continue in the days to come, even if such procedures certainly imply certain challenges with respect to the concurrent centralisation of the control and approval of technological hardware and software. These challenges deserve closer examination and should be considered by the project group in the future.

Increased use of ICT is an important aspect of a modern society. The availability and use of ICT increase in all areas. According to a TNS Gallup Intertrack-poll more than three million Norwegians over the age of 12 have access to the Internet as by August 2005, and more than two million people make daily use of it. The number of people in the latter group is growing. A great number of people have already made it a matter of routine to pay their bills, send in applications to public authorities, send in their tax returns and make purchases over the Internet. Over a very short period of time the individual citizen has grown accustomed to, or is getting accustomed to (or for some: are forced to get accustomed to) the Internet as the central source of information and the central channel of communication on a personal level as well as on a professional and a public level. This fact may, in turn, trigger an expectation from the citizen that private and public services be available on the Internet in a simple and direct fashion.

3.4 Electronic voting

Wouldn't it, then, be a matter of course that the citizens be given the opportunity to cast their votes over the Internet – from their computers at home or at work? Voting is a very simple task once a voter has decided what politician or political party to vote for. For a voter an election for the parliamentary Storting means to decide on an already approved list of candidates and submit it in the right place. Local elections give a few more options, such as the right to attach a personal vote to one or more candidates on the list. On a computer the task will consist in marking one's choices on a checklist or marking one's suggested changes for one or more candidates and then push the send-button. This may be done from any geographical site in the country – or any place in the world for that matter. The voter does not have to meet personally in his or her home district. The availability increases drastically for the student living away from home, for the disabled who have problems moving from one place to another, for the vision impaired, for citizens temporarily living abroad or travelling. Availability is an important aspect of a democratic society. The term *entitled* voter has been chosen for a reason. To be entitled to vote is a democratic privilege. At a time in which voter participation is decreasing in many countries, the option to vote over the Internet may certainly strengthen participation, not least among voter groups whose participation is known to be low, such as the younger generation. Moreover, the counting of the votes and the seat allocation calculation will be very fast and accurate. Given the correct computer programs, manual mistakes in the counting of the votes will more or less disappear, and the costs related

to running an election, both with respect to human resources and other resources, will be reduced.

But is it this simple? A comparison with bank transactions over the Internet is interesting, but does not quite hold water. When a bill is paid over the Internet, both the sender and the receiver may control the correctness of the transaction at any time by checking the transcripts of the accounts and the payments. In a voting system, the principle of secret suffrage makes this type of control and verification impossible. A voting system must be designed in such a way that no doubt whatsoever may be raised as to the registration and counting of every single ballot cast, so that the voter is guaranteed that he or she has contributed to the final result in a correct manner. At the same time it must never be possible to reconstruct the content of any voter's ballot and link it to the voter who cast it. An e-voting system will be more complicated than a traditional paper ballot system that the layman can understand and control. Only people with expert knowledge can understand the operations performed in the computer and the computer network. The voter's confidence in layman control will have to be replaced by confidence in the expert – that is, the experts who have designed and implemented the systems and the experts who certify and verify the complete and proper operation of these systems.

At the same time it is important to keep in mind that a manual, paper ballot system is not foolproof. Operational mistakes are reported from individual voters from time to time (see chapter 5 and appendix D of this report). For the lack of training, faulting routines or cheating, human errors may result in votes being lost, not counted or disclosed. However, even though we know that mistakes occur, Norwegian voters have great confidence that the elections are run properly and that the results are correct. An electronic system may be exposed to deliberate or unintended errors, which may seriously affect the voting results. A computer breakdown due to power failure or some other failure may have the effect that votes have been lost, the computer(s) in the receiving end may be blocked because they are bombarded with other tasks, somebody may intervene and get hold of the vote while it is being transported over the network, and change it, the network may be tapped, a virus or Trojan horses in the voter's system may occur (cf. Security Challenges in Appendix B, and the terminology list in Appendix E).

One important difference between manual and electronic voting systems is this: for the operation to be seriously harmed, a manual system would require a number of people spread in a number of polling stations to do the harm, while for electronic voting a lot of harm can be done by one single person. Even more problematic is the fact that deliberate or unintended irregularities in the system may be hard to detect. Even if no mistake has been made, only a *claim* to the contrary may cause a total loss of confidence in the process as well as the results. Although counterattacks may be mounted, absolute security cannot be guaranteed. Confidence in the voting system is of utmost importance. Even if mistakes occur in manual systems, people are confident that fraud does not occur. This confidence should be maintained when modern technology is put to use, whether in administrating the election or in the voting process.[4]

Another important factor to take into account is the unbalanced access to and use of information and communication technology, known as the digital divide (Norris 2001, Van Dijk 2005, Rønning et al. 2005). This type of inequality not only relates to technology access,

[4] Even in well established democracies like the US, confidence in the way the elections are run may be rather meagre (Fund 2004).

but also to the competence and confidence needed to use the technology. Although the number of people having access to the Internet is very high, the distribution of the groups of people who operate the new technology with confidence is uneven. Young men with higher education are the most frequent users of the Internet. The same group has the greatest confidence in their own understanding of this technology. Internet access and use also correlate with the level of income. Norwegian research shows that people with higher education and a good income are more favourable to voting over the Internet than other groups of people (Karlsen, Aardal and Christensen 2005). Swiss pilot projects on electronic voting report similar results (Cristin and Trechsel 2004). Voting over the Internet, therefore, may attract very resourceful people and strengthen their participation, only to increase the difference between more and less resourceful voters. On the other hand, voting over the Internet may also result in a more even distribution of voters in different age groups.

3.5 Central aspects of the voting procedure

The aim of the present report is to consider different aspects of electronic voting. To help the ensuing discussion, we present the different phases of the voting process along three dimensions: First, a division is made between traditional paper ballot systems and electronic systems. An electronic system does not necessarily imply voting over the Internet. There may be different automated systems or kiosk solutions in which the vote is cast in a terminal, much like a cash machine, in the polling station. This type of solution was tested in three municipalities in Norway during the 2003 municipal election (the municipalities of Oppdal, Larvik and Bykle) as well as in the election for the local political administration in Svalbard in the same year.[5]

The second division is made according to where the vote is cast, whether in the polling station under the supervision of publicly appointed election officials or in a place where nobody can control the way in which the vote is cast, whether at home or at work. The first type of case will be called voting in controlled environments, the other type is voting in uncontrolled environments. The reason for an election to be under public supervision is to secure secret suffrage and to secure that a voter chooses his or her ballot without undue influence from others. A case of coercion or undue influence would be one in which for example a family member forces another member to cast a given vote (so-called family voting), or if somebody is willing to buy or sell votes. Table 3.1 combines the two dimensions presented above.

[5] Cf. Christensen et al. 2004. Cf. also chapter 4 of the present report.

Table 3.1: Voting according to medium and environment

	Controlled environments	Uncontrolled environments
Paper	**1.** Traditional paper ballot in the polling station	**3.** Casting a paper ballot outside the polling station (voting by post)
Electronic	**2.** Electronic equipment in the polling station (computer with a touch screen, mouse or keyboard)	**4.** E-voting outside the polling station (Internet, SMS, etc.)

Source: (Karlsen et al. 2005)

Cell 1 relates to the traditional voting procedure. Cell 2 relates to the type of project tested in the 2003 election with electronic terminals in the polling stations. Cell 3 relates to paper ballot voting outside the polling station. In accordance with Norwegian legislation voting by post is an alternative, but only as an exception for Norwegians residing abroad.[6] The exception is the result of striking a balance between the voter's right to participate in the election and the principle of secret suffrage.[7] In some countries, like England, voting by post is practiced extensively. As of 2006 postal voting is introduced in Sweden as a regular option for expatriates.[8] It is important to take into consideration that voting by post takes place in uncontrolled environments, not supervised by an election official. Cell 4 relates to the most controversial voting alternative, i.e. that a vote is cast electronically outside the polling station, over the Internet, SMS or a similar system.

Beyond questions relating to paper ballots vs. electronic ballots, and to controlled vs. uncontrolled environments, there is yet another dimension which may be important for the question of electronic voting. It is a question of *when* the voting takes place. Later in this report it will become evident that electronic voting may have different effects if it is introduced for advance voting than if it is introduced as an option during the voting period on Election Day. In this report advance voting is referred to as *phase 1*, voting during the voting period on Election Day is referred to as *phase 2*.

The main alternatives in table 3.2 below are the same as in table 3.1. However, a division is made between the two time periods of the voting, either before or during Election Day. The opportunity to vote more than once is important to prevent undue influence and trading, as will become evident in the discussion in chapter 5. However, having the opportunity to cast an electronic vote in uncontrolled environments in the voting period in addition to having the opportunity to vote again in the same voting period, will lead to serious technical and

[6] The Elections Act, section 8-2, subsection three states that "Where an elector who is outside the realm has no possibility of going to a returning officer, the person in question may cast his or her vote by letter post without the presence of a returning officer at the casting of the vote."
[7] Voting by post, then, is a different voting procedure than advance voting in the Post Office, as is an alternative in some countries.
[8] Sweden also emphasizes that they have had to strike a balance between the voter's right to vote on the one hand and the principle of secret suffrage on the other (SOU 2004:111).

administrative problems. The alternative in cell 8 below, therefore, is not considered a real alternative.

Table 3.2: Voting according to medium, environments and time

	Controlled environments (in the polling station)		**Uncontrolled environments (outside the polling station)**	
	Paper ballot	Electronic ballot	Paper ballot	Electronic ballot
Phase 1 Before the voting period	**1.** Traditional paper ballot in the polling station	**2.** Electronic equipment in the polling station (computer with a touch screen, mouse or keyboard)	**3.** Casting a paper ballot outside the polling station (voting by post)	**4.** E-voting outside the polling station (Internet, SMS, etc.)
Phase 2 During the voting period	**5.** Traditional paper ballot in the polling station	**6.** Electronic equipment in the polling station (computer with a touch screen, mouse or keyboard)	**7.** Casting a paper ballot outside the polling station (voting by post)	**8.** E-voting outside the polling station (Internet, SMS, etc.)

The discussion in the following sections focuses on the non-shaded cells in table 3.2 above, i.e. cells 2, 4 and 6, in accordance with the working committee's mandate. However, it is important to take into consideration that many of the objections which may be raised against electronic voting are not primarily related to the use of an electronic medium as such, but to the fact that the voting takes place in *uncontrolled environments.* It may be argued that once the opportunity to vote in uncontrolled environments is provided for, electronic solutions are safer than paper based solutions. Electronic solutions provide better identification and authentication procedures, and the opportunity to re-cast a ballot prevents potential problems in the form of coercion or undue influence or trading.

The reader is referred to the classification in table 3.2 above in the following discussions.

3.6 Electronic voting: experience from abroad

The discussion relating to electronic voting is not uniquely Norwegian. Several countries are testing different technological solutions provided for voting in elections. The need for cooperation and common regulatory practice across national borders has been felt in many countries. The European Council, under the long-term project "Making democratic institutions work", has invested serious efforts in working out guidelines for democratic practice. As part of that project the Committee of Ministers of the European Council, 30 September 2004, adopted a Recommendation relating to legal, operational and technical

standards for electronic voting.[9] In the closing document from the project[10] the Council recommends voting opportunities outside the polling stations, either by post or electronically. Until electronic voting is generally accepted, electronic solutions are recommended as a supplement to traditional voting practice. Generally, voting by post should be introduced before electronic voting, and voting opportunities should be simultaneously available outside and inside polling stations.

The idea of providing opportunities for voting in uncontrolled environments, in other words, is well known in influential, international circles. Before we proceed in the discussion, however, we will report on test projects from some other countries relating to different types of electronic voting, and the experience drawn from them. This is the topic of chapter 4.

[9] A Recommendation of the European Council is a legal instrument which must be unanimously approved by the member states, but it is not binding from the point of view of international law. Its standards may not be made legally binding in Norway unless the regulations are adopted by Norwegian law or legal provisions.
[10] *Green Paper: The Future of Democracy in Europe.*

4 Electronic voting – experience at home and abroad

4.1 Introduction

In this chapter we report on the debates pertaining to electronic voting (e-voting) and the experience drawn from various projects related to e-voting at home and abroad. For a first approximation, there are three different perspectives from which e-voting may be considered. One is the negative perspective: that e-voting is not interesting as an option at all. Another is a restrictive perspective: that e-voting may be considered only in the polling stations. The third perspective is the more liberal one: that voting over the internet (VOI) may be considered in uncontrolled environments.
E-voting in the polling stations has been practised extensively in the US, Belgium and the Netherlands, Brazil and India. Voting over the Internet (VOI) is less common, and has been met with greater scepticism. VOI tests have been carried out in connection with local elections in the UK (2002, 2003) and in Estonia (2005) as well as in connection with national referendums in Switzerland.
The attitudes to e-voting, in other words, vary a lot, and should be seen in relation to the different political traditions in these countries and particular characteristics/features of their political development. Countries enjoying strong voter participation and whose population has great confidence in the legitimacy of the elections, such as the Nordic countries, have attached little interest to electronic voting. Countries, in which voter participation has been relatively weak, have shown greater interest. Traditions of running frequent elections and referendums, as in Switzerland, and complicated elections, as in Belgium and the Netherlands, contribute to increased interest in e-voting.

There is a considerable amount of literature on the subject of e-voting, in the form of reports, books and scientific articles. This working committee has taken the literature as basic for their task, and used it as background material for their study tours to the US, the UK, Geneva and Estonia. The study tours thus supplement and extend the experience drawn from the written sources. This chapter relates to the tasks defined in points17 and 18 of the mandate, repeated below:

- Summon reports and research done in this area (17)
- Give an account of the experience drawn on different types of voting system in other countries (18)

We start by focusing on the positions taken in our neighbouring countries and relate them to the Norwegian experience. We then turn to the UK where experimental e-voting has been made an integral part of a major modernisation process. We then focus on the experience drawn and the debates going on in the US, where e-voting in the polling stations is widely used, but where VOI is met with great scepticism. Switzerland and Estonia have both run VOI experiments during official elections. We look into these experiments more closely before we report on e-voting experiences in other parts of the world towards the end of the chapter.

4.2 The Nordic countries

The Nordic countries, Sweden in particular, have shown little interest in e-voting. Discussions in Sweden appear in many public documents, but they all conclude by not recommending e-voting (Olsson 2001, Ju2002E, SOU 2004: 111). The Swedish voters have great confidence in their elections, and voter participation is very strong. A fear is felt that the introduction of e-voting may ruin an already well functioning system. In their closing report, the committee appointed to re-consider the Representation of the People Act in Sweden, do not recommend e-voting as an option for the voters in official elections at present. They point to problems related to the principle of secret suffrage, risks of fraud and undue influence as well as to security problems related to the technology (SOU 2004: 111, pp175-185).

Denmark is not at the forefront either in this matter. Although electronic solutions have been tested in some local referendums, no initiatives have been taken by the authorities.

In Finland the opinion is more positive than in Sweden and Denmark. In the fall of 2005 an officially appointed working committee gave their recommendations to a gradual introduction of e-voting in controlled environments. A pilot project on e-voting will be run in three counties in Finland during the 2007 parliamentary election. The working committee argues in favour of e-voting on the grounds that it will increase voting accessibility, reduce administration load and save costs. E-voting is discussed as an integral part of a larger project in the Finnish Ministry of Justice initiated to reform the computer system for elections[11].

Norway has run four pilot projects on e-voting in controlled environments, as mentioned in the previous chapter. These projects are described in more detail in the next section

4.2.1 The Norwegian experience

Experiments were run in the three municipalities of Oppdal, Bykle and Larvik during the regular local and regional elections on 15 September 2003. An experiment was also run during the election for the local political administration in Svalbard on 26 and 27 October 2003. The technological solutions, delivered by ErgoEphorma, a firm specializing in ICT solutions, were identical in all four places.

The voters were provided with the opportunity to cast their ballots through an electronic ballot box instead of casting a regular paper ballot in a traditional ballot box. The electronic ballot box was designed as a computer with a touch screen, much like a minibank terminal. The electronically submitted ballots were counted as regular ballots in the election.
The Oppdal experiment was more comprehensive than the rest. Oppdal municipality has almost 5000 voters, and the electronic option was available in all of the seven polling areas in the municipality.
The municipality of Bykle, on the other hand, is very small, counting just under 700 voters and only two polling districts. Electronic voting, however, was available in both.

The municipality of Larvik has a higher population than the other three, counting almost 32000 voters, yet the electronic terminal was set up in only one voting district, albeit a big one counting about 4000 voters. All the voting districts providing the electronic option had just one e-voting terminal each.

[11] http://www.vaalit.fi/21331.htm

In the Svalbard experiment there were about 1300 voters, a single polling station and two e-voting terminals. The voters could opt for a paper ballot, but had to request this personally to be given this option. E-voting was the regular mode of voting in this election.

The voting proceeded as follows:

The voter was identified by placing his/her smart card in the reader, and was then able to start the process of casting his or her vote. The first image on the screen invited the voter to identify which election he/she was taking part in: the local election or the regional election. This was done by a touch on the chosen image on the screen. The voter then touched the image of the party he or she voted for. The next step was to attach one or more personal votes by touching the name of one or more candidates of their personal choice. As the voter touched a candidate name, a ticker to the left of the name was automatically crossed off. The same procedure was used for the local and for the regional election.

The election for the municipal council also provides the opportunity to submit a personal vote for one or more candidates from a different list. If a voter opted for this choice, he or she had to enter into an alphabetic list of candidates or to search in the lists of candidates from the different parties. The voter also had the opportunity to submit a blank vote in one or both of the elections, or he or she could choose to cast a vote in only one election. The opportunities given to the voters to attach a personal vote on a regular ballot paper were the same for the e-voters. In other words, the same opportunities were given in the electronic mode as in the regular, paper ballot mode of voting.

91 per cent of the voters cast their votes electronically in the Svalbard election. In the municipality of Bykle 53 per cent opted for the e-voting mode. In Oppdal 34 per cent of the voters voted electronically. In the one polling district of Larvik, Østre Halsen, 18 per cent opted for the electronic mode.[12]

The evaluation of the experiments is first and foremost an assessment of the user-friendliness of the technological solution, and the voter responses were of central concern. The technical solution as such was not an issue.

The most frequently given reason for choosing the e-voting option was an interest in trying out something new, to participate in a new and exciting experiment. The voters who opted for the traditional paper ballot were divided in four equally large groups according to the responses they gave. One fourth said they were opposed to the idea of e-voting, another fourth said they did not have the time, the third group thought it would be complicated and the fourth group gave other responses ("lack of information", "don't understand computers" were typical answers).

The data collected in these experiments demonstrate that the voters are generally very positive to using ICT in casting their votes. E-voters, of course, are more positive than non-e-voters. The non-e-voters of the second group answering "didn't have the time", are very similar to the e-voters in their attitude to e-voting. The voters who feared that using the e-voting system would be too complicated also responded favourably to the use of ICT. As expected, the fourth group gave the most negative answers.

[12] Source: ErgoEphorma

Seven out of ten voters who chose the e-voting option were favourable to voting over the Internet if this opportunity had been available. More than 50 per cent of those who cast their votes in accordance with traditional practice were also positive to VOI if that option had been provided. Almost nine out of ten who took part in the project found it easy to vote electronically and just as many would use the same voting mode in the future if it was provided.

4.2.2 Do the Norwegians want to vote over the Internet?

During the project period at the local elections in 2003 Norwegian voters were asked their opinions on VOI if such a voting procedure had been provided. It should be noted that they were not presented with the possible advantages and disadvantages related to this voting option. In sum, six out of ten voters said they would like to vote over the Internet. Among the voters who took part in the poll, important differences were found with respect to the voters' age, their education and their income. While eight out of ten under the age of 44 were positive to VOI, 56 per cent in the age group 45-66 were positive and in the age group over 67 only 18 per cent gave a positive response. Furthermore, while three out of ten with only ten years of schooling would like VOI, 74 per cent with a college or university background were in favour of it. . In the lowest income group about 50 per cent gave a positive answer, while three out of four in the highest income group wanted VOI (Karlsen, Aardal and Christensen 2005).

4.3 The United Kingdom

The whole voting procedure in the UK is going through a major modernization process, in which electronic voting, primarily outside the regular polling stations, is playing a major role. The background for this process is the serious decline in voter participation over the years. In the years 1990-1999 voter participation was on an average 36 per cent, and in 2000 just above 30 per cent. Several experiments on e-voting have been run in the UK, particularly at the local elections in 2002 and 2003. In 2002 nine local authorities ran projects on e-voting, the year after there were twenty of them. The Government allocated 30 million GBP to e-voting projects over a period of three years (The Electoral Commission, 2003). 18.5 million GBP was spent in 2003. The projects included several different system suppliers.

The most important issue for the British Election Commission is the security of the electronic solutions, which must be at least as good as in the more traditional methods. The projects have been launched to make the voting process simpler, to make it as easy as possible for the voters to make use of their privilege to vote. A major task has been to introduce VOI. Fourteen experiments involved VOI as a voting-method. Three experiments have been related to the use of electronic booths in the polling station, while three other experiments have tested new technology in the counting of the votes. Voting by means of an interactive digital TV has also been tested for the first time. In sum an estimate of 160 000 voters made use of an electronic medium. In the subsections below a short description is presented of the various technical solutions that were used.

4.3.1 Voting over the Internet

In the Internet solution the voter was linked up to the web address of a ballot receiver (the role of a returning officer). The voter could get access to the link from any computer with Internet access. The ballot receiver's address was obtained either from the polling card sent to the voter, or from the ballot receiver's home page. The voter logged on with a personal password that he or she received with the polling card (either a PIN code or a password). The

next step was to choose a candidate, either by clicking the ballot paper of his or her choice or by choosing one of the candidate codes attached to the polling card. The voters could opt for a blank vote. In the end the system would present the choices made by the voter, who was then asked to confirm his or her ballot. The process ended when the system returned a receipt to the voter that his or her ballot had been registered. In the evaluation report the election commission remarks that the use of a PIN code created confusion. The various system providers had made use of different authentication procedures as well as different code systems in the same election, depending on which system the voter decided to use. The PIN codes were also sent with the polling card in the same envelope, not in two different ones as is regular practice when credit cards are issued. The Commission report also remarks that information about the link between PIN code and voter identification should be available to the election authorities only, and not to the system providers. Kitcat (2003) who is critical to the experiment points out that the security analyses from the voting stage and the post-voting stage were insufficient.

4.3.2 Voting over the telephone

This procedure gave the voter a telephone number (a ballot receiver) to call, free of charge. The voter was answered by an automatic answering machine. The first step was to log on by pressing a code, then to press the candidate code(s) of his or her choice. The system then returned to the voter by reading out the candidate(s) on the voter's ballot and asking him or her to confirm. The voter could then either confirm or go back and make another choice. As the voter finally confirmed his or her ballot, a voice confirmed that the vote had been registered. The Election Commission is sceptical to this procedure and does not recommend this option for future use. One reason is that the procedure is accessible only to a very limited extent for people with disabilities. Furthermore, the voters were confused by having to press relatively complicated codes. In several experiments the voters had to press the number codes as they read them off the polling card.

4.3.3 SMS

The SMS solution, in contrast to the previous solutions presented, is not interactive. The call, furthermore, was not free of charge for the voter. The casting of the vote took place in one single message, which in order to be approved had to contain the voter's code, the code for the voter's polling district and the code for the chosen candidate(s). If the message was approved, the voter got a return message that his or her ballot had been registered. The return message did not identify the voter's choice. An error message meant that the ballot was invalid. The Commission is sceptical to the procedure. The solution is not a viable option for many of the disabled, and the procedure makes the act of voting too trivial

4.3.4 Digital TV and touch screens

Voting by means of a digital TV follows a procedure very similar to VOI. The only difference relates to the method of logging on to the voting service (ballot receiver). To log on to the service the voter had to navigate the menu system of the television set, but as soon as the link was made, the same procedure was followed as with VOI.

Kiosks equipped with touch screens were also put up in several places. In four municipalities these kiosks were the only option for the voters to cast their ballots on Election Day, while in five other municipalities the electronic kiosks were set up in centrally located libraries and

supermarkets as an alternative to the polling stations. Most of them were equipped with a touch screen. One municipality had an electronic kiosk solution as an option in addition to the traditional paper ballot system in the polling station. In Sheffield a smart card system was tried out to simplify the registration process (the voter might opt not to use it). The voter received the smart card in the mail before the election. In Chester and in Epping the voter received the smart card in the polling station. In the smart card experiments the cards were encoded with a ballot.

4.3.5 The Election Commission's general assessment of the experiments

The Commission remarks that it has been the responsibility of the Government to set up the contracts with the electronic hardware, software and service providers. A list of sixty one requirements was specified. The requirements covered a wide spectrum relating to aspects of the functionality, security, administration and evaluation of the electronic voting system. As for the operation results, the Electoral Commission has several critical comments to make.

The Commission remarks that no single authority had the overall responsibility of integrating the e-voting solutions in the local ICT systems, one effect being that the security was not sufficiently taken care of. Specified procedures for solving any potential confusion were lacking. Competing system providers had to cooperate on a relatively short term basis without due notice and without a contract to this effect, contributing to serious difficulties in making sufficient, reliable security analyses during the voting period as well as in retrospect.

The Commission also remarks that the local Electoral Committees took insufficient account of the fact that new technology was being used, and levels criticism against the fact that a lot of the responsibility was delegated to the system suppliers. Particular criticism is levelled against the counting procedures in which data was transported manually via e-mail and then imported to Word or Excel applications for counting the results.

The Commission concludes that future solutions for VOI must take account of local ICT systems, and must invest in training local election authorities in the technology. These requirements must be met for VOI to be a correct and secure channel.

The Commission demurs at the quality control of the technological infrastructure. The key issue is verification. The technology should be certified by an independent body to verify the correct operation of the system and to ensure its legitimacy. This means that independent authorities should be able to audit the results, and the system suppliers should provide systems which are open to external inspection and control.

To enhance the usability of e-voting systems, the Commission suggests that the user interface should be standardized. This does not imply that only one system supplier must be chosen, but that the suppliers deliver a standard interface which the voters will recognize as the same in all the voting districts.

Cost has been another of the Commission's concerns. A central argument for introducing new technology is that it may reduce the costs related to holding elections. The Commission emphasizes that cost reduction is highly improbable as long as the voters also can opt for the traditional voting mode in the polling stations. On the other hand, the use of different channels will give the voters more options. Pratchett (2002), who is also concerned about costs, argues that there is a cost reduction potential if the e-voting equipment can be used for other purposes as well. The counter-argument is that it is much easier to control the software

if the equipment is used only for election purposes. Striking the proper balance between the security of the system on the one hand and its areas of application on the other is a matter of fine judgment.

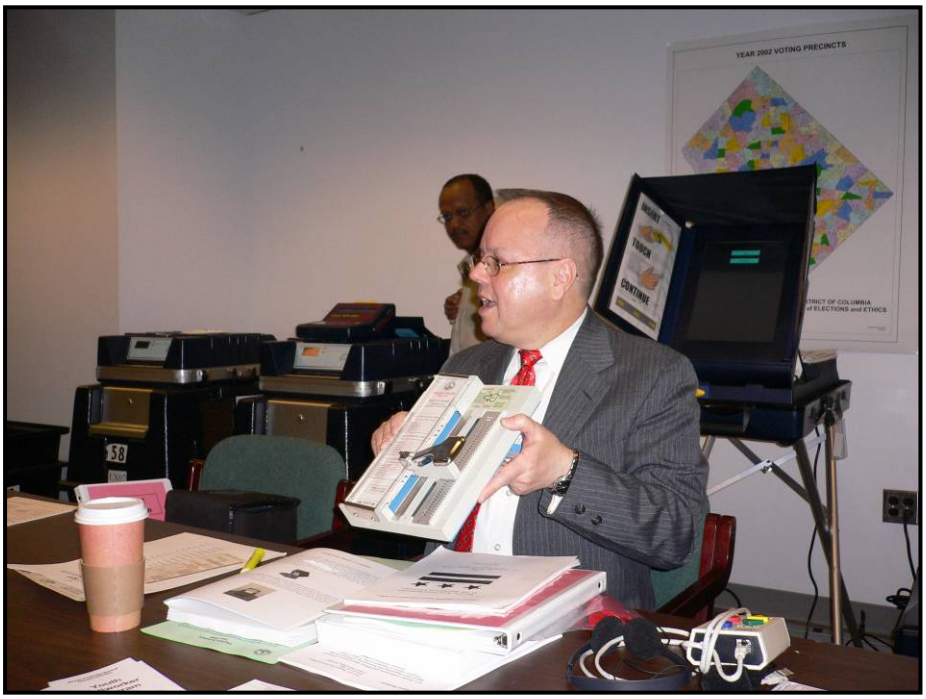
In the opinion of the Commission, the availability of kiosk-operated e-voting systems should be more goal-oriented than was the case in 2003. Their argument is that the availability of kiosks in the polling stations does not increase voter participation. They therefore favour decentralized kiosk solutions (outside the polling stations), particularly in the advance voting period.

What, then, about the stated objective of having an Internet-based voting solution in place by 2006? The Commission is sceptical, and thinks there still is a long way ahead: "pilots should have more demonstrable and rigorous security with formalised accreditation; more mature processes are needed with greater control exercised by local authorities" (Electoral Commission 2003: 81).

4.3.6 Further e-voting projects cancelled by the UK

In the autumn of 2005 the authorities announced that they had decided to cancel the e-voting projects planned for the 2006 local elections for the reason that the time is not yet right.[13]

4.4 The US.



← Bill O'Field from DC Board of Elections and Ethics in Washington DC, demonstrating technological voting equipment.

Electronic e-voting in the polling stations is now the custom in the US. In the 2004 presidential election around 40 million electronic votes were cast. Voting over the Internet, on the other hand, is met with great scepticism.

[13] On September 6, according to the Independent, The Department of Constitutional Affairs had announced that "The Government believes that the time is not yet right to take forward the piloting of e-voting"

Federal legislation on voting in the US is meagre, as it is up to the individual state to introduce e-voting as one or the only option. As an aftermath to the problems that occurred with the punching machines used in the 2000 elections the Help America Vote Act (HAVA) was passed. This Act caused The U.S. Election Assistance Commission (EAC) to be established as "a national clearinghouse and resource for information and review of procedures with respect to the administration of Federal elections." The tasks for the EAC were to provide technical guidelines for administrating Federal elections, to establish procedures for e-voting systems and to develop a federal program for testing and certifying e-voting systems.[14]

The US has come a long way in implementing e-voting systems in the polling stations. The debate going on in the US differs from the discussions in Europe because the US is more sceptical to the security of the Internet. Several computer specialists, Rebecca Mercuri[15] and Aviel D. Rubin[16] in particular[17], have taken a negative stand on the issue of VOI.

Touch screen → for e-voting in Washington DC.

The political opinions on voting reforms in the US are polarized. On the whole, the Democrats favour reforms that enhance voter registration and voter participation, while the Republicans are more concerned with the integrity of the registration and operation of the election.

A technical solution called SERVE was provided for VOI before the 2004 elections, primarily directed at military personnel stationed abroad. An expert group was appointed in 2003 to evaluate the system. A minority group of four members decided to publish their own assessment report (Jefferson, Simons, Rubin and Wagner 2004)[18] , concluding that he solution developed was not to be recommended. The most important threats, they report, are attacks on

[14] Cf. 2005 Voluntary Voting System Guidelines. http://guidelines.kennesaw.edu/vvsg/docs/Volume1Section1.pdf, and a review of NIST in Appendix C
[15] A lot of relevant information and literature references are available on Mercuri's home page http://www.notablesoftware.com/evote.html .
[16] The Working Committee met Rubin during their study tour to the US. A summary report from the meeting is attached in Appendix C of this report.
[17] See Appendix C for more detailed information in this matter, as related in the report from the meetings between the Working Committee and a number of US individuals and organizations.
[18] http://www.servesecurityreport.org

the voter's computer, Internet vulnerability and supplier designed and supplier controlled software.

> *"The vulnerabilities we describe cannot be fixed by design changes or bug fixes to SERVE. These vulnerabilities are fundamental in the architecture of the Internet and of the PC hardware and software that is ubiquitous today. They cannot all be eliminated for the foreseeable future without some unforeseen radical breakthrough. It is quite possible that they will not be eliminated without a wholesale redesign and replacement of much of the hardware and software security systems that are part of, or connected to, today's Internet." (Jefferson, Simons, Rubin and Wagner 2004)*

4.5 Estonia

The idea of e-voting was first introduced in Estonia in 2001.Their vision was to introduce VOI in uncontrolled environments (Dreschler og Madise 2004). Although at first they thought VOI could be operated in the elections of 2002, they had to wait until 2005 for VOI to be a real option in the local elections.[19]

The first objective of VOI is to increase voter participation by maintaining the voters' interest in voting and increasing the interest of the younger generation. The other objective is to keep in touch with modern ICT and make voting easier.

The e-voting system in Estonia exploits the use of a personal ID-card to be held by every citizen in the country. This is a smart card with all the keys and PIN-codes required. The card is intended for use in all transactions that require secure user identification and legally binding signatures, including e-voting.

The Estonian set-up is of particular interest for Norway because it is in line with this Working Committee's vision of how e-voting should be implemented. In the 2005 election in Estonia VOI was made an available option only during the advance voting period. Although the advance voting period lasted for nine days (from the 13th to the 4th day before Election Day), VOI was only available for a restricted period of three days (from the 6th to the 4th day before Election Day). To avoid the buying and selling of votes, and to avoid undue influence, multiple submissions of e-votes were accepted, but only the last vote cast was counted. At first the idea was also to give voters who submitted their vote over the Internet the opportunity to cast their vote on Election Day, as has been suggested by this Working Committee, but this opportunity was dropped to guarantee equal opportunities for all advance voters.

The casting of the vote took place at www.valimised.ee. The voting sites found to be most popular were the home premises, banks, state and municipal government offices and the premises of telecommunication operators. Voting from the home premises required a personal computer with Internet access and with a slot for the voter's smart card.

To separate the vote from the voter, a double envelope system based on an asymmetric encryption system was provided. This system is in line with the system suggested by this

[19] The account of the Estonian elections are based on lectures by Maaten http://www.vvk.ee/english/epp.ppt and Madise http://www.vvk.ee/english/ylle.ppt

Working Committee in chapter 8 of the present report. The separation of voter and vote through decryption was successfully done by means of a strictly secret private key in a ceremonial meeting in the Estonian Parliament at the end of Election Day.

Nine thousand voters voted over the Internet. The distribution of votes over the three days was 3683, 2967 and 3031. In sum these numbers make up just below eight per cent of all the advance votes submitted, which means 1.8 per cent of all votes cast.

The software used has been developed by a private Estonian company, Cybernetica Inc., which was established as an answer to the Estonian initiative to develop competence in the area of data security. The software developed is meant to be so simple that it can be verified that it does not contain any security loopholes. A group of Estonian security experts have made a security analysis[20] on the system and the software specifications. One notable difference between the Estonian and the Norwegian election procedures is that the Estonian ballots are considerably simpler, and the voters have no opportunity add a personal vote. The Estonian voting system makes the electronic solutions easier to handle.

The majority of the politicians in Estonia are in favour of e-voting in uncontrolled environments. Two political parties are against it. Their objections relate to the non-observability of the voting procedure, to the danger of buying and selling votes, and the danger of undue influence. Potential security problems related to the technological solutions are mentioned only as a side problem[21]. However, inquiries show that there are just as many voters for these two parties as there are voters for other parties who are in favour of electronic voting[22].

4.6 Switzerland

Switzerland has between four and six elections/referendums per year. This means that there is a lot more to be gained from introducing e-voting in Switzerland than in most other countries. The country has come a long way in this respect. Possibly due to the frequent referendums the country has suffered from weak voter participation, leading to the introduction of voting by post in 25 of the 26 cantons about ten years ago. To keep up the good results of introducing postal voting, the authorities decided to extend the solution to comprise voting over the Internet. Several empirical studies were made to survey the potential for electronic voting. The surveys showed that VOI was strongly supported by the people. According to a representative group of people 66 per cent of the voters wanted the opportunity to vote over the Internet. Most of the political parties and the political administration were also in favour of e-voting (Geser 2004:80). In 1999 the central authorities established a pilot project on e-voting. All the cantons were invited to participate in the pilot. Three cantons were selected: Geneva, Zürich and Neuchatel. The central authorities covered about 80 per cent of the costs.

Geneva was the first canton to start, mainly because this canton already possessed an electronic voters' register, their Representation of the People Act allowed such a project and voting by post was already established. Also the people were greatly in favour of e-voting,

[20] For documentation related to the system and the security analysis (in Estonian), see http://www.vvk.ee/elektr/
[21] See "Position of the Estonian People's Union Faction of the Riigikogu on the use of the Internet voting outside the polling station", of 15 October.2005
[22] Ülle Madise: http://www.vvk.ee/english/ylle.ppt

along with the politicians and the administration. E-voting solutions have been operated on a total of seven occasions, the last two occasions being on a national level. E-voting has been restricted to referendums and has not been tested in connection with elections to representative bodies.

The Recommendation of the European Council pertaining to e-voting has not formed a basis for the development of the system, although the present solution does satisfy the main principles stated in the Recommendation. The system is not based on the EML standard.[23]

The canton of Geneva received about ten offers for the operation. The solution offered by Hewlett Packard and Wisekey was selected. The first specification required the distribution of a CD-ROM to all voters, but eventually a solution was found based on three separate keys: one to log on to the system, one for the receipt from the ballot receiver, and one for authentication of the vote.

In the advance voting period, a period of three weeks lasting up to the day of the referendum, the voters may vote by post or via the Internet. If the voter wants to vote on the day assigned for the referendum, the voter must meet in a polling station.

A federal referendum was held on 28 November 2005. 41 per cent of the eligible voters cast their votes. Four municipalities provided the Internet option to all their voters, and 23 per cent of the votes cast in these municipalities came in over the Internet. The percentage is the same as in the first six polls which provided this opportunity. The percentage of people opting for this solution is higher among the young people. People with higher education also choose this option more frequently than voters with less education (Cristin and Trechsel 2004).

4.7 E-voting in controlled environments in other countries

4.7.1 The Netherlands and Belgium

The Netherlands has been offering e-voting as an option since the late nineties. When it was first introduced, little attention was paid to the security of the system and to questions relating to how the results were actually arrived at, according to election observers.[24] The usability, in particular for elderly people, was considered more central. During the 2005 election for the European Parliament voters living abroad had the opportunity to vote over the Internet or over the phone.

E-voting in the polling station was first introduced in Belgium as early as 1991, mainly because the traditional voting system is complex and requires counting and audit procedures which are very time consuming.[25] Relevant jurisdiction was in place in 1994, and e-voting was extensive during the elections in 1999, 2000, 2003 and 2004. In 2003, 44 per cent of the voters cast electronic votes (3.2 million voters) .[26] The voting machine is a personal computer with a screen, an optical pen and a magnetic card reader. The ballot box is a personal

[23] The EML standard is described in section 8.7.3
[24] http://www.cs.ru.nl/sos/research/society/voting/index.html
[25] Voting is mandatory in Belgium, up to five elections are run simultaneously, in three different languages. Voters may vote for individual candidates, and there may be up to 87 candidates per list.
[26] se http://www.steria.com

computer with two readers: one to check/control the magnetic card, the other to register the incoming votes.

4.7.2 India and Brazil

Brazil as well as India held elections with e-voting in controlled environments in 2000 and 2003 respectively. The objective here has been to make voting more accessible for illiterate voters. India furthermore has had problems of extensive sabotage related to voting.

Around 370 million Indian voters, (India has 675 million voters), submitted electronic votes in the all-electronic 2004 general election, One million electronic voting machines were distributed in a total of 800 000 polling stations. The machine has the size of a suitcase and consists of two units: The *control unit* was administrated by the polling station staff, while the *balloting unit* was placed in the polling booth. The voters pressed the button next to a candidate's name. In addition, a symbol was provided next to the candidate's name

The investment of 800 000 voting machines amounted to 200 million US dollars. But the authorities will save around 10 000 tons of ballot paper for every future election.

To minimize risks of a virus attack or hacking, the machines were not linked up to a network. Although the election was rated as a great success by the authorities, several critical questions were raised. The machines did not provide any printed receipt, which means that there was no way the results could be trailed. Another critical remark was that the source code was not open for inspection.[27]

Brazil held elections providing e-voting for the first time in1996. At that time electronic solutions were offered only in the major cities. E-voting was extended in 1998 and no less than 400 000 electronic voting machines were provided in the 2000 and 2002 elections.

4.7.3 Ireland

The plans were all set for e-voting by touch screens in the Irish election for the European Parliament and their local elections in June 2004. Test projects had been run in 3 out of 42 voting districts during the 2002 elections, in which 138 011 e-votes were submitted (Laver 2004).

The Evaluation Commission appointed did not recommend the use of e-voting, however, so all plans were stopped pending further notice. The conclusion drawn by the Commission was not based on any findings to the effect that the system would not work. The argument was that the Commission was not *convinced* that it would work.[28]

There are signs, however, that the Irish authorities have not completely given up the idea of running electronic elections. During 2005 initiatives have been taken to run risk analyses and security analyses of their e-voting system. It is unclear whether this will result in the provision of e-voting options in the next election in Ireland.

[27] http://europa.eu.int/ida/en/document/2551/358
[28] See the commission's report: http://www.cev.ie/index.htm

4.7.4 Some minor pilots[29]

France had an e-voting project in the constituency of Brest during the 2004 local elections held on 21 and 28 March that year. The technical solutions were provided by the Dutch Nedap Company. The voters were provided with the opportunity to cast their votes in an electronic ballot box in the polling stations. Another five constituencies took part in an e-voting pilot, but these were not part of the official election. Also, in the elections for the European Parliament on 13 June, 18 constituencies in France took part in pilot projects on e-voting, although not as an integral part of the official elections. The pilot projects were related to the voters' opportunity to submit their votes electronically. Three different solutions were tested in these experiments.[30] E-voting has been legally accepted in France since 1969, and a decree from the authorities on 18 March 2004, authorizing 33 constituencies to run pilots, created new initiatives.[31] In the referendum on the EU Constitution 29 May 2005 e-voting machines were put to use in 60 constituencies. In some of them the votes submitted electronically were also legally binding. 75% of the constituencies used the NedDap Powervote voting equipment. One constituency tested voting machines in which a smart card was used for voter identification.

Spain performed some minor experiments during 2003 and 2004, but ran a larger pilot project in connection with the referendum on the EU Constitution held in February 2005. Two million voters from 52 municipalities were given the opportunity to participate in the experiment, which was run from 1 to 18 February. The referendum was not legally binding. The voters could cast their votes from any computer with access to the Internet, after identifying themselves by using a smart card and a PIN code. A mere 10 000 entitled voters took part in the project.[32]
The 2004 projects were run in connection with the general election on 14 March, but was not an integral part of the official election.[33] SMS-solutions as well as Internet solutions accessible from a personal computer were provided. The computers were placed in the polling stations. The system was supplied by Indra. The company took this opportunity to demonstrate the experiments to a group of invited guests from 27 European and South American countries. Indra also provided the solutions for the pilot in February 2005.

In Portugal more than 9000 voters participated in an e-voting pilot during the elections to the European Parliament 13 June 2004.[34] The pilot was run in nine municipalities selected on the basis of size, political preferences and geographical setting, but it was not part of the official election. The participants were asked to take part after having cast their votes in the election. From a pool of 50 562, 9300 voters accepted the offer. Three different solutions were tested: A touch screen e-voting machine, a light pen system or an electronic card solution. According to the assessment report 93 per cent of the participants said that they preferred this way of voting to the traditional method. Self-selection must be taken into consideration in the assessment of these results.

An experiment was also run in Romania 18 and 19 October 2003 in which military personnel stationed abroad were offered the opportunity to vote over the Internet. The pilot was run in connection with a referendum on the revision of the Constitution of Romania. 97 per cent of a

[29] This section is based on http://focus.at.org/e-voting/countries
[30] Nedap 2.07, Ivotronic and Point&Vote (Indra)
[31] se http://europa.eu.int/ida/en/document/2635/358 og http://europa.eu.int/ida/en/document/2314/358
[32] se http://europa.eu.int/idabc/en/document/3923/358
[33] se http://europa.eu.int/ida/en/document/2287/358
[34] se http://europa.eu.int/ida/en/document/2633/358

total of 1600 entitled voters participated in the experiment, which was rated as very successful.

In Venezuela e-voting was offered in the polling stations in connection with the referendum on the re-election of Hugo Chàvez as President. As is well known, the President earned a new term. The opposition claimed the election to be marked by large-scale fraud. They were concerned that a revision of the election results, although offered by the election observers, would not lead anywhere, because the election had been electronic. The operations were conducted by SBC, a consortium of three firms. More than 14 000 people were mobilized and trained by the SBC to run the operations, which cost the authorities around 22 million euros. The SBC claims that Venezuela can save between 25 and 30 million euros pr election in the years ahead.

5 Democratic principles and legitimacy

5.1 Introduction

In the objectives of the Norwegian Elections Act it is stated that "the purpose of this Act is to establish such conditions that citizens shall be able to elect their representatives to the Storting, county councils and municipal councils by means of a secret ballot in free and direct elections" (Article 1-1). This chapter takes up some of the general principles regulating elections. These principles must be met in order to secure democracy and the people's confidence that the election is a legitimate expression of their opinions.

Over the last years Information and Communication Technology (ICT) has opened up new possibilities also in the field of democratic procedures (McLean 1989; Kersting and Baldersheim 2004). One aspect that has been given particular emphasis is how easy it has become to access information, to communicate with others and to engage in democratic processes. These changes may imply a strengthening of democratic procedures which emphasize discussion, dialogue and participation. At the same time different forms of "instant" participation may have negative effects on the traditional channels, such as the political parties and organizations (Westholm 2002).

The present chapter will not take up the whole topic of e-democracy, but be restricted to electronic voting. We concentrate on the following points in the mandate:

- Consider the importance of introducing an electronic system from a democratic perspective, including legitimacy and voter participation (1).
- Address and pay particular attention to the problem of undue influence related to voting in uncontrolled environments outside the polling station, cf. also the discussion pertaining to postal voting. (7)
- Consider the problems relating to the buying and selling of votes and the identification of a voter casting a ballot outside the polling station. (8)
- Consider the advantages and disadvantages of e-voting compared with regular voting in a polling station. (12)
- Consider effects changing control routines, from that of the layman to the professional expert, including effects on the voting system with respect to the audit and administration of the election and the competence of the administrators. (14)
- Summarize reports and research done in this area (17)

Point 14 is merely touched upon in this chapter, as it will be treated in detail in chapters 6 and 9. Research findings are reported and discussed where relevant, not least with respect to aspects affecting voting participation. Most of the discussion found in this chapter is of a principal nature. The principles taken up in section 5.2 are anchored in normative theories of democracy, but to some extent they are also found in relevant international provisions and recommendations. Section 5.3 is an in-depth analysis of phase 1 of an election, i.e. advance voting. We concentrate on the advance voting phase because this is the phase in which remote e-voting seems to be viable, principally or normatively. Section 5.4 takes up possible sources of error with respect to traditional manual voting procedures. These are important in considering advantages and disadvantages of e-voting and traditional voting procedures. Our

conclusions are drawn in section 5.5. These form an important basis for the technical solutions discussed in chapter 8.

5.2 Free and equal suffrage

Democracy means a government of the people, but can exist in a variety of forms and operate differently, and still appear as a representative form of government. The governing bodies are appointed by and act on behalf of the governed, and are obliged to act systematically in the interest of the governed. The means to make this possible is to hold elections to leading positions. In a democracy the members of the parliament – and corresponding assemblies at a regional and local level – are elected directly by the people. Many people claim that a democracy requires more than elections. They point to strong voter participation in the elections and in other political channels, and extensive political engagement and thorough discussions leading to the decisions made in the periods between the elections. Such ingredients are clearly necessary for living democratic governance. At the same time there is little doubt that without elections there is no democracy.

Democratic elections have two major functions. First of all they are a method to select the political leadership. Elections are meant to guarantee that the governing body is a representative selection of the population in terms of their values, attitudes, opinions and perhaps also in terms of important characteristics of their background. Secondly, elections are a method of controlling and placing the responsibility on the political leaders in parliament and government. In a democracy the voters may remove the people in power, and elect new ones. The representatives of the people must do their best to act in the interest of the people in order to be re-elected. Elections are thus a contribution to make governing bodies representative and to guaranteeing representative governance.

Elections are held in many contexts, not all of which are democratic. In the following we give an account of some requirements that must be met for elections to be legitimate from a democratic point of view. Many formulations of such requirements are found in the literature,[35] not least in instructions and manuals from different organisations involved in elections.[36] Although the terminology chosen to designate the different principles may vary, there is broad agreement as to the central elements.

On a general level the principles of *free and equal suffrage* are emphasized. The expression was first used to characterize elections as late as in the mid fifties. Free suffrage in this context means that no pressure or inhibiting restrictions may be exerted at any stage in the election process. In practice this implies that elections must be held within a framework respecting the human rights. By equal suffrage is primarily meant that the elections are conducted in a way characterized by impartiality, neutrality and equality. In the following we take up some of the fundamental principles that must be respected within a democratic framework of free and equal suffrage.

[35] For an overview, see Nygård (2003), Choe (1997) or Elklit and Svensson (1997).
[36] Cf. Chapter 6. The fundamental principles we have in mind have been discussed thoroughly in connection with election observation, as reflected in documents of the type ”Declaration of Principles for International Election Observation” (UN, 7 July 2005).

5.2.1 Periodic elections

In democratic systems the political representatives are elected for a specified period of time. For a parliamentary system this means that a maximum time session is set for a representative or a body of representatives to be in power. This time period may be ”interrupted” if a call is made for a new election. Recurring elections make political parties and representatives dependent on renewed voter confidence to continue their work. They also contribute to heightening the representatives' sense of responsibility, and to some extent ensure that the representatives do their best to act in accordance with the current interests and attitudes of their voters. How definite this regulation of responsibility is in practice, depends, among other things, on the election system chosen and the structure and importance of the political parties.

The future may find ICT a central factor in simplifying election proceedings, because the voting procedure will be less demanding – particularly if it may take place outside the polling stations on an electronic basis – and because counting may be automated. Simplifications like these in turn may create a pressure in the direction of using the voting mechanism more often than is the case today. One direction may be that elections are held more often and the election periods are shorter. Opinions will certainly vary as to the advantages and disadvantages of the increased ”voter sensitivity” that will result. A different direction may be that referendums are held more often. Why not let the people decide in more matters – or give their (not binding) advice to the politicians more often – if it can be done at low cost? (Morris 1999). Over time the representative character of today's system of government may change (cf. Buchstein 1997). Critical voices paint ugly sketches of the ”Push-Button Democracy” or the ”Instant Democracy”, including short-term thinking and reduced sense of responsibility of the political leaders.

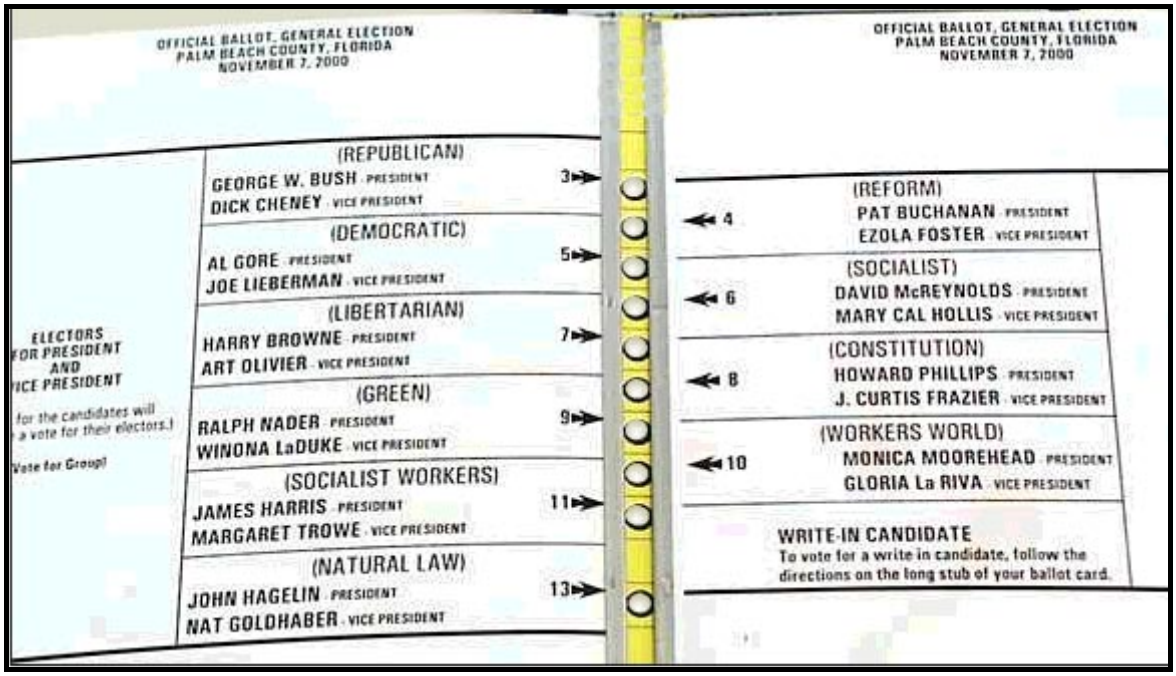
5.2.2 Different political alternatives

In a democratic election different political parties compete for the voters. A democratic society should have a broad range of political groups - well established groups or new ones – presenting themselves for election, and the voters should have a real choice among several parties, lists or candidates. Such requirements place specific demands on the period before an election, including the election campaign itself. The campaigning conditions must be reasonably similar for all the different groups, neutrality must be maintained in order that no party or group is unreasonably favoured. Furthermore, the voters' right to choose freely and without undue influence must be maintained.

Fair political strife in the campaign period presupposes a respect for fundamental rights and freedoms, such as the freedom of speech and expression and the freedom of association and peaceful assembly. The positions of political alternatives must be made clear to the voters. At the same time, the procedures for being registered as a political party and for nominating candidates or candidate lists must be impartial, and the criteria established for approval must be reasonable.

The new technology has a great potential in this field as well, not least with respect to making registration procedures simpler, and to giving a better overview. As for the voting procedure itself there are certain subtle – sometimes changing − effects of traditional voting procedures which may have their parallels in electronic voting The design of the ballot paper, for instance, may have important consequences for the outcome of the election, as was made quite clear during the 2000 Presidential Election in the US. “The butterfly ballot” in Palm Beach County in Florida (fig. 5.1 below) probably cost the democratic candidate Al Gore over 2,000 votes (Democrats who mistakenly voted for the candidate Pat Buchanan), and helped

George W. Bush win Florida by 537 votes − and the State of Florida decided who would occupy the White House (see Wand et al. 2001 and the New York Times 2001). Recent research has shown that the design of the ballot as well as the technology chosen in the polling stations may have an impact on how many votes and which votes are cast and registered in accordance with the voters' intentions.[37] A comprehensive survey made by Reynolds and Steenbergen (2005) confirms that simple designs cause fewer votes to be rejected. Controlled experiments suggest that most voters will cast the same ballot whatever the design of the ballot (use of symbols, colours, photographs etc.), but the design may systematically distort an important number of voters' ballots − such as perhaps a very hasty voter, or a voter with little education or weak reading skills.



Palm Beach County was responsible for the design of the ballot paper. The special design with two columns of candidates instead of one was motivated by the wish to make the font size as large as possible, given the restrictions set by the technical equipment available in the polling station, to help the many elderly voters in the county. The voters were to punch the small hole that corresponds to the name of the chosen candidates. The holes appear in the middle. The top hole is for the candidates in the top left column (Bush), the next is for the candidates in the top right column (Buchanan) and the third from the top is for the second row in the left column (Gore) etc. Many voters who punched the second hole, had intended to vote for Al Gore. If this was the case, they cast the wrong vote. Furthermore, the number of "overvotes" in Palm Beach County was exceptionally high (too many holes punched in the ballot paper). These ballots were rejected, which in fact means that the design of the ballot paper may have deprived many voters of their constitutional right to vote.

Figure 5.1: "The Butterfly ballot" in Palm Beach County, Florida, at the 2000 Presidential Election.

The user interface in e-voting may be compared with the design of a paper ballot, with corresponding importance. The user interface, the structure of the screen image and the methods for making (additional) information visible on the screen, are important aspects to consider if the ballot is to be cast from a computer, whether inside or outside the polling station. Even with a very simple user interface design, handling a complicated voting system

[37] See for example Bullock and Hood (2002), Niemi and Herrnson (2003) and Ansolabehere and Stewart (2005).

with complex rules for making changes on the ballot paper, may be unproblematic. It is hardly a coincidence that the countries having chosen to provide the polling stations with computers (specially designed voting machines, for example), are countries in which the voting systems are rather complicated (Belgium, The Netherlands, Ireland). The electronic technology furthermore has given us important advantages in the form of very fast and accurate counting.

If the user interface facilitates the voter's right to make changes on the ballot paper (crossing out, adding a personal vote etc.), one would think that more voters will make use of this option. The projects on e-voting in a selection of polling stations in the 2003 election in Norway do not give enough evidence to draw unambiguous conclusions in this matter.[38] On the other hand, e-voting may prevent ballots from being rejected on the grounds that the voter has not made the correct changes, since the voter will be warned of the error in trying to submit the ballot. Modern technology also helps to control the possibilities for change. SMS-voting over the mobile phones, the way they are designed today, is restricted to submissions of unchanged ballots only.

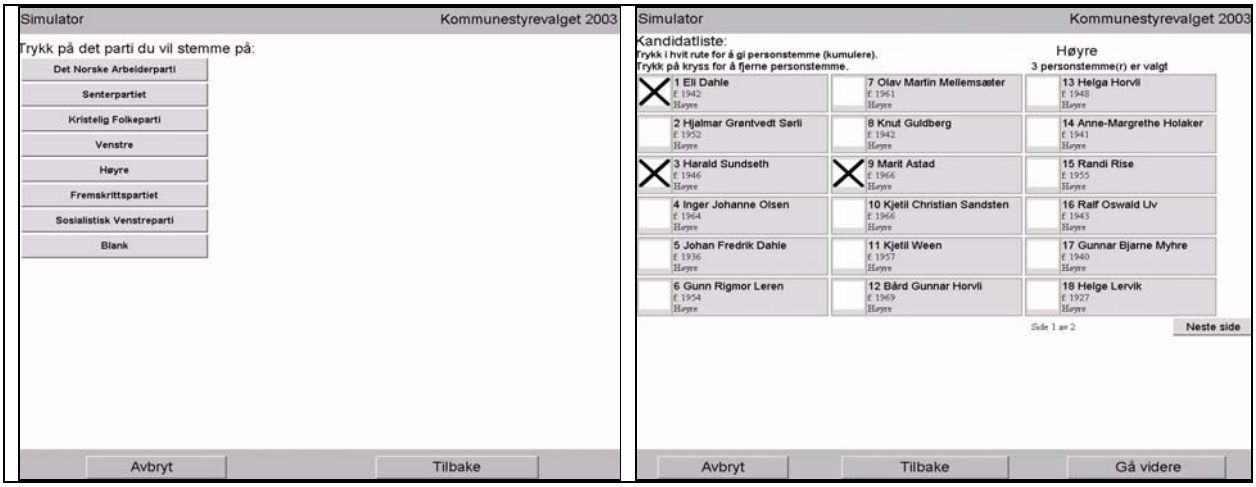


Figure 5.2: An example of a user interface, from the experiments on electronic voting in a selection of Norwegian municipalities in the 2003 election.

To better understand the importance of the user interface design, important experience may be gained from controlled experiments before a given design or electronic solution is put to regular use. The objective must be to provide electronic solutions which do not yield premeditated preferences for any of the political campaigners or influence the election results in any other way.

5.2.3 Inclusive elections and universal suffrage

Universal suffrage is a fundamental principle in democratic theory and practice, and has been so since at least the beginning of the 20th century. The right to vote can not be restricted to a minority of the people, but must comprise the adult population as a whole. Nor should the

[38] See Christensen, Karlsen and Aardal (2004: 39). Experience from the experiments is limited since the results from only two municipalities (Bykle and Oppdal) have been surveyed. As for votes cast in the advance voting period, the number of changes made was higher among the votes submitted electronically than the votes submitted by traditional means. Among the votes submitted on Election Day, a few more changes were made on the ballots submitted manually in Bykle, but no difference was found in the municipality of Oppdal. This means that the results are not conclusive.

case be that actual participation is restricted. Most people tend to think of weak voter participation as a problem, in spite of the fact that it is difficult to establish a lower limit for what is an acceptable level of participation.

In a democracy it is also important not to make an essential distinction between the criteria for being entitled to vote and the criteria for being eligible as a candidate, although the latter may be somewhat more restrictive than the former. Correspondingly, it should take a lot to lose the right to vote (cf. the Norwegian Constitution, Article 53). The voting system, however, must secure against the acceptance of ballots from adults who are not entitled to a vote.

If elections are not inclusive −in terms of the right to vote as well as in terms of being eligible as a candidate – the representativity of the system is weakened. Moreover, chances are that the assembly of representatives will act in accordance with the interests and attitudes of the voters if all the entitled voters are mobilized to submit take part in the poll, and more so than if the voter participation is skewed. If the representation is skewed in relation to the population as a whole, this may in turn skew policy-making and the directions of government action. Factors such as age, education and socio-economic status are found to be more or less relevant in this context.

5.2.4 More about voter participation

Several factors influence voter participation, as has been shown in a lot of research on the topic. Four factors are considered of particular interest. First, the voting system itself plays a role along with corresponding institutional mechanisms. Voter participation is generally lower in countries with a plurality-majority voting system than in countries with proportional voting systems. This has been well documented (Lijphart 1997). The Norwegian system is of the latter type, in which the return of representatives from the different political parties is very much in line with the population's support for the parties. Secondly, importance is also attached to the costs of voting – in a broad sense. The higher the cost and complexity of casting a ballot, the lower is the voter turnout. Voter registration procedures have also been found important in this context, i.e. whether voter registration is automated (as in Norway) or the voter has to take personal steps to be registered as an entitled voter (as in France and the US). Complicated registration procedures reduce voter participation. Other circumstances influencing costs are the duration of the voting period, whether Election Day is a weekday or a holiday, the distance to the polling station, the size of the queue at the polling station, etc. The effects of these circumstances on voter turnout are less clear, however. Some countries practice mandatory voting and issue a fine to voters who do not participate. Even a relatively low fine seems to affect voter participation.
Thirdly, political circumstances play a role for voter turnout. Voter participation increases when the political oppositions are clearly stated and there is tension and insecurity associated with the election results.
Finally, many surveys show that characteristics of the voters themselves are important to understand the patterns of voter turnout at elections. Generally the participation of young voters is lower than of other groups. Participation increases proportionally with higher education and higher income.

VOI has been mentioned repeatedly as a reform that will increase participation and particularly attract younger voters. Since our experience with e-voting is very limited, it is difficult to say whether - and not least in what way – VOI will affect participation. One possibility is simply that voter turnout will be even more skewed. We are still witnessing a digital divide (cf. Rønning et al. 2005), and e-voting may have the effect that the participation

of groups already showing a high rate of participation is further increased (Norris 2004a, Gibson 2001, Kenski 2005, Alvarez and Nagler 2001). Voter turnout may increase, in other words, but not necessarily among groups that are not already active participants.

Voting by post resembles VOI in certain respects. Both represent a simpler way of casting a vote, and may turn out to have similar effects. No analyses suggest that ample opportunities to vote by post from home unambiguously yield positive effects on voter turnout. Although participation has improved in certain places, other places seem more or less unaffected (Qvortrup 2005).[39] On the whole, we do not find that new groups of voters are mobilized to vote. The pattern remains much the same in postal voting as in traditional voting practice. A number of studies show that where participation increases, the more resourceful voters are responsible for the higher turnout (Magleby 1987, Karp and Banducci 2000, Berinsky et al. 2001). In Switzerland, a survey relating to the opportunity to vote by post showed that participation in the relevant cantons was not affected (Funk 2004).[40] Norris (2004a) made a comparison of voter participation in 25 different countries in the nineties. She concludes that the opportunity to vote by post does not affect the participation rate significantly. Among the factors that do have an effect, is the type of day chosen for the election: participation rates rise if the day of election falls on a Saturday or a Sunday.
The electoral commission in Great Britain draws other conclusions on the basis of the pilots run in 2002 and 2003. These pilots indicate that the opportunity to vote by post has been an effective means to increase voter participation (The Electoral Commission 2003). Norris (2004b:211) also emphasizes the success of the postal voting experiments. In voting districts providing postal voting as an alternative, the voter participation rate increased from 34 to 49 per cent.[41]

It is quite unclear whether e-voting outside the polling stations will contribute to higher voter turnouts in the long run. It is also unclear whether e-voting is a means to mobilize a significant number of young voters. Even though e-voting will make voting much more available and thus make voting easier, research on e-voting does not give firm evidence that voter participation will increase substantially. Increased voter participation, in other words, is not a very strong argument for introducing e-voting in uncontrolled environments, as it is highly uncertain that this in fact will be the outcome.

In this context, it should also be mentioned that e-voting outside the polling station during the advance voting period (phase 1 of the election) may reduce the number of polling stations required on Election Day. If e-voting availability reduces the need for polling stations, certain voters may experience this reduction as an unwanted effect of the new development

5.2.5 Equal suffrage

Democratic elections assume equal political rights. A democracy is fundamentally a system for the distribution of power. Every voter's ballot is equally powerful; at elections each vote counts approximately the same – and each vote cast in the same counting district, at least, has

[39] Two reasons have been given for introducing postal voting. One motivating factor is to counter low voter participation. The other is an incentive to reduce administration costs.
[40] The same survey shows that abolishing the obligation to vote (the obligation to vote has been abolished in several cantons over the last years) affected voter participation negatively, in spite of the fact that the provisions were to a large extent symbolic, and the sanctions for breach of duty were negligent (small fines).
[41] In Sweden the total number of votes from abroad grew from 32,000 in 1998, when postal voting was accepted only if the voter resided in Germany or Switzerland, to 50,000 in 2003, when postal voting was made an option for all Swedish citizens residing abroad (SOU 2004:111).

the same value. Political equality implies that no importance is attached to *who* the voter is. The ballots, in other words, could be swapped among the voters without having any effect on the results. The expression "approximately the same" is used above, because in some elections, notably the general election in Norway, a voter's assigned voting district may have an impact on the value of the vote.[42] This type of inequality must be particularly motivated, as it becomes a democratic problem once it becomes significant.

Equal suffrage also implies that the procedures followed and the technology used for the elections must ensure that each voter submits no more than one counting vote, and the system must guarantee that this vote is registered and counted. The system must prevent a voter from submitting more than one vote, prevent a vote from counting more than one, prevent any loss of votes and any alterations on the ballot once it has been submitted (i.e. to guarantee that a registered vote is in accordance with the voter's intention and action). In many countries manual voting procedures have been modified and improved over a long period of time, and the procedures generally ensure that equal suffrage is maintained. New technology no doubt can contribute to a very fast production of the correct results, but the voting procedure will be less transparent.

5.2.6 Transparency and auditability

Transparency of the voting procedures is important for several reasons. It makes the procedure predictable, and makes voting a task the voter understands and can follow, and this in turn is fundamental for gaining people's confidence. Confidence and legitimacy are closely related. Auditability and good auditing practices are considered to have similar effects. These practices maintain accountability and are a source to the credibility of the results. It takes time and effort to build trust, at the same time trust is a vulnerable matter and can be lost easily.

The requirement that an election system must be so transparent that the voters can understand how it works, regulates the procedures that have to be followed. Simplicity is an important value in any voting system.

The operations of the voting system and the regulations on voting routines which are provided in the legal provisions for elections make it possible for the voter to understand the system, albeit with a certain amount of effort. In this respect there is an essential difference between a manual voting system and a system based on electronic solutions. The technical aspects of e-voting can only be fully understood by a small number of experts; the voters must have confidence that the experts or expert organizations do the right thing, and make the systems function properly. Notably, the foundation of people's confidence in the system is much weaker than for electronic bank services, for example, because bank services are documented and retrievable in a way that is prohibited for elections: people's votes must be held secret.

It is essential that the system is secure and reliable. If there is any doubt as to the correctness of the results, as for example if credible claims are made about a technical failure or fraud, it must be possible to audit the process in order that the truth of the claims can be verified or

[42] One Oslo vote weighs less than one vote from the northernmost county of Norway (Finnmark). The election system put into force for the first time in the 2001 Parliamentary election includes an "area factor"; the number of representatives in a county is determined by a weighed sum of the number of citizens and the area size (one citizen weighs one point, one square kilometre of area weighs 1.8 points). This principle breaks with the principle of equal suffrage since people live in counties of different sizes. Note also that the weighing system is based on the number of citizens – not the number of voters.

dismissed, and the correctness of the results can be validated. In an electronic system, some type of log tracking can hardly be avoided if acts and operations are to be traceable to settle any question about their correctness.

The use of ICT in the elections automatically pulls in the direction of professionalizing the process. It will be very hard to attach as much importance to the layman for operation control and confidence building as in the manual system.

5.2.7 Secret suffrage

Secret suffrage is a cardinal principle in all modern democracies. This is reflected in the fact that it is common practice to make this principle a constitutional right. Interestingly, there is no wording in the Norwegian Constitution to this effect, but a related provision was formulated in 1814, namely that any voter who bought votes or sold his own vote, would lose the right to vote(Article 53, d). The regulation was abolished in 2003.[43]

Secret suffrage is closely related to what has already been said about political equality and equal suffrage. The *secrecy* itself is the central issue. Secrecy is a decisive means to guarantee free and equal suffrage. Hardly any voices today would suggest the introduction or re-introduction of open voting in a parliamentary election or any corresponding election (but see Sturgis 2005).

Secret suffrage was introduced in Norway in 1884. Only a small minority of Conservatives voted against this constitutional amendment. Their argument was that the freedom of the voter would be limited as the voter would no longer have the right to make their vote known to the public. Norway was in the front with respect to making secret suffrage a constitutional right. The principle was spreading in the British Colonies in the 1850ies and was referred to as "The Australian ballot". (Newman 2003).

From a technical point of view secret suffrage was warranted by amendments in the Norwegian Elections Act to the effect that ballot papers with any kind of personal signature were refused and the polling stations had to set up polling stalls or booths. Furthermore, it was required that the voters use envelopes that were approved by the authorities and delivered to the voters in the polling station. The voter had to insert the ballot in the paper ballot envelope personally, and personally insert the envelope in the ballot box. This procedure would guarantee that nobody else could see which ballot paper the voter opted for and would secure the separation of the voter and the vote.

Secret suffrage has two important characteristics. First, voter privacy must be guaranteed: the voter has the right to cast his or her ballot in privacy, undisturbed and in confidence, in contradistinction to open or public voting. Secondly, all traces must be erased once the ballot has been cast in order to prevent any possible link between the vote and the voter. The votes that are counted are anonymous. These characteristics imply that the voter *can not give any proof* of his or her vote. This is essential for the secrecy of the vote. A voter is free to publicly express his choice of party or list, but all claims about a voter's ballot is non-verifiable and loses credibility when secret suffrage is in place. Notably, it is the responsibility of the

[43] The regulation was no longer considered relevant. The following reason was also given: "The decision implies that the electoral committee has the right and duty to deny a person permission to vote if he is caught in voting fraud, without awaiting the decisions of the court on his case." Cf. Innst. S. no 209 (2002-03) from the Standing Committee on Scrutiny and Constitutional Affairs (p. 1).

authorities, and not the voter, to provide procedures and regulations to guarantee the secrecy of the vote.

There are two reasons why secret suffrage is considered so important for a democracy. First, secrecy prevents undue influence, i.e. it in fact prevents a voter from being deprived of the right to cast his or her personal vote, and at the same time it prevents the coercer from casting more than one vote. Undue influence in the form of threats, coercion or similar actions, in other words, would violate the principle of equal suffrage. In the early days of democratic practice, particularly before women had the right to vote, people feared undue coercion from employers, people of high rank and local authorities. Today our focus of attention is the risk of undue influence within the family (family voting). If every voter can cast his or her vote in privacy and undisturbed, no authoritarian family member can dictate other family members' polls. Thanks to the anonymity of the vote – the non-traceability of any link between the voter and the vote – no family member can control the content of ballot cast by anybody else.

The other reason secret suffrage is important is that it prevents the buying and selling of votes. As long as a voter cannot prove which party or candidate he or she voted for, buying a vote will have no guaranteed value, and no market for such trade will develop. The trading of votes would also violate the principle of equal suffrage: some people would have more influence on the results than others, by means of resources (money for example) considered illegitimate in a democratic setting.

In spite of what has been said above, in practice secret suffrage can not be understood as an absolute requirement. On the one hand procedures may have developed that somehow violates the principle. This is also the case in Norway. On Election Day current practice is for the voter to enter the polling booth, choose a ballot paper, fold it and walk over to the election official and the ballot box. The ballot is not inserted in an envelope. In other words, the voters, and not the authorities, are now responsible for keeping their votes secret on the way from the polling booth to the ballot box. A voter may show his or her ballot unintentionally by having folded the ballot incorrectly. More importantly, somebody else may be present in the polling station, notably a "buyer" – who can control the ballot. Such circumstances are highly relevant also in view of family voting. Under unfortunate circumstances an authoritarian family member will be able to control another family member's poll before it is inserted in the ballot box.

The fact that many countries accept voting by post as an alternative means of voting also means that the secrecy of the vote cannot be an absolute requirement. When a voter casts his or her ballot by post, it is the voter's responsibility to avoid undue influence. Furthermore, there is no absolute guarantee that ballots coming in by post have not been bought or sold. The validation of these votes, in other words, is based on the trust that they are true expressions of the voters' own political preference.

For Norwegian voters, voting by post is only an option if the voter resides abroad and does not have the opportunity to go to a polling station (the Norwegian Embassy, for example). The number of votes cast in this way is very small. As will become clear in the next section, however, postal voting has been an option in Norway since 1814 (The Norwegian Constitution, Article 60). Postal voting was withdrawn as a regular option 75 years ago, due to the risk of undue influence and other misuse.

How does e-voting outside supervised polling stations relate to the principle of secret suffrage? The voter alone will be responsible for maintaining the principles of casting the vote in privacy and without undue influence. In this respect e-voting is identical to postal voting. To the extent that voting by post is accepted and approved as a democratic means which observes the principle of secret suffrage, the same must apply to VOI and similar options (in remote environments).

One possible remedy to the problem of undue influence in voting outside controlled environments is to allow this form of voting only in the advance voting period (phase 1) and give the voters the right to vote again, either in phase 1 or phase 2. For administrative and practical purposes (see chapter 7) this procedure is recommended for postal voting. Practical and administrative reasons do not play the same role in the case of e-voting. We conclude that e-voting in uncontrolled environments in phase 1, combined with the right to vote again for people who make use of this option, is a reasonably secure procedure in view of the principle of private voting and voting without undue influence. Given a two phase procedure and the option of re-casting an electronic ballot, the voter cannot prove the content of his or her ballot.

However, e-voting outside the polling station raises new problems with respect to traceability, i.e. the principle that any link between a vote and its voter shall be erased when the ballot is cast (anonymity of the vote). It is important to remember that it is not possible to give the voter a receipt to confirm that his or her vote has been registered without creating problems related to the secrecy of the vote.

Central principles related to auditing the democratic practices in an election

”Free suffrage”
— *Good opportunities to maintain democratic principles, freedom from undue influence in particular*
— *Impartial and neutral operation of the election*

- ✘ Direct suffrage
  - The voters cast a ballot paper listing their choice of candidates to the representative assembly directly
- ✘ Periodic election
  - Representatives are elected for a limited period of time
- ✘ Political alternatives
  - Ample opportunity to establish political alternatives
  - The voters have real alternatives
- ✘ Inclusive election
  - Universal suffrage
  - Wide voter participation
- ✘ Equality
  - Equal suffrage
- ✘ Transparency and auditability
  - Transparent, neutral and competent administration
  - Verifiability and traceability
- ✘ Secret suffrage
  - Privacy (individual or private voting)
  - Anonymity (all traces erased when the vote is cast)

5.3 Advance voting - phase 1 and phase 2

Most democracies today – up to 90 per cent – run parliamentary elections with a voting period of one day only. In a very few cases the voting period extends over more than two days. In most countries Sunday is chosen as the best day to run a one day election, but Saturdays and Mondays are also popular election days. Empirical analyses suggest that voter participation is higher when Election Day falls on a non-working day (cf. Franklin 1996).

One reason for restricting the voting period to one day only is the challenges related to keeping the voting material overnight. Another reason is the administration costs related to keeping polling stations open for a longer period of time. By restricting the voting period to one day, a reasonable balance has been found with respect to availability, costs and security.

In some people's opinion it is important to maintain Election Day (or Days) as an established custom, to make it a special and ceremonial day. The act of voting is considered a civic duty and should – so they claim – take place in public space or controlled environments. From this perspective voting from home, from the work place or from some other place would seem an unfortunate privatisation of the voting act. It will endorse an element of voting which undermines living political culture and good citizenship.

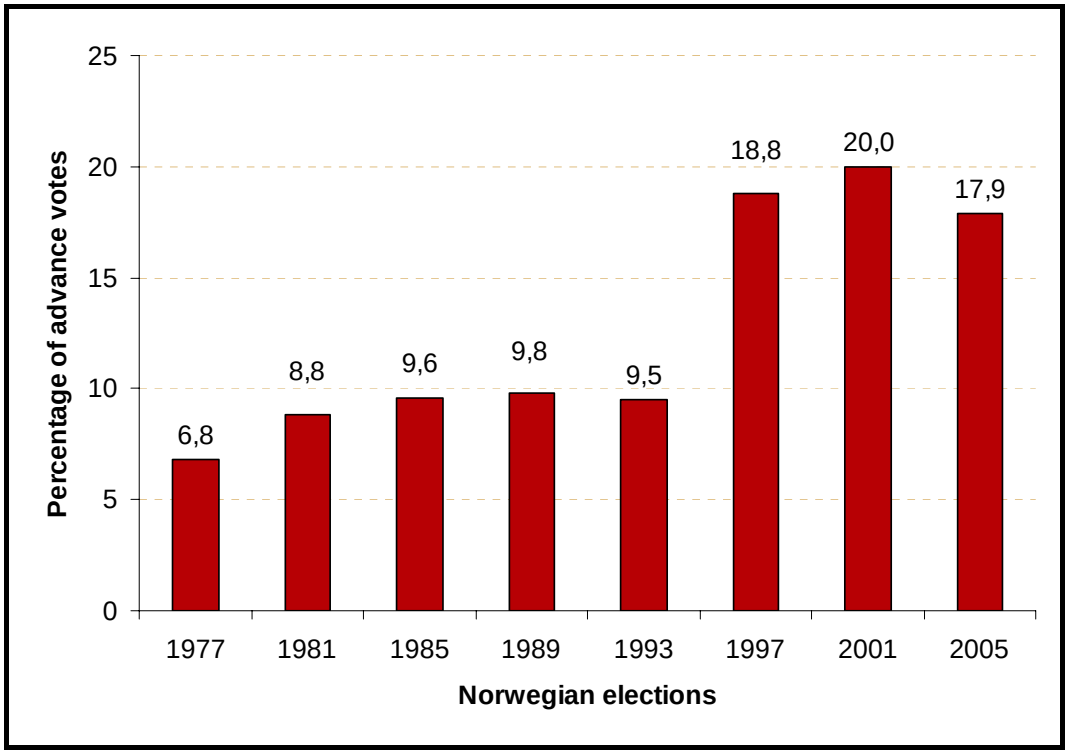


Figure 5.3: Percentage of advance votes in the general elections in Norway from 1977-2005.
Source: SSB (www.ssb.no/00/01/10/stortingsvalg).

At the same time, Election Day is also under pressure for another reason, and has been for a long time. Most democracies have made advance voting available (phase 1) for a longer or shorter period of time before Election Day (phase 2). In Norway as well as in other countries, a significant percentage of the incoming ballots have been cast in advance. Fig 5.3 above gives a graphic representation of the growing percentage of votes cast in advance in the period

from 1977 to 2005. There is little reason to believe that less than one fifth of the votes will be cast as advance votes in the foreseeable future. There is no real possibility for restricting the permission to cast advance votes without significant effects on voting participation. Considerations with respect to the principle of inclusive elections and universal suffrage suggest that elections must allow for two voting phases, however much Election Day is sought to be kept an established custom.

Advance voting has long traditions in Norway. As early as 1814 the Constitution stated that voters unable to cast their ballots in a polling station should be provided with the opportunity to cast their polls in advance (Norwegian Constitution, Article 60). At that time advance voting was made available in the form of a postal vote, which voters might opt for in the case of illness, absentee residence or other lawful absence. Postal voting became gradually more important for sailors and fishermen who were at sea on Election Day.

In practice the voter undertook the responsibility to cast his vote, without undue influence, insert his ballot in an envelope which was then to be sealed. The signature of the voter was to be witnessed by a person of age (21 years of age at that time), and the ballot paper envelope was to be sent along with an account of the voter's reason to cast an advance vote. Notably, every voter who cast a postal ballot in advance, had the right to cast a new ballot: Either he could cast a new advance vote (which had to arrive before the polling stations closed), or the voter could go to the polling station to cast a new ballot if this turned out to be possible after all (the advance vote was then withdrawn before counting).

At that time Norway had a considerable number of advance votes, but the rate varied a lot from election to election and from county to county. In the 1912 election about five per cent of the votes were cast in advance in the first round, nationwide, and one third of the voters from the northernmost county of Finnmark opted for advance voting (Saby 1918: 298).

In the 1930s advance voting changed in many respects. The fear of "misuse in the form of undue influence on the voters on behalf of agitators"(Castberg 1947: 406) caused advance postal voting to be more or less abandoned. From this time on the legislation pertaining to elections stated that advance votes could only be submitted if the voter personally cast his or her vote on designated premises with a certified returning officer.

The voting period on Election Day (phase 2) is short, whereas phase 1 in principle may extend over weeks or months. In a Norwegian context it has been emphasized that the voter should be acquainted with the political situation at the time of the election. This means that the period of time for advance voting must be limited. Voters casting their ballots on Election Day will be more informed about the political situation than advance voters, since they go to the polling station after the political campaigns have terminated, and the political alternatives presumably have been made clearer than earlier in the process.

The consideration of satisfactory voter participation suggests a provision for advance voting. Democratic responsibility presumes that the voters are informed about the political situation before they cast their ballots, and that the advance voting period does not extend over a long period of time. A realistic system for e-voting must be based on a two phase system for elections, as will be taken up in chapter 8. Electronic voting in uncontrolled environments is relevant only in phase 1.

5.4 Sources of error in current manual voting procedures

Errors may occur in all forms of election, whether the voting procedures are manual or electronic. The focus has often been on the (considerable) risks related to e-voting, but there are risks related to manual voting procedures as well. The difference is considerable, however, with respect to the seriousness of the errors that may occur in our well tested, paper based voting system, and a system which includes e-voting in uncontrolled environments (see Appendix B). Irregularities occurring in manually handled voting systems in established democracies only very rarely have consequences which are serious enough to issue a re-election. Credible claims about manipulation are also very infrequent, and examples of detected fraud are hard to find.

Our intention in this section is to raise the awareness of the sources of error that exist in the Norwegian voting system today. We begin by giving some examples of errors which may occur at different stages in the election. We then report on formal complaints that have been taken up in the Credentials Committee in the Norwegian Storting from 1965 to 2005.

5.4.1 Some sources of error

The new Elections Act of 2002 involved certain practical arrangements meant to eliminate previous sources of error, such as for example the ballot paper envelope and the problems of assessing whether or not a cast ballot should be rejected. Since the 2003 regional and local election the ballot paper envelope has been dropped in ordinary elections. A new arrangement has been provided in which the ballot paper is not inserted in an envelope, but is folded before it is inserted in the ballot box. Experience from the 2003 election showed that many voters had not folded the ballot paper correctly, to the effect that the name of the political party was visible when the ballot was submitted. At the 2005 parliamentary election this source of error was considerably reduced. There is reason to believe that this source of error will be eliminated as the voters get used to the arrangement.

Some voters have used a blank ballot as a kind of cover envelope before they have inserted their ballot in the ballot box. The result is that the blank ballot is the valid one, and the voter's intended ballot is rejected, since it is the blank ballot that is approved with the election official's stamp.

All changes made on a ballot must be interpreted and validated. This work is performed by an election official and is always to some extent a matter of assessment, which implies a potential for misinterpretation. However, the new Act has led to fewer rejections of votes due to formal errors than we had before.

Experience from the 2003 and 2005 elections also showed that several ballots had not been stamped. One source of this error may be that the voter has gone directly from the voting booth to the ballot box and the voter's ballot has not been registered and stamped before it has been inserted in the ballot box. Another source may be that the voter has inserted more than one ballot in the ballot box. In this event only one of the votes is stamped. It is important that the polling station is well organized, and that the election officials are sufficiently attentive to avoid such errors.

The ballot papers in the voting booths may be re-arranged or corrected. This may have the consequence that a hasty voter unintentionally picks the wrong list or votes for the wrong party or attaches a personal vote to the wrong candidate.

When a voter is manually crossed off in the voters' register, it can easily happen that the wrong voter is crossed off. This occurs from time to time when the polling station is crammed with people waiting in queue and the election official is under stress.

In preparing the ballots for counting, stations need to be set up for the reception, registration, exchange and validation of the ballots**.** If the procedures are not followed with precision, errors may very well occur. Ballots may be misplaced or get lost. Mistakes may be made in sorting the ballots during the counting in the polling stations. During the final counting it has occurred that relatively major sorting errors have been detected. The risk of cheating or fraud on behalf of the election officials is highest during the preparation of the ballots for counting. Ballot papers may be exchanged at this stage. For this to happen, the election officials need ballot papers and a stamp, and may change authentic ballots with other ballots at this stage. Preparation for counting takes place in open environments, however, and any cheater is at great risk to get caught.

In advance voting, voting in institutions or at home (including distant voting) the ballot is placed in a ballot paper envelope which is then inserted in a cover envelope along with the voter's polling card. It is important that this takes place immediately after the casting of the vote. Errors may occur as the election official may forget to attach the voting card or does not take care to use a cover envelope. In such events the ballot is rejected.

Ballot papers have to be stored from the time the advance voting period starts until Election Day. They are often stored in lockers or locked rooms, and are vulnerable to fire, water leakages or any election official's cheating. This is the case also with ballot papers in institutions, homes or abroad. The postal services or internal delivery services are often responsible for the transportation of the ballots, for example from the advance voting premises to the relevant municipal office or station. In this context the ballot papers are vulnerable to external circumstances or mistakes made by the delivery services or postal services. Since advance voting may take place up until Friday afternoon before Election Day (i.e. two days before the polling stations open), the postal services will not be able to deliver all the ballots in time. Advance votes may also be sent to the wrong address and the receiving end can not open them. Slow postal services may cause cast ballots to arrive too late to be counted and therefore to be rejected. This happened as recently as in the 2005 election.

Ballots need to be transported from advance voting premises, from institutions and from individual voters' homes, as well as from the polling stations. Ballots should always be transported by two persons. If these two persons agree, they may exchange ballots. An unfaithful officer will have access to ballot papers, envelopes, stamps, cover envelopes and sealing equipment.

.

5.4.2 Formal complaints on electoral matters

The Credential Committee's reports include complaints issued by voters and the committee's general remarks on the complaints. A total of 90 complaints have been registered from voters in the period from 1965 to 2005. Most of them are not grave in view of the democratic principles. Some of the complaints lack formal grounds. One recurring complaint is for example that no blank ballot papers were provided in the polling station (the electoral committee is not obliged to provide them).

Among the complaints that have been issued 44 complaints pertain to matters relating to the period before Election Day, 18 of them relate to candidate lists, 14 to the advance voting process. The complaints regarding candidate lists have to do with internal party matters or rights to party names.

The complaints concerning the voting period are of greater relevance here. The committee has received 42 complaints of this kind in the period 1965 – 2005. On the whole these complaints pertain to the lack of ballot papers in voting booths or circumstances that have occurred while the voter has been in the polling station. Only four complaints relate to circumstances in the post-voting stage, the small amount following naturally from the fact that very few voters participate in the counting and post-auditing stages of the election. These complaints have been examined by the committee in more detail.

The reports from the Credentials Committee include some general remarks. The remarks do not differ greatly from year to year, and are concerned with the following five circumstances.

- *The polling stations* have not stayed open long enough, or the opening hours have not been announced broadly enough.
- *The election officials* have not been trained well enough, and have made formal errors.
- *The ballot papers* have stuck on to each other, the quality of the paper has not been good enough.
- *Minute books* have not been adequately written or have been inconsistently written from one voting district area to the next.
- Two cases have been registered in which ballots have been missing or disappeared during the *transportation*, or the transportation has not followed regulatory practice

The most serious consequences of errors in an election are that a re-election must be issued. In the period 1965-2005 this has occurred only once, in1981 in the counties of Buskerud and Troms. The reason was that the number of mistakes made in the crossing off of voters in the voter register exceeded the margin for nominating the last representative (7 votes in Troms County, 28 votes in Buskerud County)

5.5 Conclusion and recommendations

In this chapter we have discussed some central aspects of the principles for democratic elections and pointed to challenges the use of new voting technology is certain to represent. The principle of secret suffrage in particular challenges the introduction of voting in uncontrolled environments, whether the vote is cast electronically or not.
Introducing e-voting in uncontrolled environments on Election Day *is certainly in conflict with the principle of giving every voter the right to secret suffrage.* The working committee therefore recommends that any further considerations of finding satisfactory technical solutions for e-voting be based on the following condition:

- The system for elections in Norway continues to consist of two voting phases, one for advance voting (phase 1) and one on Election Day (phase 2). E-voting in uncontrolled environments is relevant only in the advance voting period (phase 1)

Voters may of course be under undue influence if the ballot is cast in uncontrolled environments in phase 1, cf. the problem of family voting. The problem of buying and selling

votes is also still a possibility, and must be prevented. To act against problems of this sort a system is suggested in which a voter who has submitted an electronic ballot in phase 1, *is given the right to cancel or annul his or her vote.* Traditional voting in polling stations is maintained, i.e. places are provided in which the voters are guaranteed the secrecy of the vote even if they have already cast an electronic ballot one or more times in the advance voting period.
Technical solutions for e-voting should be sought within this framework, and require the following:

- Voting on Election Day should continue to follow traditional paper ballot practice in the foreseeable future. In phase 2 of the election a voter can only submit one ballot. Voters who have submitted an electronic ballot in phase 1, can submit a (new) ballot in paper, either as an advance vote in phase1 or in phase 2 – and in case the voter opts to do so, this is the vote that is counted.
- Voters who submit electronic ballots (e-voters only) can re-cast his or her ballot several times during the advance voting period. The last ballot submitted is counted.

Given the conditions suggested above, there is good reason to believe that the voters are guaranteed privacy and freedom from undue influence, even if e-voting in uncontrolled environments is introduced as an option. Furthermore, the buying and selling of votes is prevented because a potential buyer will never be guaranteed that an e-vote he has bought is actually counted.

Providing secure technical solutions in the e-voting system, we recommend that e-voting is made the only advance voting option in uncontrolled environments. The use of postal voting should not be less restrictive than it is today, even though this form of voting in principle is the same as e-voting in uncontrolled environments. The reason for this is that e-voting systems allow for very simple procedures for re-casting ballots. In a paper-based manual system (by post), administration costs will surge**.** Withdrawal of paper ballots is a very time consuming process. Our recommendation implies that we have to accept a certain difference between voters who submit electronic ballots in uncontrolled environments in phase 1 and voters who submit their ballots in controlled environments in phase 1 or 2. The right to submit a new ballot or vote again, is restricted to the former group of voters. The reasoning behind this is motivated by the intention to prevent undue influence and the buying and selling of ballots (which does not appear as a problem in controlled environments).

6 Legal matters

6.1 Introduction

E-voting raises a number of important and fundamental legal issues. The most controversial issue has been touched upon already in the previous chapter: the issue of whether e-voting in uncontrolled environments is consistent with the principle of secret suffrage. The question we ask ourselves is: How can we ensure secrecy of the vote and prevent undue influence on the voter, as required by the provisions of the Elections Act, when a vote is cast from home on a personal computer?

The basis for the discussion in this chapter is stated in the working committee's mandate: *"to consider and make recommendations as to regulations and requirements that should pertain to systems for electronic voting"*. Furthermore, the following points in the mandate are considered particularly relevant for the legal considerations:

- Address and pay particular attention to the problem of undue influence related to voting in uncontrolled environments outside the polling station, cf. also the discussion pertaining to postal voting. (7)
- Consider the use of an electronic Population Registry, and the implications of this for an e-voting system. (11)
- Consider effects of changing control routines, from that of the layman to the professional expert, including effects on the voting system with respect to the audit and administration of the election and the competence of the administrators.(14)
- Consider the responsibilities related to electronic voting, from a local, regional and national perspective. (15)

In this chapter we give an account of the Norwegian legislation on election procedures. The account is followed by a consideration of other national legislation relevant to electronic voting. We then turn to central aspects of international jurisdiction in these matters, notably the European Convention on the Protection of Human Rights (ECHR) and the Recommendation by the European Council on Standards for e-voting, including considerations by the Venice Commission relating to Article 3 of the ECHR pertaining to e-voting.

Our main conclusion is that eventually, the introduction of e-voting will require substantial changes in our national legislation on elections. However, our opinion is that such extensive legislative amendments are neither wanted nor needed until e-voting has been implemented on a national or large-scale basis. In a pilot project framework e-voting may be warranted by special provisions pertaining to experimental projects.

Norwegian legal provisions for elections have been developed and formulated to secure that the cardinal principles of democratic elections are maintained. It is essential that these principles are not undermined as new modes of voting are introduced. An electronic voting system must not only be designed, but also function to guarantee the accountability and security of the voting process. The secrecy of the vote is one of the most important principles in free, democratic elections. As will become clear in this chapter, however, (see section 6.5.3

below), there may be circumstances in which certain modifications will have to be allowed in the interpretation of this principle.

6.2 Norwegian national legislation on elections

6.2.1 General

Elections are regulated by Act No.57 of 28 June 2002 on Elections to the national assembly – the Storting - to the County Councils and the Municipal Councils (The Elections Act). Additional provisions have been formulated by legal authority in the 0005 Statutory Provisions for Elections of 2 January 2003. Statutory provisions regulating elections for the Storting are also laid down in the Constitution. Elections for the Sami Assembly are regulated by Act No.56 of 10 December 2004 on the Sami Parliament and other legal matters pertaining to the Sami (the Sami Act), and pursuant to this Act, the 1641 Statutory Provisions of 10 December 2004 (Regulations on Elections to the Sami Assembly).

In accordance with current legal provisions, *e-voting is not permitted*. Norwegian law states that ballot papers shall be used in the voting act, and this is implied in the provisions on printing, in regulations relating to advance voting and voting on Election Day, as well as in regulations pertaining to the approval and the counting of the votes.

On the one hand, the electoral provisions protect our essential democratic rights and state the fundamental principles of the election system. On the other hand, the same provisions regulate technical and administrative aspects of running elections. For example, they include detailed regulations on practical procedures to be followed in the election, including the voting process, as well as on the distribution of responsibility among the various official authorities etc. Although these aspects of the provisions are intended to satisfy our fundamental democratic principles, many of them provide regulations that could well be replaced by others.

6.2.2 The Objective of the Elections Act

The fundamental principles on which our election system is founded are expressively stated in the objectives of the Elections Act. Section 1-1 states that the Purpose of the Act is *to establish such conditions that citizens shall be able to elect their representatives* (to the popularly elected authorities) *by means of a secret ballot in free and direct elections.*

The preparations of the Act state that "*our democratic system is founded on a representative government, or what we call a representative democracy."* The representatives nominated to the Storting and to the County and Municipal Councils are to be elected by direct suffrage. This entails that the citizens have political influence through the political representatives they vote for in the elections. The right to free suffrage ensures that provisions are made for people to cast their votes freely. Furthermore the voter can cast a ballot for the party or list of candidates of his or her free choice, without interference or influence from public or other authorities. The principle of free suffrage is also intended to ensure all citizens the right to establish political parties or lists of candidates and present themselves for election. The regulations are furthermore intended to guarantee that the principle of secret suffrage is maintained. The voter should be guaranteed that no public link can be made between the voter and the vote, unless the voter personally decides to make this link public.

The purpose of the Act is important in many respects. It makes statements about the principles that are fundamental to the remaining provisions of the Act. The principles give the citizens privileges. At the same time they entail certain obligations on the part of the authorities, to the effect that election officials must provide the citizens with the means to execute their privileges. Moreover, the objective is relevant when decisions are to be made on questions of interpretation. This means, for example, that in case a provision is open to different interpretations, the interpretation that is closest to satisfying the objective of the Act should be employed.

The fundamental democratic principles pertaining to elections are challenged once provisions are made for the option to vote electronically. This topic is elaborated on in chapter 5 above, and in section 6 of the present chapter.

6.2.3 The electoral authorities – responsibility and control

The Ministry of Local Government and Regional Development is the national authority responsible for running the elections. The practical arrangements of preparing and running the election are allocated to the individual municipalities, and are put into force by the electoral committees. In accordance with article 4-1 of the Elections Act, each municipality in the country is to have an electoral committee, elected by the Municipal Council.

Local electoral authorities are responsible for auditing and approving candidate lists, printing ballot papers, arranging polling stations and running the voting process. The electoral committee is responsible for handling all the returned ballots from the municipal voting districts. In every polling station a polling committee is responsible for administering the poll on Election Day, as stated in Section 4-2 of the Elections Act. The electoral committee appoints the returning officer to be responsible for handling the advance votes. Votes cast abroad, in Svalbard and in the Island of Jan Mayen are received and handled by legally appointed returning officers and returning officers appointed by the state authorities. When the voting period is closed on Election Day, all the ballots cast are validated and counted by the electoral committee, and the returning representatives are nominated in accordance with the allocation of votes. The Municipal Council formally approves the (local) election for the municipal council

In accordance with Section 4-3 of the Elections Act, each county is obliged to have an electoral committee elected by the county itself. The county authorities are also responsible for the practical arrangement related to elections for the County Council as well as for the Storting, i.e. auditing and the approval and printing of ballot papers. The County is also an important body for auditing the allocation of returning representatives in these elections. The County Council formally approves the County Council election. The Storting formally approves the election for the national assembly. After national elections for the Storting, it is the responsibility of the national electoral committee to make decisions on any issued complaints and to nominate the representatives for the seats at large. National elections are approved by the Storting.

In the opinion of this working committee, provisions will have to be amended for the allocation of authority and responsibility related to elections if electronic voting is established on a national or large-scale basis. The basis for this opinion resides not least in the observation that a gradual change from a layman control to professional control is already evident in pilot projects on e-voting. An independent regime for the certification of computer systems for e-voting has to be established, cf. chapter 9. This will have an effect on the

allocation of responsibility. Eventually it will also have to affect the system by which the election results are approved.

However, it is the opinion of the working committee that today's allocation of responsibility can be maintained if pilot projects are run. Significant changes on a short-term basis are not to the purpose, because the pilot projects themselves will contribute with considerable experience that may itself be suggestive of good and sensible ways of allocating the responsibilities.

6.2.4 The Voters' Register

Section 2, sub-sections 1 and 2of the Elections Act state the requirements for voter eligibility. To exercise the right to vote, the citizen must be registered in the voters' register. The voters' register has many purposes. First of all it is intended to secure that only entitled voters cast their votes. Secondly, it gives an overview of the individual voter's assigned voting district, in which the voter has to submit his or her vote. Finally, it is intended to secure that each voter submits one vote only. All entitled voters are registered to vote in the municipality of their residence as of 31 May of the Election Year, as registered in the Population Registry.

The voters' register and the Population Registry are also used to control the eligibility of candidates who present themselves for elections.

The electoral committee of the individual municipalities is responsible for setting up a voters' register in the year of the election, cf. Sections 2 – 3 of the Act. The voters' register is set up on the basis of information from the Population Registry. It has therefore been laid down in the Elections Act that the Central Population Registrar's Office makes the Population Registry available in a manner that facilitates the Electoral committees' task of setting up correct voters' registers in each municipality; cf. Section 2 -5 of the Act. In practice the Population Registrar's Office enters into an agreement with a computer software provider to distribute general information about the Population Registry, including information for use in the preparation of voters' registers for elections. Included in the agreement is the task of the service provider to distribute voters' registers in accordance with the Population Registry of 31 May as well as all updates after 31 May to the municipalities in the Election Year. The Population Registry may be updated up to Election Day, but updates are only to be made under special circumstances, cf. Article 1 in the Provisions to the Act.

An electronic voters' register is not a prerequisite for e-voting in the polling station. For e-voting in uncontrolled environments, however, authentication of the voter against the voters' register must be performed electronically, cf. Standards no 39 – 41 of the Recommendation. As a consequence, the technical solution provided for the e-voting system must include a machine-readable voters' register. The authenticity, confidentiality, availability and integrity of the voters' register must be maintained, cf. the Recommendation, standard no 86.

6.3 Other national legislation to be considered if e-voting is introduced

If voters are provided with the opportunity to submit their ballots *electronically*, a number of acts and provisions come into play beyond the general provisions for elections. In this section we give an account of the most important legislation and consider its relevance for e-voting.

The working committee does not exclude the possibility that other legislature may be relevant, but this may vary, depending on the type of pilot project started.

6.3.1 Legislation on the Protection of Privacy

Any system providing the voters with the means to submit their ballots electronically will require measures for protecting the privacy of the voter. A computer system for e-voting in uncontrolled environments requires an electronic voters' register to check that the voter is entitled to submit his or her ballot, i.e. it authenticates the voter electronically.
An electronic register is also used when the voters submit their ballots electronically in controlled environments. The register is intended as a system to verify that a voter has cast his or her ballot. Furthermore, a provisional link must be maintained between the voter and his or her ballot if provisions are made for the e-voter to cast a new ballot, cf. chapter 8.

Requirements on the protection of privacy are regulated by Act 31 of 14 April 2000 on the protection of privacy (the Protection of Privacy Act). The Act is intended to protect the individual against privacy violation when personal information is processed electronically, cf. Section 1. The Act provides the framework for the requirements, and is supplemented by the regulations laid down in the 1265 Provision of 15 December 2000 (Statutory Provisions for the Protection of Privacy).

The Act applies to the wholly or partially electronic processing of personal information. *"Processing"* personal information in this context means any use of personal information, collecting, registering, combining, storing or distributing, or any combination of these, cf. Sections 2 and 3 of the Act.

The working committee recommends that the Protection of Privacy Act is applied if e-voting is provided as a real option. The committee also recommends that the regulations on processing *sensitive* personal information apply. In accordance with Section 2, subsection 8 of the Act, a citizen's personal political opinion is considered sensitive personal information.

Processing personal information is legal only if it is in compliance with Articles 8 and 9 of the legal provisions. The provisions relate to informed consent, legal title, or a decision that processing personal information is necessary. The legal title to make a voters' register complies with Chapter 2 of the Elections Act. There are no legal provisions for making electronic voters' registers, nor is any regulation provided to prohibit such processing of personal information. The Population Registry is regulated by Act 1 of 16 January 1970 pertaining to national population registration and the provisions relating to this Act. The voters' register is a copy of parts of the Population Registry, and is not considered sensitive personal information.

The Protection of Privacy Act is particularly relevant with respect to the link between the voter (register) and the ballot cast. Any link between the voter and his or her ballot is considered sensitive information. No provision for this type of link is stated in the Norwegian legislation on elections. However, it is our consideration that a voter who chooses to submit an electronic ballot at the same time gives his or her consent to a provisional storage of this link, on the assumption that the voter is well informed about the link before he submits his or her ballot, cf. Subsection 2, paragraph 7 of the Act. If the voter is not informed, the person in question has not given his or her consent, in which case legal provisions for a preliminary storage of this link are necessary.

Anyone processing personal information in the sense described above must report it to the Data Inspectorate. A special licence is needed for processing sensitive information, unless this processing is provided for by the legal provisions cf. Subsections 33 and 31. The Data Inspectorate is the Supervisory Authority, cf. chapter VIII of the Act.

The Protection of Privacy Act states the conditions and requirements for the data processing authorities and the person(s) processing the data. For the present purposes, the data processing authorities are the relevant Electoral committees, cf. Subsection 2, paragraph 4 of the Act. The persons processing the personal information do so on behalf of the data processing authorities, cf. subsection 2 paragraph 5 of the Act.

One central issue relates to the formulation of a strategy for security measures. Through systematically structured initiatives the electoral authorities (the data processing authorities) shall provide adequate measures for the security of the information, cf. Subsection13[44]. Before introducing electronic voting options, adequate procedures must be established in compliance with the regulations of the Protection of Privacy Act and the provisions pertaining to this Act. The formulation of such procedures is also needed to work out a set of rules and specified requirements for the e-voting technology. The formulation of such procedures should take adequate account of the strict requirements on e-voting set out in the Recommendation of the European Council.

The Protection of Privacy Act applies in the processing of personal information unless otherwise stated in separate laws, cf. subsection 5. Separate provisions may have to be stated if the regulations provided by the Protection of Privacy Act are not sufficiently clear. If this is the case, the regulations provided by the Protection of Privacy Act apply in as far as no other provisions are made in a separate Act to regulate the procedure of processing personal information. Current legislation on elections does not provide any such regulations. However, the Recommendation has formulated very strict guiding principles for securing the quality, integrity, confidentiality and accessibility of electronic information which should be taken into account in providing e-voting as a real option. The formulation of separate provisions pertaining to e-voting should therefore be considered if e-voting is established as a permanent option in elections in the future. The working committee considers it natural that such provisions are made before e-voting is introduced on a permanent or large-scale basis.

Conclusion: The working committee is of the opinion that the Protection of Privacy Act applies if e-voting is provided as an option in elections. Alternatively, the Government may formulate separate provisions for all the electronic processing of personal information related to elections.

6.3.2 The eSignature Act

When a ballot is to be submitted electronically, the voter must identify himself and be authenticated by the voting system. The system, moreover, must ensure that the voter does not submit more than one valid vote. When ballots are cast electronically in controlled environments, the voter does not always have to be identified by electronic means. Voting in uncontrolled environments is different. The identity of the person submitting information must be confirmed (authentication). Any interference with the ballot during transportation

[44] For more detailed information, see the Data Inspectorate Guidelines ”Veileder om informasjonssikkerhet for kommuner og fylker” TV-202-2005.

must be prevented, both in terms of obtaining information that links the content of the ballot to the voter (secrecy) and in terms of making changes on the ballot (integrity). The system must also ensure that the voter is not able to deny that he or she submitted a ballot (non-deniability).

Legal provisions on e-Signatures are laid down in Act No 104 of 17 June 2005 on e-Signatures (the e-Signature Act). Electronic signatures are data in electronic form that are attached to other electronic data, and which serve as a method of authentication (cf. Section 3, No 1). The definition includes a type of e-signature based on PKI technology. This type of e-signature satisfies the above requirements.

The e-Signature Act shall make provisions to ensure secure e-signature services and products (examples are PKI solutions such as smart cards, bank IDs, e-IDs, etc.) on the market, by specifying regulatory requirements on certificate qualification, certification providers and the secure-signature-creation device itself, cf. Section 2. The e-Signature Act applies generally to all electronic signatures used in open or closed networks. The objective is that e-signatures create trust between communicating parties who must know with certainty that they are in fact the parties they pass themselves to be. To strengthen confidence and trust between the communicating parties the electronic signature is issued with an electronic certificate from a third party: the certification-provider.

The system depends on the two parties' confidence in the certification provider. The certification provider is responsible for authenticating the identity of the party receiving the certificate. A detailed description of the technical solution in PKI-based signatures is found in the Norwegian Official Report (NOU) No 10, 2001.

In accordance with the definition in Section 3, No 3 of the Act, a qualified electronic signature is an advanced electronic signature (see Section 3, No 2) based on a qualified certificate (see Section 4) and created by an accredited secure-signature-creation device (Sections 8 and 9). On the basis of current technological advancement a PKI-based signature is a qualified signature. This may change over time. PKI technology satisfies the functionality defined in Section 3, No 2 of the Act. An advanced electronic signature means that the signature meets the following requirements:

1. It is uniquely linked to the signatory (voter)
2. It is capable of identifying the signatory (voter)
3. It is created using means that the signatory can maintain under his sole control, and
4. It is linked to the electronic data to which it relates in such a way that any subsequent change of the data is detectable.

The requirements in 1 –4 above are strictly necessary for the accreditation of e-signatures to serve in e-voting systems in uncontrolled environments. Further details pertaining to the properties of qualified certificates are laid down in Section 4 of the e-Signature Act.

Regulations pertaining to the certification-service-providers are laid down in Sections 10 to 15 of the e-Signature Act. One important requirement for ensuring adequate confidence in the certificates relates to signature verification. In compliance with Section 13 of the Act the qualified-certificate-service-provider is responsible for working out secure procedures and routines for authenticating the signatory's identity and other relevant information pertaining to the signatory. Requirements on identity authentication and verification are provided in

Article 7 of the Regulations pertaining to certification-service providers. The Regulations state that "identification requires that the communicator appears in person", i.e. meets the certificate-service provider or his/her representative personally, unless the signatory has already been identified by personal appearance in establishing existing client relationships. The signatory may not appear by proxy.

The Act does not state general provisions for electronic communication, but it applies wherever electronic communication is legally provided for. Section 6 of the Act states that if a signature is required by law or other legal provisions in order for a communicated arrangement to have legal effect, and if the disposition may be arranged electronically, *"A qualified electronic signature satisfies the requirements"*. The regulation implies that the authority to demand an electronic signature by authentication must be regulated by law or other provisions.

In the Provisions of the Act the Norwegian Post and Telecommunication Authority is appointed the Supervisory Authority responsible for controlling qualified-certificate-providers. The Data Inspectorate is appointed the Supervisory Authority for certain parts of the Act (Section 7).

In compliance with Section 5 of the Act, His Majesty the King may lay down additional regulations on the requirements for qualified electronic signatures to serve in electronic communication with and within the public sector, see 6.3.3 below.

Conclusion: For e-voting in uncontrolled environments to be introduced as a real option, the legal requirements on qualified certificates as laid down in the e-Signature Act must be satisfied.

6.3.3 Regulations on e-Administration

The 2001 Amendments to the Public Administration Act, Section 15 a, make provisions for electronic communication with and within the Public Administration, including regulatory provisions for signatures, authentication and measures for securing system integrity and secrecy. The provisions were laid down on 25 June 2004 (No 988) and enacted on 1 July 2004 (Provisions for e-Administration). The provisions are sanctioned by the e-Signature Act Section 5, see 6.3.2 above.

The regulations pertain to electronic communication between the Public Administration and the public and to electronic procedures and communication within the Public Administration; cf. Article 1 of the Provisions. The objective is to provide secure and efficient means for electronic communication with and within the Public Administration. Detailed procedures are specified for this type of communication.

The individual administrative bodies have great freedom to decide whether an electronic communication system should be provided for, and if it is provided for, how such a system should be operated. As stated above, authentication related to e-voting in uncontrolled environments requires a PKI-technological solution. The use of electronic communication in the submission of ballots at an election must be sanctioned by law or legal provisions pertaining to e-voting. The Provisions on e-Administration apply here.

The provisions do not require the use of qualified electronic signatures. In compliance with Article 4 (1), anyone who communicates electronically with the Public Administration may on the whole do so "without a security service or product". It follows from this that the citizen may communicate via e-mail.

However, on the basis of the regulations in Article 4 (2), or if otherwise permitted by law or legal provisions, the Public Administration may demand a security service, such as a qualified electronic signature, for e-communication with the administration. "A security service or product" means, for example, a technological device that confirms a person's identity (PKI as an authentication method). The definition is spelled out in Article 4 (1), letter a.
A security service device must be adjusted to the needs and be based on the security strategy of the individual administrative body. In other words, the solution chosen must accommodate the relevant needs, and must be easy to operate. The requirement of a security service device to authenticate e-voters must be sanctioned by the legal provisions for e-voting.

The formulation of a security strategy is also considered a central issue, cf. Article 13, as it forms the basis for requiring a security service, in accordance with Article 4. The security strategy chosen must comply with highly recognized principles for the security of information systems, cf. Article 13 (2). The regulations make statements about a number of circumstances that should be considered and possibly be regulated by specified procedures, cf. subsection 3.

The authorities must also indicate which products (the technical solutions) they select, and how they are put to use, cf. Article 4, subsection 4. Separate requirements are placed on the technical solutions selected for the collection of privileged information, cf. Article 5. To give an example: the Data Inspectorate recommends encryption for the transportation of sensitive personal information. Secure transportation channels must be provided.

Related to the topics already discussed, a number of additional requirements are formulated in the Provisions on e-Administration, which will come into force as soon as the Provisions apply. The working committee refers the reader to Guidelines for the Provisions for further information.[45].

Conclusion: The Working committee recommends that the Provisions on e-Administration apply if a PKI solution is used as an authentication method in e-voting.

6.3.4 The Penal Code

There are no separate penalty clauses in the legislation on e-voting in this country. Possible breaches of the legal provisions laid down in the Elections Act are captured in the Penal Code. The same legal provisions apply if e-voting is introduced. Part 10 of the Penal Code states the regulations on criminal action related to the execution of the Civic Rights.

In compliance with Section 105 of the Penal Code it is illegal to make any attempts to influence any voter's decision unduly, whether by intimidation, threat, purchase, promise of gain, deceptive prospect or by any other undue means. The same applies to any attempts to prevent a voter from casting his or her vote. The legal provision has a bearing on any person who imposes his will on a subservient person /exposes any other person to undue influence.

[45] Guidelines to the provisions on electronic communication with and within the public administration: http://odin.dep.no/fad/norsk/dok/andre_dok/veiledninger/002001-120010/dok-bn.html

Any attempt at such action is considered a completed offence, as there is no requirement that the voter has in fact submitted his or her ballot against his or her personal will under undue influence. The principle of secret suffrage makes it generally impossible to verify which ballot the voter actually submitted.

In accordance with section 106 of the Penal Code, it is illegal for any person to select his or her ballot, or refrain from voting, on the basis of an agreement, a personal gain or a promise. The regulations comprise the purchase of votes and have a bearing on anyone who accepts a personal gain in exchange for the submission of a particular ballot. For the regulation to apply, a direct link must be established between the choice of ballot and the gain promised or received. No agreement need in fact be settled, but initiatives have been taken for the purpose of a purchase agreement. Tactic voting initiatives in the sense of inviting groups of people to vote for the same party for tactical reasons is not against the law.

In compliance with Section 107 of the Penal Code it is illegal for any person to act untruthfully for the purpose of establishing his, her or somebody else's wrongful eligibility to register or vote, or to falsify any material fact for the purpose of giving himself, herself or somebody else admission to vote in election. Such untruthful action includes wilful manipulations of information in the Population Registry for the purpose of unrightfully establishing the right to vote. It also includes cases in which somebody knowingly submits a vote on the basis of false statements or fraudulent register entry.

- ✘ It is illegal to mutilate voting results
- ✘ It is illegal to coerce a voter to vote or cast a vote against his or her will
- ✘ It is illegal to act negligently for the purpose of failing to count somebody's cast vote
- ✘ It is illegal to sell an entitlement to vote
- ✘ It is illegal to buy somebody's vote

It is also a legal offence to make somebody cast an invalid ballot or cast a ballot which is not in accordance with his or her persuasion, or unlawfully prevent somebody from casting a vote, cf. also Section 105 of the Penal Code. Offences are of this kind if for example a voter is misguided about which ballot has actually been inserted in the ballot box, or if a voter is deliberately misguided with respect to the preference changes he or she may make on the ballot paper, or if the voter is deluded to submit his or her ballot in a way which causes it to be rejected. Unlawful voting prevention comprises cases in which somebody knowingly prevents a voter from appearing in person at the polling station. Cases of deliberate prevention are regulated in Section 105 of the Penal Code. Another type of case is when somebody knowingly and wilfully gives incorrect information about the time and duration of the voting period, to the effect that the voter arrives too late to cast his or her ballot.

In compliance with Section 108 it is a punishable offence to mutilate or forfeit voting results or to wilfully contribute to causing an approved ballot not to be counted. Mutilation may occur if for example the correct voting results are replaced by fake minutes, or alternatively, counting mistakes are wilfully made or incorrect counts are knowingly and wilfully quoted. The regulations also pertain to voters who submit their ballots several times in the same election, or insert more than one ballot in the ballot box.

Part 11 of the Penal Code, pertaining to criminal offences committed by a person while on public duty, and Part 33, pertaining to summary offences committed by people while

performing a public duty, are regulations which also apply here. These regulations are not discussed any further in the present report.

The penal provisions attended to in this chapter also apply to e-voting. However, computer systems used in elections avail themselves to a very different type of punishable offence. A number of penal provisions regulate computer crime. The working committee does not consider it suitable to the purpose to discuss all of them in this report. We note, however, that the central and more important provisions on computer crime relating to e-voting are the provisions on data theft in Section 145, subsection 2 of the Penal Code. The provisions penalize anyone who breaches any security measures or in any other way gets illegitimate access to data or software stored or transported by electronic or technical means. The term "data" comprises all types of machine-readable information, such as for example information about personal, technical or economical matters.

The Protection of Privacy Act, the e-Administration Act and the e-Signature Act state requirements and regulations on the security of information. Not to take measures to prevent security threats is also in some respects an offence; cf. Section 48 of the Protection of Privacy Act and Section 21 of the e-Signature Act.

The working committee is aware that work is currently being carried out to consider parts of the Penal Code. We strongly suggest that penal provisions relating to elections are also considered as part of this work, as an important question is whether additional penal provisions or amendments are required if e-voting is implemented as a real option in elections.

6.4 International commitments

It is our basic assumption that Norwegian jurisdiction is in accordance with international law. Principles for democratic elections are reflected in a number of international commitments/obligations, such as the European Convention of Human Rights (ECHR) and the Code of Good Practice in Electoral Matters, which have resulted from joint efforts in the European Council[46]. Commitment to our cooperation with the European Council is of primary importance to developments in the area of elections. Established in 1949, the European Council today has 46 member states, among which is Norway. The most important task of the European Council is to protect the Human Rights, the Democratic Principles and the Rule of Law. The cooperation has resulted in a network of international agreements and conventions. The Venice Commission, the European Commission for Democracy through Law, was appointed by the European Council. The Commission provides analyses, reports, and publications relating to constitutional matters. It also provides expert opinions relating to the understanding of fundamental national and international legal values. Another important institution established through co-operation with the European Council, is the European Court of Human Rights. The role of this Court is to take up complaints brought before the Court and make final binding judgment on the Contracting States.

6.4.1 The European Convention on Human Rights

The European Convention on Human Rights (ECHR) of 1950, Article 3 (the Additional Protocols) states that the member states *"undertake to hold free elections at reasonable*

[46] www.coe.int.com

intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature."

The objective of Article 3 is to ensure free and secret suffrage. In accordance with general practice laid down by the European Court of Human Rights, this Article does not only refer to the obligation to hold free elections, but warrants the voters' individual right to vote and to present himself or herself for election. The same applies to universal and equal suffrage, and means that each voter has individual rights in accordance with the decision. Elections must be organized in a manner that warrants the free expression of opinion. The decision is intended to guarantee that the voting procedure is organized in a way which secures the secrecy of the votes.

In accordance with legal practice the rights stated in Article 3 of the protocols are not absolute; they are subject to certain implicit constraints. This means that the Member States may exercise reasonable judgment in formulating the conditions for universal suffrage and the election system. However, the constraints and conditions stated must serve legitimate purposes.

It is obvious that the ECHR, Article 3 of the additional Protocols, regulates national parliamentary elections. Whether it also regulates the election of other representative bodies, however, depends in practice[47] on considerations of the comprehensiveness and the extent of independence of the authority given to the representative body in question. There is reason to believe that the decisions in the Article do not necessarily apply in local and regional elections, in view of the relatively restricted authority of the municipal and county councils (Aall 2004).

6.4.2 The Code of Good Practice in Electoral Matters

The Code of Good Practice in Electoral Matters 2002, laid down by the Venice Commission, regulates the procedures for elections in the Member States. The regulations are approved by the EC Committee of Ministers. The Code is based on the "European electoral heritage", a set of common principles for European elections based on the right to universal, equal, free and secret suffrage. The democratic heritage is built on a set of international standards, and is given expression in Article 3 of the European Convention of Human Rights

The Code of Good Practice in Electoral Matters presumes that e-voting may be introduced. The regulations state that a voter shall always have the opportunity to cast his or her vote in a polling station, cf. Part I 3.2 ii. Given that this opportunity is provided, the regulations state that e-voting may be accepted if the e-voting system is *secure and reliable*, cf. Part I 3.2, iv.

In the notes to the Guidelines, the Venice Commission emphasizes that the authorities are obliged to protect the voter from any threat or undue coercion to ensure that the voter may cast the ballot of his or her own persuasion. Furthermore, they point out that certain security measures should be taken to minimize risks of fraud. One such measure might be to give the voter the opportunity to control his or her ballot immediately after submission. Furthermore, the voter should be given the opportunity to get a receipt that the ballot has been registered. This does not mean that the voter is given a paper receipt that lays bare the content of the vote.

[47] Decisions of the Court 5 July 1985 (Booth-Clibborn) an 2 March 1987 (Mathieu-Mohin and Clerfayt)

To provide for verification and new counting of the votes, a system may be developed in which the incoming, registered ballots are printed out on paper. If this system is chosen, the votes must be sealed in a device that ensures that the ballot submitted by the voter may not be seen by others. Whichever method is chosen, it must secure the secrecy of the vote.

The voter must have the opportunity to correct his or her vote if necessary, without violation of the principle of secrecy. This means that the voter must have the means to make corrections before he or she presses the send-button and submits the ballot.

The system must be transparent, in the sense that its functionality may be tested.

6.4.3 Recommendations on standards for electronic voting

On 30 September 2004, the Committee of Ministers to the European Council approved a recommendation on legal, operational and technical standards for e-voting, cf. Appendix A. The recommendation is a legal instrument, which must be unanimously approved by the Member States, but which is not binding by international law. The working committee recommends that the Recommendation applies if the opportunity to vote electronically is introduced on a large scale basis. Its standards should then be made legally binding in Norwegian law or legal provisions.

The European Council emphasizes that the objective of the Recommendation is to contribute to the development of common European standards. Common European standards are fundamental to warrant the principles for democratic elections in connection with e-voting, and to create confidence and trust in national arrangements for e-voting.

Furthermore, the interoperability of the voting systems across the member states is important. Regulations for interoperability and open technical standards within and across a member state may ensure combined and continued use of e-voting systems from different providers, and the national procurement costs are reduced.

The Recommendation is comprehensive with respect to statements and requirements on how an e-voting system should be designed, including requirements to meet the principles for running an election. The Recommendation does not comprise a complete set of regulations for the running of electronic elections. The standards must be seen in relation to, and be supplemented by, international commitments and relevant national legislature.

The regulations in the Recommendation should be seen as minimum standards. The legal standards are based on our cardinal democratic principles, and establish requirements, in addition to principles laid down in the national legislature, which must be met once the voters are given the option to vote electronically. The operational standards place requirements on the hardware and the software put to use in e-voting. The technical requirements involve the construction and use of hardware and software in e-voting systems, and are meant to guarantee technical security, availability and interoperability.

6.5 Democratic principles in elections – current legislature

In this section the working committee discusses the legal requirements that must be maintained if e-voting is introduced. The discussion is based on existing Norwegian legislature on political elections and the 2004 Recommendation. Existing legislature must be

supplemented by operational and technical requirements as stated in Appendix II and III of the Recommendation as well as by chapters 5, 8 and 9 of this report.

6.5.1 The Principle of Universal Suffrage

The Principle of universal suffrage requires a voting system which makes it possible for all entitled voters to participate in the election. Section 8-3 (1) of the Elections Act states that advance voting shall take place on "premises suited for the purpose". This regulation places certain requirements on the premises to be used as well as to the interior design of the stations. Details pertaining to these requirements are laid down in Article 26 of the statutory provisions for elections.
The same requirements must be maintained for polling stations used on Election Day, cf. Article 30 of the Provisions. It is particularly emphasized that special needs for voters with disabilities are accommodated. Good arrangements include well-designed ballot papers. Article 3 of the Provisions requires that the ballot papers are "reader friendly" Special requirements are stated for the size of the ballot paper, its colour, font and font size used, and the design laid out for making personal changes on the ballot.

The same principles must apply to an electronic voting system. The Recommendation states that unless the means to submit a vote outside the polling station are equally accessible to all the voters, such means should be offered only as a supplementary, optional voting channel, cf. Standard no. 4 of the Recommendation. The point is made to avoid the possibility that some voters are prevented from voting because the particular design of the voting system is a hindrance. The regulation is important in that equally accessible e-voting channels must be provided for all the voters, and traditional paper ballot systems must be preserved.

The design of a user interface in an e-voting system may be compared with the design of the paper ballot in manual voting systems. The Recommendation states that the user interface in an e-voting system must be understandable and easy to operate for the voter cf. Standard No. 1 of the Recommendation. Moreover, Standard No. 3 states that to the extent possible the system shall be designed in a manner that maximizes the accessibility for voters with disabilities. The objective must be to make all the voting channels maximally available, accessible and usable for the disabled.

To the extent it is technically possible and feasible, the user interface shall accommodate people with different disabilities. People with a visual impairment, for example, can not make use of a visual-only system, such as a touching screen, but need a special arrangement[48]. We recommend that the Web Content Accessibility Guidelines (WCAG) are adhered to by the user interface designers. The initiative to these guidelines was taken by the Web Accessibility Initiative (WAI) and is now known as the WAI-guidelines. The guidelines are also in compliance with the Norwegian strategy for ICT in the public sector[49].

6.5.2 The Principle of Equal Suffrage

This principle is fundamental and entails that each voter can submit only one counting vote. The system must ensure that the vote is registered and counted. This presupposes that the system can prevent a voter from submitting several counting ballots, prevent one ballot from being counted several times, being lost or changed in the transmission.

[48] Cf. Guidelines provided by the Delta Center at The Directorate of Health and Social Affairs, "Self service for all?"
[49] "Strategy for ICT in the Public Sector 2003-2005" (Norwegian version)
http://odin.dep.no/filarkiv/171428/AAD_IKT.pdf

The conditions stated are taken care of in the Acts and Provisions relating to Elections through the voters' register system, whereby a citizen's right to vote requires registration in the voters' register, cf. Chapter 2 of the Elections Act. When a ballot is cast, the voter may be asked to identify himself or herself, cf. Sections 8-4 (3) and 9-5 (2), to secure correct identity. In practice it is possible for the voter to cast more than one ballot. However, it is impossible to have more than one ballot approved. Our manual system is designed in such a way that when the voter has been crossed off in the voters' register, any subsequent ballot submitted by this voter is rejected. Cf. Sections 10-1 and 10-2.

Corresponding conditions must be secured in an e-voting system. The Recommendation states that a system must be designed to prevent a voter from inserting more than one ballot in the electronic ballot box. A voter shall be authorised to vote only if it has been established that his or her ballot has not yet been inserted into the ballot box, cf. Standard no.5 of the Recommendation. This does not mean that a voter cannot cast more than one ballot, but the system must secure that only one ballot from that voter is approved for counting. Correspondingly, procedures must be developed which ensure that if more than one voting channel is made accessible, only one ballot from each voter is approved, cf. Standard No.6 of the Recommendation. The regulation places requirements on the voters' register and corresponds to a manual system in which the principle of one voter, one approved vote is guaranteed.

Every ballot inserted in an electronic ballot box shall be counted, and each ballot cast in the election or referendum shall be counted only once, cf. Standard no.7 of the Recommendation. The regulation is identical with the regulations stated for traditional voting, although this has not been explicitly stated in the standard.

Procedures must be developed to provide a secure and reliable system for aggregating the ballots from different voting channels and for calculating the correct results, cf. Standard no.8 of the Recommendation. We also refer the reader to a technical description in chapter 8 below.

6.5.3 The Principles of Free and Secret Suffrage

The principle of free suffrage gives all entitled voters the right to vote for the party or list of candidates of his or her own free choice, without interference, coercion or undue influence from public authorities or any other authority. This entails an obligation on the part of the public authorities to make voting arrangements that guarantee that the principle is maintained. It means that the arrangement must secure the voter's opportunity to cast his or her ballot without undue influence. The content of a voter's ballot must be guaranteed secrecy.

Secret suffrage, however, cannot be an absolute requirement. Under certain conditions, considerations of the voter may suggest that an exception to this principle is accepted. Moreover, the authorities cannot guarantee that the voter himself or herself does not make his or her choice of ballot known to the public.

The principles of free and secret suffrage are provided for by the legal requirement stating that the voter shall cast his or her ballot in a secluded room, unobserved and in confidence, cf. Sections 8-4 (1) and 9-5 (3) of the Elections Act. The regulation applies to advance voting as well as voting in the polling station on Election Day, at home or abroad, and requires that the voter is alone when the vote is cast. Furthermore, our jurisdiction gives directions with

respect to who can be appointed Returning Officer. The regulations ensure a secure voting environment and mean that ballots can only be submitted to an already appointed and approved returning officer.

There is one exception to the requirement that the vote is cast ”in a secluded room and unobserved”. In consideration of voters who need assistance to cast his or her ballot the jurisdiction states that it is the task of the electoral official to provide this assistance. If the voter is seriously disabled physically or mentally, he or she can appoint an extra assistant, cf. the Elections Act, Sections 8-4 (1) and 9-5 (5). In consideration of the voter, an exception is also made for citizens who reside outside the country and do not have the opportunity to appear in person to vote in a designated place with a returning officer. These voters may submit a postal vote, cf. Section 8-2 (3).

The principles of free and secret suffrage must also be maintained if e-voting is introduced as an option. This is considered unproblematic if the electronic ballots are cast in controlled environments.

The problem arises as soon as the voting process is moved out of the public environment to a space in which it is not supervised and controlled by an election official. The voter will be personally responsible for maintaining the secrecy of the vote, and the authorities can not guarantee that undue influence is prevented. Nevertheless, this may not be a sufficient argument, in view of the fact that the authorities are legally obliged to make arrangements to secure secret voting without undue influence.

The individual citizen’s right to vote is an essential and fundamental principle. The Recommendation states that e-voting must be organized in a way which secures the voter’s right to freely form and express his or her own opinion, and, where required, personally exercise his or her right to vote, cf. Standard No.9 of the Recommendation. Some member states allow voting procedures in which the principle of universal suffrage has priority over the principle of personal attendance. The latter principle is of no relevance to Norway, as the Norwegian legislature on voting does not allow voting by proxy.

Standard No.9 of the Recommendation formulates requirements on the organization of the voting system to the effect that the principle of secret suffrage is maintained cf. also Standard no.16 of the Recommendation. It is somewhat uncertain that the problem related to the absolute maintenance of the principle in an e-voting system can be solved by formulating special provisions. The reader is referred to a discussion of the problem in 6.6 below.

The Recommendation requires that e-voting systems should be organized so that the secrecy of the individual citizen’s ballot, at any stage of the voting process, and in particular at voter authentication, is not endangered, cf. Standard No.16 of the Recommendation. This requires that the secrecy of the vote must be maintained at all stages of the voting process:, the pre-voting stage (relating to the transmission of PIN-codes or electronic messages to the voter), the voting stage (relating to filling out the ballot paper, casting the ballot) and the transportation and counting of the ballot. The principle places specific requirements on the design of the technical solution and must be expressively stated in the requirement specifications.

In a manual voting system a link between the vote and its voter will exist for a certain period of time, in particular with respect to advance votes, but under certain conditions also with

respect to votes cast in the polling station on Election Day. The procedures for establishing the link are formulated to secure secrecy in the best way possible. In advance voting the voter inserts his or her ballot in a ballot paper envelope. This envelope is subsequently inserted in a cover envelope along with the voter's ballot card holding information about the voter, and this is sent off to the electoral committee. The procedure for advance voting is necessary as long as the voter has the opportunity to cast his or her ballot in a voting district outside the municipality of his or her registered residence, and the ballot must be sent to the voter's municipality for validation. To cross the voter off in the voters' register once the ballot has been received, the Electoral committee must know the voter's identity. In a manual system secrecy control is secured, as a minimum of two election officials must be present when the polling card is physically separated from the ballot paper envelope containing the ballot, cf. article 35 of the Provisions**.** Correspondingly, a link must be maintained between the voter's identity and his or her ballot in an electronic voting system if the voter is given the opportunity to re-cast his or her ballot several times, or to change his or her mind in the process. Previously submitted ballots from this voter must be annulled if a new ballot is submitted by the same person.

The e-voting system shall guarantee that the ballots in the electronic ballot box and the ballots counted remain anonymous, and it must be impossible to reconstruct any link between the voter and the vote, cf. Standard no.17 of the Recommendation. This standard does not prevent a technical link to be maintained between the voter's identity and the vote at a given stage in the process, as long as secrecy is maintained. If the voter is given the opportunity to change his or her mind and submit a new ballot, it is necessary to store the link between the voter's identity and his or her ballot until the voting period is over. During this process secrecy must be maintained, which means that a cast ballot must be sealed and remain sealed throughout the voting process, the storing process and the withdrawal process. But the sealed vote must still be linked to the identity of its voter.

In traditional voting systems the voter identity and the ballot cast are kept separate by physical separation, which is easily audited by election officials and election observers. E-voting systems in uncontrolled environments require separation by electronic means. If the voter is given the opportunity to change his or her mind, the last ballot submitted is the ballot that is validated and counted. Only the last ballot submitted is inserted in the electronic ballot box when the voting period is over, and at this stage the connection between the voter and the vote is broken. Only the approved vote is inserted in the electronic ballot box. Any possibility of reconstructing the link after the ballot has been inserted and approved must be prevented. Electronic separation requires special technical solutions that must be formulated in the system specifications. Audit and certification of the system is a central prerequisite for e-voting, cf. Chapter 9 in the present report.

The e-voting system shall be so designed that the expected number of votes in any electronic ballot box will not allow the result to be linked to individual voters, cf. Standard no.18 of the Recommendation. Moreover, measures must be taken to ensure that the information needed during electronic processing cannot be used to breach the secrecy of the vote, cf. Standard no.19.

The required measures include the need to create a system for random storage of ballots in the electronic ballot box, to the effect that no systematic relation can be reconstructed between the order in which the votes are stored and the order in which they were inserted.

The requirement that the voter be secured the free formation and expression of his or her opinion must be maintained in the design of the user interface and in the way voters are guided through the e-voting process. Guidance must be given in a form preventing the voter from making a precipitate or un-reflected decision, cf. Standard no.10 of the Recommendation. ”Un-reflected” in this context implies that the voter must be given sufficient time to consider his or her choice before the vote is cast.

The user interface must be so designed that it does not permit any manipulative influence to be exercised over the voter during voting, cf. Standard no.12 of the Recommendation. This standard places certain requirements on the technical solution, but also on the user interface. Examples are special audio elements that are associated with a certain candidate or voting option, or pop-up screens promoting a candidate or a party.

Voters shall be able to alter their choice at any point in the e-voting process before casting their vote, or to break off the procedure, without their previous choices being recorded or made available to any other person, cf. Standard no.11 of the Recommendation. The voter is the only person to have access to the content of his or her vote. This means that the system shall not permit the voter to save the ballot in his or her personal computer or store it in the device used for voting, for example with the intention to submit it later. No system or person but the voter personally shall have access to the content of his or her vote, whether in the voting device or in the transmission of the vote to the ballot box.

The principle of free suffrage also implies that the voter has the right to cast a blank vote, i.e. the voter participates in the election but does not exercise a preference for any of the voting options cf. Standard no.13 of the Recommendation. The same right applies when traditional paper ballots are used cf. Article 20 of the Provisions for Elections.

The e-voting system shall indicate clearly to the voter when the ballot has been cast successfully and when the whole voting procedure has been completed, cf. Standard no 14 of the Recommendation. This standard places certain requirements on the technical solution and the user interface developed for e-voting to ensure that the voter knows when his or her ballot has been cast. This is important in order to create confidence and trust in the system, and in view of the principle that each ballot cast shall be counted. Furthermore the voter has the right to know when the voting procedure is successfully completed, in order to break the connection or leave the voting booth.

The voting process is successfully completed when the correct e-vote has been inserted in a secure electronic ballot box within the voting period (phase 1 or 2) and without access to intruders. In uncontrolled environments the procedure is not successfully completed until the ballot has been sent from the voter’s voting device (personal computer, telephone etc.) over the Internet or some other network and reached its destination, i.e. the ballot-receiving server. If the voter is given the opportunity to submit his or her electronic ballot several times (or also to submit a paper ballot), a system must be developed which ensures that only the last ballot cast is approved and inserted in the ballot box. A provisional ballot box may therefore be needed to store the e-ballots submitted in advance.

6.5.4 Is e-voting consistent with the Principle of Secret Suffrage?

The fundamental democratic principle of secret suffrage implies the voter’s right to cast his or her vote in privacy, unobserved and without any undue influence. In the Elections Act this principle is ensured in a number of ways. In traditional voting methods the voter is provided

with a balloting booth in which she or he casts her ballot unobserved and without any undue influence. To coerce a voter's choice of ballot is punishable by law cf. Chapter 10 of the Penal Code.

Given the opportunity to vote in uncontrolled environments, i.e. at home, at work, by post etc., this principle is seriously challenged. Under such circumstances the voting procedure is not supervised by an election official, which increases the risk of undue influence.

The question has been discussed by the Venice Commission. The Commission's opinion[50] was adopted in connection with the development of the Recommendation on standards for electronic voting. The problem presented to the Commission was the question of whether voting in remote environments without supervision is consistent with the ECHR. The ECHR secures the voter's individual right to cast a ballot by "secret voting". This right relates to the obligation of the authorities to make appropriate arrangements for voting *"under conditions securing the voter's right to freely express his or her opinion"*.

The question is relevant also in relation to voting by post (postal voting). Postal voting is considered a traditional form of remote voting in uncontrolled environments. The Commission refers to the fact that postal voting – remote voting in an unsupervised environment - has become common practice[51] in several member states in recent years, and therefore should be defined as a European Standard. This is a *common* European standard, and it is therefore used as a basis in the Commission's "The Code of Good Practice in Electoral Matters".

Article 3 of the ECHR clearly implies certain restrictions, since it has been claimed to impose a minimal standard on the member states to secure the secrecy of the votes. A standard of this type is defined on the basis of common legislature and forms the basis for the directives laid down in the Code of Good Practice in Electoral Matters. The directive for postal voting laid down in the Code, states that this form of voting is permissible only under conditions of a secure and reliable postal system. The Commission's opinion is that even though the Code is not binding, it is reasonable that the European standards included in the Code may have an impact on the interpretation of Article 3 of the ECHR.

With regard to e-voting, the Commission also refers to the Code of Good Practice in Electoral Matters, which states that this form of voting is pending the security and reliability of the system. Based on an analysis of postal voting in uncontrolled environments, the Commission states the opinion that similar standards may be developed for e-voting. In accordance with the ECHR, e-voting is not generally permitted, but not totally precluded. Acceptance is pending on the provision of acceptable legal, procedural and technical standards. Over time certain developed standards may become common practice.

---

[50] CDL-AD (2004)012 Or. Fr. Adopted during the 58th plenary session of the Venice Commission, 2004. http://www.venice.coe.int/docs/2004/CDL-AD(2004)012-e.asp

[51] Five countries permit unrestricted postal voting; Germany, Spain, the UK, Ireland and Switzerland. Postal voting is permitted in Norway only under the conditions that the voter resides abroad and does not have the possibility to cast his or her ballot with a returning officer at a Norwegian embassy or a consulate There are other varieties of postal voting opportunities in about half of the member states surveyed, in particular for citizens residing abroad. The survey, referred to in the opinion stated by the Venice Commission in the CDL-AD (2004) 012, was made by the EC in connection with the formulation of their Recommendation for Standards of e-voting. Moreover, Sweden introduced postal voting as a permanent option for citizens residing abroad as of January 1, 2006.

The Commission has thus come to the conclusion that e-voting is in compliance with European standards, and thereby also with the ECHR, on the condition that security measures are taken in the development of the procedures for this form of voting.

The question of undue influence in voting is especially relevant in connection with what has been called ”family voting”; in which a family member unduly directs another family member’s choice of ballot. The European Council has adopted a Recommendation, 2004 (1676), in which the Committee of Ministers is asked to draft a charter on ”electoral equality”, giving directives comprising all the measures that need to be taken to ban and censor ”family voting”. Initiatives in the form of attitude campaigns, training, sanctions against election officials who accept this form of voting, etc. have been proposed. However, the problem has not been raised with respect to e-voting in uncontrolled environments.

In a few court cases (Scotland 1922 and the US 1999), conclusions have been that the principle of secret suffrage does not oblige the authorities to guarantee absolute secrecy. The individual voter is also partly responsible.

The European Court of Human Rights has not taken up this question for consideration. However, when a system has been successfully practised in many member states over a longer period of time, this practice is an important source for the legal opinion of this Court (ECHR**).** This is also the case if a European standard has been adopted in the field.

The question of e-voting and its relation to the ECHR has also been taken up in the individual member states as they have run a variety of pilot projects on e-voting or introduced postal voting as a real option.

The UK has introduced the practice of postal voting in uncontrolled environments. This country has also had a variety of pilot projects on e-voting in uncontrolled environments. British authorities are of the opinion that this form of voting opportunity is unproblematic as long as the voters are provided with alternative voting channels

Professor Bob Watt at the University of Essex in England claims that international obligations prevent the introduction of e-voting in uncontrolled environments (Watt 2002). He refers to the fact that the ECHR does not contain a clause admitting exceptions. He also holds that postal voting and e-voting place the whole responsibility for guaranteeing voter secrecy on the individual voter.

Watt’s position has been countered. The argument is that his view expresses a rigid interpretation of the regulations. Many examples can be pointed to in which changes in society contribute to changes in the interpretation of legal terms and concepts over time. Moreover, some people claim that it is unreasonable that the ECHR should prevent a new development like the opportunity to cast an electronic ballot (Auer 2005). Auer asks whether the interpretation of the European Convention on Human Rights can possibly be so absolute as to encroach upon the possibilities that lie ahead with the creation of e-voting. He also argues that Article 3 should not be interpreted to prevent modernisation in the area of voting, particularly in view of drastically falling voter participation.

In this connection Auer refers to the flexibility of the Court and its stated opinion that "the Convention is a living instrument which must be interpreted in the light of present-day

conditions"[52]. He is consequently very sceptical to Watt's view that the Court will express an uncompromising attitude

6.5.5 Assessment and recommendations

The right to secret suffrage is one of the cardinal principles in our democracy, and must be maintained if electronic voting channels are introduced in election.

In the Opinion of the Venice Commission e-voting is not contrary to the principles laid down in Article 3 of the ECHR, provided that certain technical precautions are taken. Some people contest this opinion.

The members of this working committee agree that the authorities will have great difficulties in guaranteeing absolute secrecy in e-voting, as this is not even possible in a manual system. However, in our opinion the question is not so much about guaranteeing absolute secrecy as it is a question of how far the authorities must go to make provisions for securing that secrecy is maintained.

At the outset it is neither possible for the authorities to ensure that the voter casts a secret vote, nor that the voter is not unduly influenced. The question, therefore, is whether this problem precludes remote e-voting altogether or whether other initiatives may be taken to accommodate this fundamental democratic principle.

Undue influence has not been a great problem in the history of general elections in Norway. The principles of secrecy and freedom from undue influence are highly respected in our voting traditions. The problem has come to the fore only in recent years, and in the 2005 elections forced the regulatory authorities to tighten the rules pertaining to personal assistance in the polling booths. For the great majority of the people, however, the problem of undue influence is only distantly relevant. Why, then refuse a serviceable and useful procedure, if it causes a problem for only a very small minority of voters? One reason, obviously, is that the right to secret suffrage applies universally to all voters, not only to the great majority.

A major argument in the UK is that secret suffrage is taken care of as long as the opportunity to vote in polling stations is maintained. Another important argument is that undue influence is a punishable offence. Given that the opportunity to vote in polling stations is maintained, the voter must see to it that his or her vote is cast in the station. On the other hand, coercion itself is the problem, and this problem is hardly solved by giving the voter an alternative.

Opinions differ as to what extent e-voting is consistent with the principle of secret suffrage. No final answer has been reached on the question, not even in international circles. Eventually the question must be answered by national or international legal jurisdiction. Since the legal status remains unclear on this point, it is clear that great importance must be attached to experience and practice in a potential case for the Courts.

The Working committee takes the view that e-voting should not be introduced as a real option unless the authorities make the appropriate provisions for securing the secrecy of the vote and the voter's freedom from undue influence. Thus, several conditions have to be met before e-voting can be made a legal option.

[52] Legal decision of 18 February 1999 (Matthews vs. United Kingdom)

E-voting should only be made an option, i.e. an alternative voting channel. Paper ballot voting must be maintained, and the voter must have the right to choose his or her preferred voting channel. If e-voting is made an option whereby the voter may cast his or her ballot from home, the voter must have the right to change his mind and cast a new ballot, for example in a polling station, either in the advance voting period or on Election Day. Moreover, e-voting in uncontrolled environments on Election Day should be precluded, since this option would greatly restrict, if not forbid, the voter's chance to cast a new vote.

It is the Working committee's opinion that if Norway takes steps to introduce e-voting, the directives laid down in international legislation should form the basis for this initiative. Pilot projects are only feasible if the technical solutions are secure and reliable. The cardinal democratic principles must be implemented in procedures securing correct operation of the system. The technical procedures are pivotal for the success of an e-voting system, cf. chapter 8 of this report. A system for audit and approval of the technical solution is also of great importance, as will be discussed in chapter 9.

On a long-term basis the introduction of e-voting in election requires important revisions in our national legislation. We assume that a major revision is neither necessary nor wanted until e-voting is a realistic alternative on a large-scale or national basis.

Furthermore, the working committee considers it impossible at this stage to formulate definite proposals for legal regulations on e-voting. It is also impossible at this stage to make any clearer statements about the application of existing legal provisions. Before this work can be started, it is necessary to decide on the pilots to be run and their frameworks. Different solutions should be tested. In a pilot regime, considerations should be made with respect to how e-voting can be operated, what technical solutions should be provided and what consequences e-voting options have for the democratic principles, etc. In the end, these considerations will form the basis for formulating the legal provisions.

In the framework of a pilot regime e-voting may be sanctioned by existing, separate regulations on experiments. Rules and regulations for such pilots may then be formulated in separate provisions.

7 Economic and administrative considerations

7.1 Introduction

The present chapter focuses on the economic and administrative aspects of e-voting, based on the following specified tasks in the mandate:

- Consider the advantages and disadvantages of e-voting compared with regular voting in a polling station. (12)
- Consider costs related to large scale e-voting, on a short term as well as a long term basis, including the short term and long term cost reduction potential. (13)

First a brief account is given of central aspects of the Norwegian election proceedings. Then the economic aspects are considered, both with respect to current election proceedings and in view of the economic consequences of introducing various electronic voting solutions.

7.2 Election proceedings

Elections are held every other year in Norway, elections for local and regional councils alternating with elections for the national assembly and the Sami assembly. All levels of public administration are involved in the election proceedings. The Ministry of Local Government and Regional Development provides the general regulations, issues the guidelines to the electoral members, prepares information brochures of various kinds and provides a system for the central counting of the results. In elections for the County Council and the Municipal Council the regional authorities have certain responsibilities, such as issuing ballot papers, re-counting the received ballots and calculating the results. Elections for the Sami Assembly follow separate procedures laid down in special statutory provisions. The Sami Assembly is responsible for issuing the Sami voters' register, the ballot papers and some other materials, and distributing them to the municipalities.

↑*Optical scanner for reading ballot papers in the municipality of Oslo.*

All other tasks relating to the preparations and operations of an election in Norway are the responsibility of the municipal bodies, the electoral committee of the municipal council taking formal responsibility. The population of the different municipalities in Norway varies greatly, ranging from 200 inhabitants in the municipality of Utsira to 530,000 in Oslo. Although the municipalities must relate to the same Acts and Provisions (the Elections Act and its Provisions), the great disparity in size requires that they find very different means of organizing the elections.

The Elections Act and its Provisions along with a set of guidelines formulated by the Ministry of Local Government and Regional Development provide detailed descriptions of the different phases of preparing and holding an election. The work may be done on the basis of manual operation systems alone. This solution is normally chosen in the smaller municipalities. In other places some technical assistance is requested for the production of voters' registers, register maintenance and counting (calculation programs for the allocation of seats and the nomination of returning representatives). In the most heavily populated municipalities technical assistance is also used for the counting operation by means of optical scanners (OMR/OCR technology) which read the ballot papers and count them. The counting systems are combined with a system for calculating the results (seat allocation and nomination of returning representatives), securing fast and accurate counting and election results.

In smaller municipalities the municipal council and a secretary will do the job of preparing and running the election proceedings. They also form the electoral body in the polling station. If the municipality offers more than one polling station, a polling committee of at least three returning officers must be appointed for each polling station. The same rules apply to the larger municipalities, but the administrative challenges differ considerably. The electoral committee administrates the election by making administrative resolutions, but they themselves are not physically involved in the practical work.

The municipalities have to prepare a variety of premises for advance voting (permanent poll stations, institutions, secondary school buildings, colleges, universities, and provisions for voting from home). The premises for advance voting and for regular voting on Election Day must be prepared for the voting procedures. In addition to having a polling committee in each polling station, the station must be staffed with election officials who must be recruited. A central ballot receiving office must be organized for the final counting of the ballots.

Offering a variety of ways and times for the voters to cast their ballots, the Norwegian election system demands well-planned and well-organized arrangements in the individual municipalities. The local authorities must keep all the received ballots under control, keep correct records of the voters in the voters' register and cross off voters as they submit their ballots, make correct counts of the ballots and the personal changes that have been made on them. The results of an election are expected to be available very soon after the polling stations are closed on Election Day. Since the election proceedings are based on a traditional paper ballot system, most of the counting and audit routines will also be based on manpower intensive procedures. The complexity increases with the size of the population in the municipality. The more heavily populated municipalities do not enjoy any advantages of large scale operations in this context. However, they have seen the need to make use of modern technology to maintain control and accuracy and at the same time deliver fast results. On an overall basis, however, the cost per vote is higher for larger municipalities than for the smaller ones.

7.3 Elections in Norway – at what cost?

Due to the diversity of municipal structure it is hard to give a precise picture of the total cost of an election for all the municipalities in sum. The working committee has made some surveys in different municipalities. The level of cost is generally proportional to the number of citizens in the municipality. Expenses increase in the larger municipalities because more

electronic solutions are chosen which in turn require complex control routines and more people. The larger municipalities also pay higher salaries and fees. Furthermore, it may be assumed that there are hidden expenses related to elections in the municipalities, since a large amount of the preparation work is done by employees whose primary tasks and functions are not related to elections. Their salaries are paid for their primary functions. There are probably also differences with respect to how the internal/external resources are made visible in the budgets and accounts of the individual municipalities.

The municipalities are responsible for the operations in local, regional, national and Sami elections. In regional and national elections the county is responsible for printing the ballot papers and some other materials for use by the municipal bodies. The county also has the responsibility of re-counting the ballots and calculating the results at county level. In elections for the Sami assembly the Sami assembly is responsible for printing the ballot papers and other materials, and for producing the Sami voters' register for the individual municipalities. The counting of ballots for the Sami elections takes place in the 13 Sami voting districts in the country.

In compliance with the principles laid down for covering election expenses, each level of administration is responsible for covering the expenses related to their respective polls. For practical reasons, there are a few smaller exceptions to this principle.

The costs related to local elections are covered by the free revenues received by the municipalities (the sum of tax revenues and block grants). This means that there are no earmarked subsidies from the state to cover polling expenses. It also means that it is impossible to isolate the exact costs for election proceedings in the individual municipalities.

In 2003, expenses related to the national election were incorporated in the income system of the municipalities, as opposed to the previous system in which the necessary expenses were covered as per account rendered. The change was made to reduce the need for extra administration and audit costs in the local and regional government administrations.
Cost estimation for settling the amount to be incorporated in the income system was based on the accounts rendered for necessary expenses related to the EU referendum proceedings in1994. Including adjustments for price rises and an expenditure increase due to some new election legislature, the expenses amounted to a total of 111.5 million NOK. An additional 5 million NOK was covered for the expected expenditure increase due to the new legislation on elections. In other words, a total sum of 116.5 million NOK was added to the amount already stipulated for the local elections.

¼ of the amount is incorporated into the municipal income system annually. The individual municipality's share varies according to the different criteria set in the income system.

The costs for the regions, on top of the limit set by the budget framework, are estimated at 17.2 million NOK. ¼ of the amount is incorporated into the county income system annually.

In addition to this, funds are set aside in the budget of the Ministry of Local Government and Regional Development for covering the Ministry's election costs. The state covers expenses related to the following tasks (all elections):

- Advance voting proceedings abroad (printing and distribution of materials).

- Printing and distribution of ballot paper envelopes and ballot papers without candidate lists for the advance voting proceedings.
- Development and operation of electronic equipment for collecting processing, prognosticating and distributing election results.
- Central information initiatives.
- Expenses relating to election proceedings in the Sami elections.

In the 2003 local elections 29 million NOK were set aside in the state budget for covering election costs. In 2004, 5million NOK were set aside, in 2005 the amount was 31.7 million NOK.

The costs that were to form the basis for the amounts to be incorporated in the income system were estimated at a total of 163 million NOK. In that same year 2,050,000 ballots were submitted in the local elections. The calculated mean cost per cast ballot amounts to NOK 80, of which NOK 57 are covered by the local government.
The costs related to holding elections spread over different types of costs, which have been tentatively grouped into the following:

- Human resources: Manpower costs on the whole comprise payment to people working in the polling stations on Election Day, either in the form of reimbursements for working overtime or in the form of regular rates. Furthermore, a great deal of the work related to advance voting takes place outside regular working hours (premises for voting have to be open in the evening, central ballot receiving premises must be open at night, advance votes must be validated and sorted for counting), all of which requires reimbursements for overtime work or other regular payments. Final counting after the polling stations are closed on Election Day takes place in the evening and during the night, which again means extra manpower expenditure. Many municipalities can cover the manpower expenditure by re-allocating their own economic resources, which is not always made visible in the accounts unless salary expenses are reimbursed. Some municipalities are not able to recruit enough manpower among their own employees, and have to resort to hired labour.
- Data system/voters' register: A great number of municipalities make use of computer systems which give access to electronic voters' registers. The electronic registers are used during the advance voting period to cross off voters who submit advance votes, and the crossed off voters' register is printed for use in the polling stations on Election Day. The system is also used to calculate the results and the return of representatives for the individual municipalities (local elections). Municipalities with a large number of citizens also make use of the computer systems to count the ballots.
- Materials (ballot papers, voting cards): A considerable number of ballot papers have to be produced before an election. Different types of envelopes, forms etc. are also needed. The quantity of produced materials is a lot higher than one might think necessary in view of the received number of ballots. However, voting takes place in a number of places simultaneously, and one would not want any place to go short of ballot papers for any party. A lot of the materials is marked for the election in question, and may not be re-used in another election.
- There may be a need for ballot boxes and other materials for the advance voting period, but heavier costs relate to the production and distribution of voting cards to the voters for the municipalities that decide to use this system.
- Polling stations/equipment: A lot of the equipment needed for the poll may be used again, or is also used for other purposes (chairs, tables etc.). Polling booths may have

to be renewed, and equipment is needed for signposts to give directions, posters of different kinds, and other materials.

- Information: The Elections Act requires that the municipalities take certain information initiatives in the form of announcements to the voters. The municipal governments may also decide on other information initiatives, such as issuing different kinds of election campaigns: brochures of various kinds may be sent to the households, posters are hung in public places, ballot papers and party programs may be distributed in various places, etc.

The chart in figure 7.1 illustrates the distribution of costs related to the 2003 local elections in the municipality of Drammen.

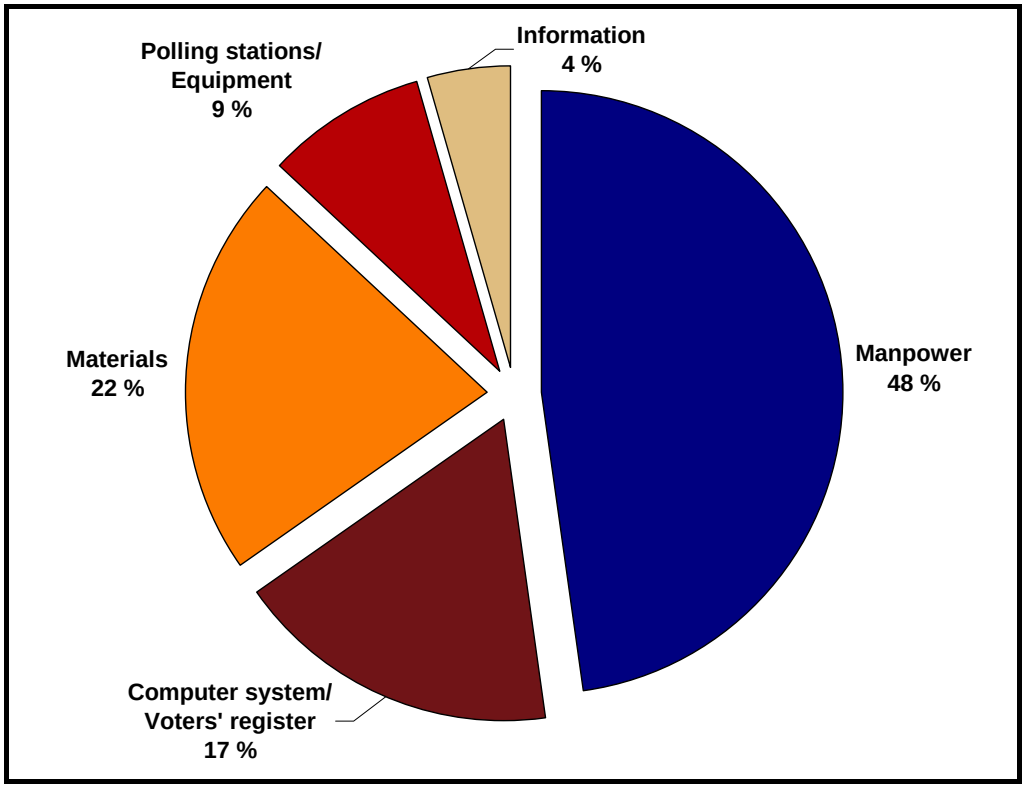


Figure 7.1: Distribution of costs related to the 2003 local elections in the municipality of Drammen.

The total costs related to the 2003 local elections in the municipality of Drammen are estimated at 2,300,000 NOK. Cost distribution is estimated on the basis of the polling operations for the local government elections and the municipal responsibilities related to the county elections. Corresponding estimates have been made in the municipalities of Trondheim and Oslo. The cost distribution has also been presented to the municipalities of Steinkjer and Grong, as examples of smaller municipalities. Estimates and surveys show that the distribution of costs is much the same in the different municipalities. Differences relate to the technical solutions chosen in the different municipalities, their payment rates, the choice of using voting cards as part of the system, etc. As already accounted for in this chapter, the differences also affect the total costs of the respective municipalities.

It is hard to estimate the cost distribution for the poll in the polling stations on Election Day and the advance voting period. In the 2005 national elections 17.9% of the votes were cast as advance votes. In view of the fact that advance voting is a more complex process, both in

terms of the voting means made available and in terms of the audit procedures, the costs related to advance voting are assumed to be higher than for voting on Election Day.

7.4 Economic assessment of various e-voting solutions

The previous section has demonstrated that there are two essential cost elements related to the election proceedings. One is manpower expenditure, which makes up about 50% of the costs, the other is the production and distribution of materials, which makes up a good 20%. If one of the objectives of introducing new technology is to reduce costs, considerations should be directed to these two areas in particular. The local and regional share of the costs related to these two groups makes up a total of about 100 million NOK.

7.4.1 Electronic voting in controlled environments

E-voting in controlled environments means that the polling stations are equipped with computers from which the voters cast their ballots and have their ballots registered in a computer system, either by being stored locally in a medium which is transported to a central counting unit or by being stored in a central counting unit via a telephone line (or other line). The effects of this system are a reduction in counting mistakes and faster results after closing.

In principle, there are two alternative solutions for the voters in the polling stations. One is to use equipment specially designed for electronic voting purposes. An example is the touch screen machine that was used in the pilots on e-voting in the 2003 elections. The unit was designed to make the voters cast their votes by pressing a finger against the chosen tickers on the screen. The other alternative is to use standard computer systems (traditional personal computers), in which case the voter may have to operate the keyboard and the mouse to submit their vote.

Time-consumption

An important point to consider for assessing e-voting in the polling stations as a real option, is the time it takes for the voter to cast his or her vote. The tendency over the last years has been that the voters spend more time in the polling booths and make more personal changes on the ballots than earlier. At the same time, there is a pressure to speed up the transportation flow, as queuing is less tolerated today than it used to be. Polling station capacity is therefore a critical factor and should be taken seriously.

In systems where the voter votes for a single candidate or a party, the time for casting a vote is probably the same whether the ballot is cast manually or electronically. The more options the voter is given for personal changes, however, the more functionality is required of the electronic solutions, and the longer it will take to try out the different possibilities before the voter finally submits his or her ballot. This assumption is based on the experience drawn from the pilot using touch screens in the 2003 local elections in Oslo. Time studies were not a defined issue in the pilot, but user responses and observations suggest very strongly that the voters spent more time to cast their votes on the touch screen machines than what is normal in traditional voting procedures.[53]

[53] Oslo municipality made a user survey during the 2003 local elections in which two differently designed technological voting solutions were put to use for the voters. The equipment was tested, but in addition short, random timing observations were made to get an impression of the time consumption of each voter.

The timing observations made in the 2003 elections indicated a mean time of 3 minutes per voter. Theoretically, then, a touch screen machine open for 11 hours can accommodate 220 voters. As the rush of voters to the polling stations is uneven, the greatest rush being between 4 pm. and 8 pm., a polling station offering a touch screen system only, must be equipped with considerably more voting machines than the theoretical estimate above indicates. A touch screen solution in the polling station will imply, in addition to the investment in the equipment itself, an increased number of polling booths, larger premises for polling and possibly also more manpower, with the ensuing increases in costs.

Specially designed equipment
As mentioned above specially designed computer solutions were used in the 2003 pilots. Today touch screens are used for many purposes. They are used extensively for checking in at the airports, where the passengers act by touching the screens in accordance with the instructions given. This technology has the advantage of being self-explanatory, and the functionality is simple in that different sections of the screen are touched according to instructions. This advantage is confirmed by the responses in the 2003 pilots. The voters responded positively to the touch screen voting technology.

At this point in time, it is hard to estimate the investments needed for specially designed equipment in the polling stations. Detailed analyses must be made, and a possible pre-qualification of certain service suppliers should be made before more exact estimates may be made. In the 2003 pilots, it was suggested that an electronic voting unit would cost around 30,000 NOK. Considering the price development of computers, as we know it, prices would be considerably lower today. If elections were to provide this voting option today on a large scale basis, considerable investments would be necessary. Additional costs would include expenses for rigging, dismantling, packing and storing the equipment between elections, which may amount to considerable expenses. If an electronic link is to be made between the voting unit and a central counting unit, there will be extra expenses related to the establishment of this connection.

It is also hard to estimate the durability of the equipment, although it is assumed that the investments may be distributed over at least a few elections. Computer equipment is normally written off over a relatively short period of time. The frequency of use is low as elections are held only every other year in Norway, which makes it uncertain that the suppliers will make any profit if they let them out for hire.

Standard computers
The considerations made above with respect to specially designed hardware and software also apply to solutions with regular computers. The expenses related to each voting unit will probably be reduced, but these computers are not normally equipped with touching screens. Hardware and software requiring the use of a keyboard or a mouse are not as user friendly as the touch screens. This implies that the voters will spend more time in front of the computer. As this option has not been tested in Norway on the basis of current legislation on elections, it is hard to estimate exactly how long it will take the voter to submit his or her vote, and so also to estimate the number of computers that will be needed. It does not seem unreasonable to think that they would need just about the double amount of time in front of the computer compared with the time needed for traditional voting procedures with ballot papers provided in the polling booths. In other words, twice the number of polling booths will be needed. An increased need for manpower in addition to the investment in the equipment implies that the

solution will not be much less expensive than the solution with specially designed voting machines.

Depreciation is considered the same for the two alternatives above. However, the use of regular computers may be coordinated with the general need for computer renewals in the local administration. This solution is assumed to be of interest in the smaller municipalities, where the purchases and distribution are made centrally. In larger municipalities organized into big, independent units, this solution will require very complicated coordination tasks, especially in view of the great demand for computers for the election. It will also have serious consequences for other local management if the local administration takes a great number of computers out of their ordinary use to make them available for voting purposes.

Economic assessment
E-voting in controlled environments does imply some saving. Expenses related to the production of ballot papers will be reduced. Some of the tasks related to the counting operation will also allow a certain reduction of manpower. Provisional counting of electronically submitted ballots will not be needed. There is also a potential expense reduction related to the optical scanning of ballot papers.

Whether a touch screen machine or an ordinary personal computer system is chosen, electronic voting in the polling stations will require heavy investments in new equipment. As electronic voting takes more time than voting by traditional means for the individual voter, the polling stations must be equipped with more booths, or more polling stations must be made available. The local administration will incur great expenses for rigging, dismantling and storing the equipment. Election officials must be available in the polling stations, and more people will be needed to assist and control the operations. The ultimate outcome of these increased expenses seen against the saving mentioned above, will depend on the individual municipality's way of organizing the operations. E-voting in polling stations will require new and different costs, and will not necessarily yield economic efficiency gains.

7.4.2 Electronic voting in uncontrolled environments.

E-voting in uncontrolled environments means casting one's ballot over the mobile phone, over the Internet, TV, an electronic terminal or any similar electronic equipment. This type of voting option requires that the public sector organizes the poll by making the necessary computer systems for ballot submission available for the voter and at the same time systems must be developed for receiving and registering the ballots and for crossing off voters in the voters' register. Taken to its extreme, such solutions might have the effect that the local administration no longer needs to make polling stations available, which would mean drastic cost reductions in relation to manpower and equipment. Since the voter will personally own the equipment needed for submitting his or her vote, major expenses related to this part of the election will be transferred from the local administration to an already existing private system. On the whole, the equipment will be in the possession of private persons (personal computers, cell phones, TV sets, etc.) or private agencies (electronic terminals). Although technical equipment such as personal computers, cell phones and TV sets is very widespread in Norway, it must be taken into consideration that some voters will not have access to any such equipment. Such equipment, therefore, must also be provided by the local authorities and made available to the public for voting purposes. Public expenditures will still be needed for electronic voters' registers, systems for electronic voting, electronic counting, publicly available equipment for casting the ballot, information initiatives/training and some manpower.

The costs related to electronic voting in uncontrolled environments are so far hard to estimate. The main costs will be related to the system development and implementation. Costs related to this are hard to estimate as long as no precisely defined requirement specifications have been made that may be tested on the market. The level of cost will depend on the chosen complexity of the solutions relative to for example the level of security.

In addition to the efficiency gains mentioned for e-voting in controlled environments, e-voting in uncontrolled environments will drastically reduce the need for polling stations and the accompanying manpower needed. This alternative may yield great efficiency gains related to manpower, equipment and materials.

7.5 Administrative considerations

No specialized formal competence is required for preparing and running traditional elections in Norway. What is needed is knowledge about and insight into the work that has to be done from the start to the final election results. The formal requirements are taken care of if the regulations formulated in the Elections Act and the guidelines provided by the Ministry of Local Government are followed. Administrating and running the election requires knowledge about the procedures, routines and the geography of the respective municipalities. It also requires the ability to be structured, accurate and results oriented.

The Elections Act defines the electoral committees' responsibilities in their respective municipalities. The electoral committees determine the voting district divisions and decide on the premises in which polling may take place. They also approve candidate lists for local elections. The electoral committee appoints returning officers for the advance voting period. If the municipality is divided into several voting districts, polling committees are appointed to administrate the election in the individual polling stations on Election Day. The electoral committee makes the records in the local voters' register and is responsible for the supervision of every part of the voting event.

Although the Elections Act is formulated for a traditional, paper-based election system, several municipalities today make use of technological support in their work.

Further development of technological solutions will contribute to make the comprehensive, manual procedures of holding an election much simpler and more efficient for the local administration and reduce manual errors. New technological solutions will also contribute to getting faster and more accurate results. Modern technology will also help to improve the voting conditions for voters who need assistance in another language, or voters with visual impairment. By permitting voting over the Internet the voting act will be more accessible for physically impaired voters.

However, the introduction of modern technology requires more competence than traditional procedures. The Norwegian municipal structure, involving many very sparsely populated municipalities, does not guarantee that there is sufficient competence in the local administration to make use of the technology in the restricted area of elections. This is a cause for worry, not least if it is used extensively. Consequently, there is a certain risk that it will be the service providers who state the premises for the solutions and for the whole operation. In view of such prospects, a national coordinating and administrative authority should be

considered, to take responsibility for the technology used in e-voting. The state should be responsible for formulating the required specifications and make provisions for certification and accreditation arrangements.

Extensive resources are put into running elections in Norway. It ought to be a central condition for using modern technology that the financial resources needed are reduced rather than increased. We refer the reader to the cost distribution list above, in which it was seen that 50 % of the expenditure on elections relates to the human resources needed. The long-term goal outlined by the working committee is in accordance with a request for cost reduction. Pilot activities, however, imply an increase in administrative and financial resources required, because the electronic solutions are used to supplement the traditional procedures. It is not to be expected that the municipalities can increase expenditures for pilot projects of the kind discussed in the present report. In the opinion of the working committee, such structured, goal-oriented pilot projects should be financed by the State.

The working committee assumes that electronic voting in uncontrolled environments are related to the possibility of re-casting one's ballot, as this is meant to take care of the secret voting requirement, and to prevent undue influence. Traditionally, to make the option of re-casting a vote available to the voter, comprehensive administrative procedures are needed to ensure that the voter only submits one counting ballot. As long as the opportunity to vote again is restricted to e-voting in uncontrolled environments, the electronic system will automatically validate only the last ballot submitted. If a voter who has submitted his or her ballot electronically, decides to vote again in the polling station on Election Day, the election official must see to it that the electronic system is informed that this voter's electronic ballot is annulled. The working committee has not come up with a precise description of how this may be done, but assumes that the extra workload for the election official will be minimal, on the assumption that very few voters will make use of this opportunity.

7.6 Recommendations

E-voting will have a number of administrative advantages in that the accuracy of the voting results are improved and the final calculation of seat allocation and nomination of returning representatives will be available faster. E-voting will also help to reduce a number of manual procedures and control routines which are associated with high costs. E-voting in controlled environments, however, will require new expenditures in the form of investments in computer equipment, rigging and more booths, possibly also more manpower in the polling stations than at present. The working committee assumes that cost reductions and the reduction of other resources are likely only when e-voting in uncontrolled environments is introduced on a large-scale basis.

In conclusion, the level of cost will be at least as high as it is today as long as the traditional voting procedures involving paper ballot voting are maintained. Only when the number of voters submitting traditional paper ballots is declining in favour of voters who submit their ballots electronically in phase 1 by means of their own electronic equipment in uncontrolled environments, will there be a reduction in the level of cost and the need for resources.

8 Technical challenges and possible solutions

In the present chapter we take up the following tasks defined in the mandate:

- Give an overview of different systems by which a vote may be cast electronically through different channels (Internet, touch screens, SMS, digital TV, etc.) (2)
- Point out advantages and disadvantages of the different systems/channels (3)
- Assess the different systems/channels with respect to user friendliness and security of the votes (4)
- Discuss and assess the recommendation of e-voting by means of Internet technology in as well as outside the polling stations (5)
- Consider solutions for proper identification and authentication of a voter ready to submit an electronic ballot (smart card, ID card, etc.) (6)
- Consider the introduction of verification solutions in the systems, and recommend possible procedures for such solutions (9)
- Consider the problems related to open source codes (10)
- Consider the use of an electronic Population Registry, and its implications for an e-voting system (11)

8.1 Conditions for technical solutions

In this section we sum up the conditions that must be met in a technical solution for e-voting, as arrived at in the previous chapters:

Two phase election
Elections in Norway will still be run in two phases (known as an advance voting period and a voting period on Election Day). The first phase runs over several days, or weeks or months, while the second phase is a one-day election (possibly two days). Between the two voting periods there is a break, the duration of which may be determined later.

Electronic voting in phase one only
The working committee's studies show that introducing e-voting in controlled environments is very expensive and the gains are rather limited. The election results will be arrived at faster with less human resources, but the cost of equipment and arrangement will be higher than if our current system is used. Only if the solution is based on technical equipment owned and administered by the voters themselves, will there be a potential for considerable reductions in election costs. Moreover, a well tested traditional voting system in the second phase should be maintained, not least as a safety measure in case problems arise with the electronic solutions in the first phase.

No changes in the voting procedures in phase 2 (on Election Day)
Voters who prefer to cast their votes in the polling stations on Election Day will still be able to do so in the future, in accordance with traditional procedures. Electronic solutions, therefore, must be designed in a way that does not affect the procedures of a traditional paper ballot system.

Different voting channels
The technical solutions should make it possible to introduce several voting channels in phase 1 of the elections. Possible channels are the Internet, a mobile phone (SMS) or other future channels.

The principle of repeated ballot-casting
A voter should be able to cast a ballot several times, but only the last ballot registered from this person is counted. In the second phase a voter may cast his or her ballot only once. A ballot cast by a voter in a controlled environment in phase 2 overrides all other ballots cast by that voter in the first phase. An electronic ballot from a voter is not a valid vote inserted in the electronic ballot box until it is made clear that this voter has not cast his or her ballot in the polling station on Election Day. A voter casting a paper ballot, whether in phase 1 or in phase 2, does not have the opportunity to cast a (new) ballot again, whether in the first or the second phase of the election.

Compromises will affect the e-voter, not the traditional voter
If compromises with respect to the voter's privileges cannot be avoided in an electronic voting solution, they should only affect the e-voter, not the voter casting a paper ballot.

E-voting requires that the voter pass personal information to the voting system (server). In the worst case this information may be used to disclose the voter's identity. Thus the voter must trust that the system processes this information correctly, and that there are adequate provisions for keeping the voter and the content of his or her vote apart. The situation is analogous to the manual system of advance voting or distant voting in which the ballot (placed in an envelope) is inserted in a cover envelope identifying the voter. The voter has to trust that his or her ballot is separated from the cover envelope in a way that secures the anonymity of the ballot.

However, the working committee is of the opinion that a somewhat higher risk that the voter identity is linked to the content of the ballot may be acceptable if this acceptance simultaneously guarantees that the voter's ballot is registered correctly.

The user interface design
The EC Recommendation on e-voting emphasizes that the user interface should be of a very high quality, cf. Standards no 47 -50 of the Recommendation. This implies that in designing the user interface it is of utmost importance that the presentation is neutral with respect to the voting options. Furthermore, voting in political elections is not an everyday task, which means that the user interface must be user friendly. The WAI- guidelines[54], intended to accommodate people with disabilities, should form the basis for the design.

The technical solutions should satisfy the standards of the EC Recommendation on e-voting
A number of technical requirements have been listed in Appendix III of the Recommendation. This working committee assumes that future solutions developed must satisfy these standards. In the present chapter we consider only the most relevant requirements listed in the Recommendation, and relate them to the overall conditions for technical solutions.

[54] Cf. W3C Web Accessibility Initiative at http://www.w3.org/WAI/

8.2 Identifying the challenges

Electronic voting solutions have obvious advantages, such as wide availability, procedural simplicity and counting efficiency. At the same time they create a number of challenging problems. Based on the fundamental democratic principles, the following challenges are defined:

- Ensure that the voter is able to cast a ballot.
- Ensure that only one ballot cast by a voter is counted.
- Ensure the secrecy of the vote.
- Ensure that the vote is not changed or falsified.
- Ensure that a cast ballot is not lost.
- Ensure that no fake ballots (votes that have not been cast by an eligible voter) are inserted into the voting system..

In Norway the voters have great confidence in the legitimacy of the elections. Traditional methods based on paper ballots are in principle so simple that the citizens can understand them and observe them in a way that makes them transparent to the layman. Once the ballots cast by the voters are read and processed by a computer, all layman observation and control must be replaced by trust in the experts who have designed, programmed, tested, controlled and certified the system. A lack of transparency and no real layman control raise questions with respect to the integrity of the system and a possible undermining of people's confidence.

Introducing new technology in the voting system also introduces new threats. Although current manual systems are not completely flawless, the threats related to them are of a kind that requires a number of independent errors or *infidels* to have any real consequences for the election results. An electronic solution enables a person with sufficient access to the system to make small changes in the system solutions, which may affect a great number of ballots. Computerized ballot storage also avails itself to threatening manipulation (extensive manipulation threats)

The main elements of an e-voting system are the following:

- The voter client – The computer used by the voter in casting a ballot
- The ballot receiving server – one or more computers receiving and transmitting the ballots cast by the voters
- A data line or a data network between the voter client and the ballot receiving server
- A core system of one or more computers, uploading the ballots from the ballot receiving server and doing further processing.

It is generally impossible to guarantee that an electronic system is absolutely flawless (Schneier 2004). The question is what failure rates may be tolerated in the different applications, and what initiatives may be taken to counter possible faults. Problems related to the security of the Internet are well known and have been widely discussed in the literature. A number of assessment reports and security analyses have been published on Internet-based solutions[55] and specially designed voting machines used in elections[56]. Generally, the

[55] The US Department of Defence developed a pilot on voting over the Internet meant for some Military personnel stationed abroad during the 2004 Presidential Election. The solution was assessed by an expert group during the fall of 2003. Four members of the expert committee published their own assessment report (Jefferson et.al 2004) concluding that the solution developed was not to be recommended. The most important threats, in their view, were possible attacks against the voters' computers, the vulnerability of the Internet, and the use of

introduction of computer systems implies a certain risk of programming errors and technical breakdowns of central components. The use of new technology also avails itself to errors resulting from user incompetence or user inadvertency.

In Appendix B we sum up the most important security challenges related to e-voting in uncontrolled environments. Other e-voting solutions are considerably less vulnerable to fraud or error.

The greatest technical challenges associated with introducing electronic voting are:

1. Fraudulent computer software in the voting client.
2. General vulnerability of the computer networks, the Internet in particular.
3. Difficulties in obtaining redundant data for trustworthy verification of counted results.
4. Inside attacks intended for sabotage or the manipulation of voting results, in particular attacks on the ballot receiving server and the core system.

Security is a central issue in the discussion in the next sections. Particular attention is paid to measures that may be taken to protect against the threats listed in 1-4 above.

8.3 Alternative solutions

In this section we discuss different electronic solutions for the voting stage of the election, cf. Fig. 8.1 below. The voting client machine may be anything from a large computer to a handy size device like a cell phone. The voting client may be made available to the voter in a public office or in other suitable premises, or it may be a machine at the voter's personal disposal at home or at work. The ballot receiving servers – several servers activated during the election – should be placed in a secure environment protected by the electoral authorities. The voting client and the ballot receiving server are connected by a data network, either a local, closed network or the Internet.

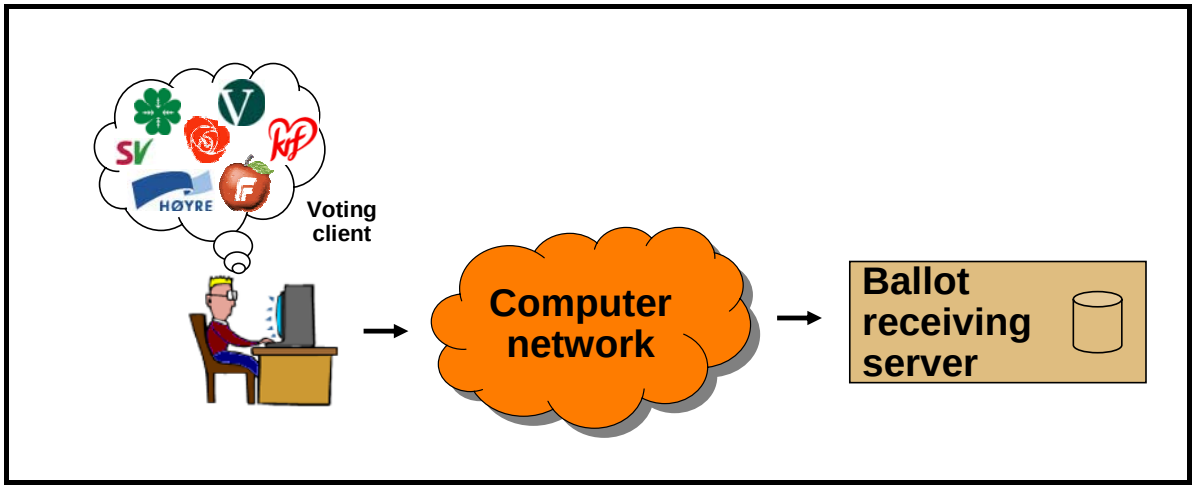


Figure8.1: Voting client and ballot receiving server

specially designed software controlled by the providers. They did not recommend continuation of the pilot, and the system was not used in the 2005 election. The conclusions drawn in the assessment report are interesting and relevant, but it should be emphasized that the assessment relates to a special version of VOI. Internet solutions may be developed using other characteristics and other security levels.

[56] See publications by Rebecca Mercuris on e-voting solutions at http://www.notablesoftware.com/evote.html

The problem we are facing with current technological equipment available in the workplace or at home is that it is impossible to guarantee one hundred per cent secure transmission channels in uncontrolled environments. Yet, innumerable security sensitive transactions are performed every day by means of this equipment, as for example banking transactions over the Internet. Such transactions are acceptable because control systems are available (we can check the correctness of the transaction in our bank statements), and – in the banking example – because the banks are responsible for any errors not attributable to the user. Electronic ballots cannot be controlled in the same way because the content of the ballot submitted must be kept secret. An alternative solution may be to duplicate the ballot in order to retrieve the duplicate if any doubt is raised with respect to the processing of the original ballot cast by the voter. The problem with this alternative is that the transmission of the ballot from the site where the voter can ascertain the correctness of his or her ballot to the duplication site must be sufficiently secured. This is the crux of the problem: How do we measure the "sufficiency" of a "sufficiently secure" system, and how is "sufficient security" achieved?

8.3.1 Electronic solutions in controlled environments.

When electronic solutions are made available in controlled environments, the electoral authorities are present to audit and control the hardware and the software used, and the data are communicated over secure networks, cf. fig. 8.2 below. Moreover, a log may be produced, keeping records of the cast ballots (paper copies for example). The system may be designed so as to let the individual voter verify his or her ballot before the send-button is pushed. This enables the voter to verify that the information received by the system is correct (cf. Section 8.7.4 below). Given this verification procedure, there is no need for an absolute security requirement attached to the transportation of the ballot to the ballot receiving server.

Two different voting client solutions are of interest: either the voting client is a personal computer or it is a voting machine specially designed for the purpose.

A personal computer

A personal computer is really too complex for the task of serving as a voting client. Its complexity also makes it an unsafe alternative. The good thing about it is that it is mass produced, which implies that it is cheap, spare parts are easily available, and it may be used for a multitude of purposes in between elections.

Although a demanding job, in controlled environments the task of testing and controlling the system thoroughly enough to create confidence in its functionality is not impossible. However, it does require a solution which is founded on well-planned, verifiable system architecture. If the hardware is equipped with a newly installed operating system, it should be reasonably well protected against fraudulent software. An alternative solution is to boot the computer from an election CD-ROM made for this particular purpose. (cf. section 8.3.2 below).

Voting machines

In controlled environments specially designed voting machines are an alternative to the personal computers. A voting machine is typically equipped with an operating system and a software solution designed for this particular purpose. It is normally operated by having the voter press his or her finger against a touch sensitive screen. The most obvious variant is electronically connected to a ballot storage server, which means that the ballots are not stored in the voting machine, but in a central server.

The advantage of this type of electronic voting machine is that it is specially designed for the purpose, and the amount of potential distraction is kept to a minimum (compared with voting from a personal computer with Internet access). Since the system suppliers are in control of the hardware and the software, it is also relatively easy to verify that the system is not modified, virus infected or the like.

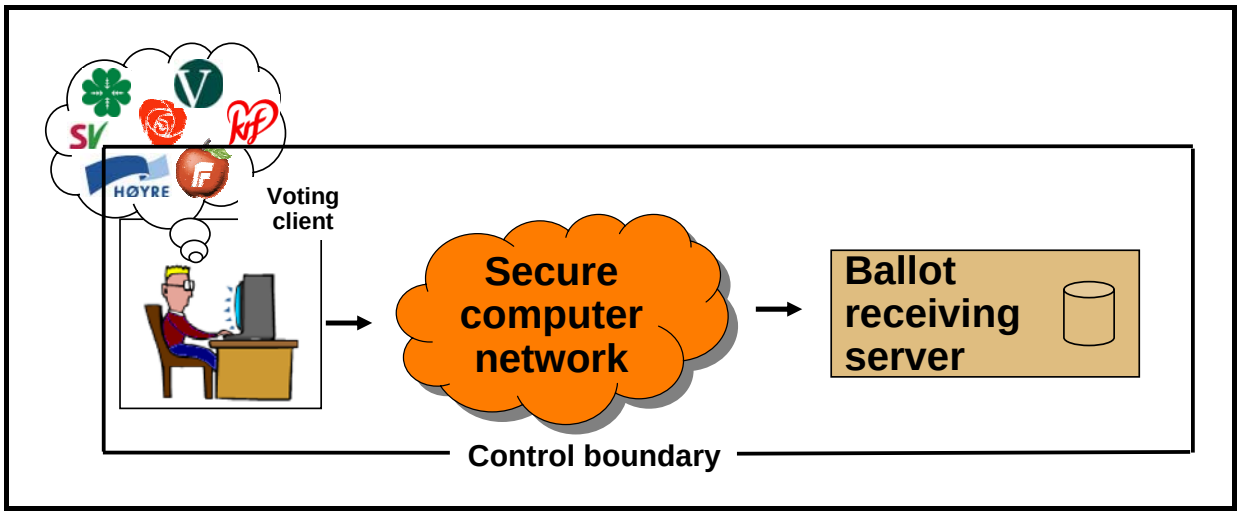


Figure 8.2: Voting in controlled environments

A touch screen voting device may be set up without any specially designed software solutions since a touch screen may be connected to an ordinary personal computer. In other words, the advantages of not having to use a keyboard and a mouse are not restricted to the specially designed voting machines. This means that the difference between a personal computer solution and a specially designed solution is only a relative one.
The working committee is of the opinion that the same software solutions should be used as far as possible in all the technological platforms chosen – whether in controlled or uncontrolled environments. Choosing specially designed voting machines for kiosks or polling stations may therefore be a blind alley in view of finding a lasting solution, since this technology may not be used in all channels.

8.3.2 Electronic solutions in uncontrolled environments.

The introduction of voting in uncontrolled environments not only challenges the principles for democratic elections (cf. Chapter 5), it is also a challenge to the security of the voting system. The voting client used by the voter is hardly available for inspection by the electoral authorities, and the data communication utilizes public networks such as the Internet, cf. fig. 8.3 below. External threats are thus a potential danger which impedes the objective of guaranteeing a well functioning voting system. Not even a series of successful tests or actual operations is proof good enough that an attack may not be mounted on the next occasion. Since the system connecting the voter to the rest of the voting system is insecure, it is extremely difficult to ensure that all the ballots cast are securely logged (see also section 8.5.2 below).

The challenges peculiar to voting in uncontrolled environments may be countered in two different ways:

- Provide the voter with technical solutions with considerably higher security than the solutions currently available, and make use of more secure data communication channels.

- Establish communication between the voter and the voting system by means of parallel, technically independent channels, to ensure that the voter may verify his or her ballot or have his or her ballot verified.

Current technology is encumbered with weaknesses which may be exploited for voting fraud. As secure solutions for electronic transactions in uncontrolled environments are needed on a general basis – not only for electronic voting – there is reason to believe that tamper-free electronic devices will be developed in the future, either as independent units linked to the Internet or to the cell phone network, or as accessories for personal computers or cell phones.

In the meantime, one possible solution is to give the voter the opportunity to cast his or her vote twice, through two technically different and independent channels (for example, a personal computer with access to the Internet and a cell phone), and have the ballot receiving server approve the ballot only if the contents of the two submissions are identical. The idea is that the probability is about nil that the same mistake occurs twice in two completely independent channels. On the other hand, it is doubtful that the great majority of voters will accept this cumbersome voting procedure.

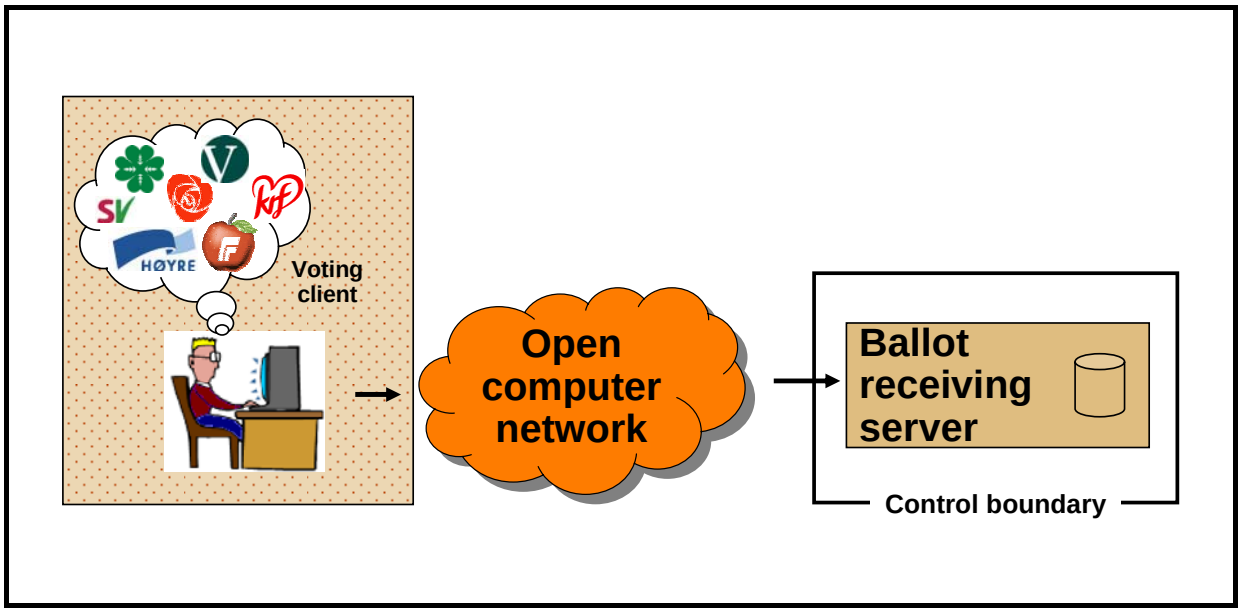


Figure 8.3: Voting in uncontrolled environments

A personal computer with access to the Internet
By "current technology" we basically mean a personal computer with access to the Internet. The weakest link in this chain is the voter's personal computer. It is way too easy to infect these machines with viruses, worms or root-kits, even without the voters' knowledge. Unfortunately, no anti-virus program can guarantee complete removal of any fraudulent software.

The fact that the ballot receiving server is connected to an open network also makes the electronic system vulnerable to various types of hacker attacks. Monitoring the traffic into the server may counter such attacks. However, one type of attack is not so easily countered: the "denial-of-service-attack" is a type of attack by which the server or the network is overloaded by irrelevant traffic, causing the receiving server to be unavailable. An obvious initiative to counter such attacks is to make several ballot receiving servers available: it is harder to knock out all the servers than to knock out one. Another way is to invite the voters to cast their votes

well in advance, in order to give them a second chance in case they do not get in touch with the ballot storage server in the first round. Should every attempt fail, they still have the opportunity to vote by traditional means on Election Day.

Duplicating the systems and the data transmission channels may guarantee a high security level (Selker & Goler 2004). However, a certain part of the system is less amenable to this type of security measure: Data produced on the keyboard are processed before their images appear on the screen. An illegal program may catch messages from the keyboard and modify them before they are sent off, although they appear on the screen as the voter typed them. Such software may be used to connect the computer to a fake ballot-receiving server.

Different types of threat in an Internet-based voting system are analyzed in more detail in Appendix B. There are also innumerable publications illuminating the weaknesses related to the security of current Internet architecture.

The operating systems, drivers and other software in personal computers today are really too complex and too general for simple, security sensitive transactions such as signing a document or casting a vote in an election. We do not preclude the possibility that alternative electronic equipment for security sensitive operations will be developed in the future. Such equipment may well be operated independently of, or as an accessory to, a personal computer. The working committee will not recommend solutions that are used solely for voting purposes. What need to be developed are general, widespread solutions which are also used for other security sensitive applications.

Personal computers with special operating systems
An intermediate solution is to equip an ordinary personal computer with a separate security certified operating system with restricted functionality. The operating system may be available on a voting CD-ROM. This solution has the advantage that the programming code on the CD is verifiable, and that the operating system normally used on the computer is not involved in the voting task. When the computer system is started with a verified and approved operating system rather than from the hard disk, there is no way that potential spy programs or similar threats in the client machine may interfere. This type of remote e-voting will be as secure as voting in controlled environments.

In order for the user not to have to configure the system, the computer should be linked to the Internet by a network card with dynamic IP address assignment. This will typically be the case for clients equipped with an ADSL router. Technically it is also possible to make the voting system recognize a modem /ISDN card in the computer and use this to connect the client to a pre-programmed phone number, giving Internet access only to the relevant ballot receiving server.

The disadvantages of this setup are first and foremost the technical complexity of the system. The operating system must be able to recognize a wide variety of configurations, not least the type of network/modem/ISDN communication card used by the client. Machines from different manufacturers require different drivers to communicate with the voting system. To enhance security, the voting system may provide a secure transmission channel from the client to the ballot receiving server through an at the outset insecure network such as the Internet (a “Virtual Private Network” connection or a VPN tunnel).

This system is well suited in controlled environments, but there is reason to doubt its suitability in uncontrolled environments on a large scale, since it requires that the user is confident with booting his machine with a different operating system. Furthermore, the operating system specially designed for the voting task requires different drivers for the relevant types of network connections. Another consideration is the amount of support needed when the home voters encounter a problem of some sort.

Digital /satellite TV
Different types of digital TVs may be used to submit ballots in uncontrolled environments. One condition is that communication is bi-directional, i.e. one direction from the "set-top" unit connected to the TV set back to the ballot receiving server, through the same network (cable TV) or through a telephone connection (satellite TV). Ballots may then be submitted providing an expansion of the menu system of the set-top unit. This system is characterized by many of the features also characterizing the voting machine solutions described above.

Software developed for the sole purpose of voting must be provided in the "set-top" unit. The units run their own operating system, which means that the voting application must be specially designed for these units. Recent set-top units have access to the Internet as well as separate browsers, and if the browser is used to log on to the Internet-based voting system, there is in principle no difference between voting on a digital TV and voting over an ordinary personal computer.

The most serious point of criticism that may be levelled against this technology is the fact that the equipment so far is not widespread (compared with the mobile phone and personal computers). Neither is a standardized PKI-solution available on this platform, and since a digital tuner is not really a "personal" unit, the voter is not identifiable through his or her TV subscription. Furthermore, voting over a 32 inch TV screen from the family living room does not invite a particularly "secret" submission of a voter's ballot.

The mobile phone
Voting over a personal cell phone is in many respects a very interesting alternative. Generally a mobile phone and its data transmission channel are more secure than a personal computer with Internet access, not least because the mobile phone networks are closed in a way that differs considerably from that of the Internet. Although it is not inconceivable that intruders may be hacking their way into the network, the chances of success are a lot lower than their chances of successful Internet attacks.

The mobile phone has the disadvantage that the screen is very small. This makes it difficult to set up a user interface which is well designed for correcting mistakes, making personal changes on the order of candidates on the lists, and transferring danglers. The voter will have to accept that this voting channel gives fewer options than the traditional system.

It is also important to consider the possibilities for concealing the content of the ballot, either by encryption in the cell phone system or in the ballot receiving server, or by "zero trust" solutions. These are discussed in the next section.

On the basis of the considerations above, the mobile phone solution should only be a supplement to other electronic channels offering a richer user interface. It is conceivable though, that the mobile phone technology develops to provide the very type of equipment for security sensitive applications we have paged here.

8.3.3 ”Zero trust”

The ”zero trust” solution is a relevant alternative when the voting client and the transmission network are not to be trusted. In this type of system the voter and the central, secure system for electronic voting share a secret which is unknown to the insecure components. For example, the voter does not spell out the name of the party, but submits it through a code, which may be a number. The coding must be different for each voter.

In this system the voting data may be transmitted openly, since no one but the voter and the central system know what they mean. It also implies that the voter can get a receipt from the central system, stating the coded information received. If the code received is the same as the code submitted, the probability is very high that the ballot has been registered and logged correctly by the central system.

The only challenge we are faced with in this solution is that of distributing the secret codes from the central system to the voter (or the other way round). In cases where this type of solution has been put into practice the codes have been sent by post to the voters before the election. In the future the codes may be sent to the voters by other channels (if the ballot is submitted over the Internet, the voter may receive the codes over the mobile phone network), or by some means which guarantee that the codes cannot be decoded by the channel. For example, the codes may have the form of pictures, which are easily interpreted by humans but non-interpretable by a text recognition system.

Figure 8.4: Voting by individual codes

To count the votes, the system must be able to connect the voter and the codes made available to him or her. A way to do that is to assign – in separate processes - a pseudo identity to the vote and to the set of codes. The pseudo identity may be derived from but not be traceable to the identity of the voter. A disadvantage is that this rather intricate decoding process must take place in a time critical period after the polling station has been closed for e-voters who change their minds and opt to exercise their right to vote by traditional means.

Another important question is whether the voters will be able to handle this rather complicated and not very user friendly voting procedure, particularly in view of the possibilities for making changes on the candidate lists. A future solution may be to produce the codes by means of a small computer with a screen on which the voter may make his changes on the actual list. This solution, however, looks a lot like the secure user unit discussed in section 8.3.2.

In sum, the working committee considers the practical disadvantages of the “zero trust” system too serious to recommend it

8.4 One voter, one vote

8.4.1 Voting permission

In order to cast a vote, a voter must be given permission to do so. In a traditional, paper based election on Election Day the voting permission is implicitly given as the voter, after identifying himself or herself, is crossed off in the voters' register and passes on to the ballot box, cf. figure 8-5. The same principle may be used for all voting in controlled environments. However, in the case of e-voting in controlled environments the election official must see to it that the voter does not cast a vote in the name of somebody else. The voter may be given voting permission by receiving a computer readable card with the voter's identity which he or she may insert in the system.

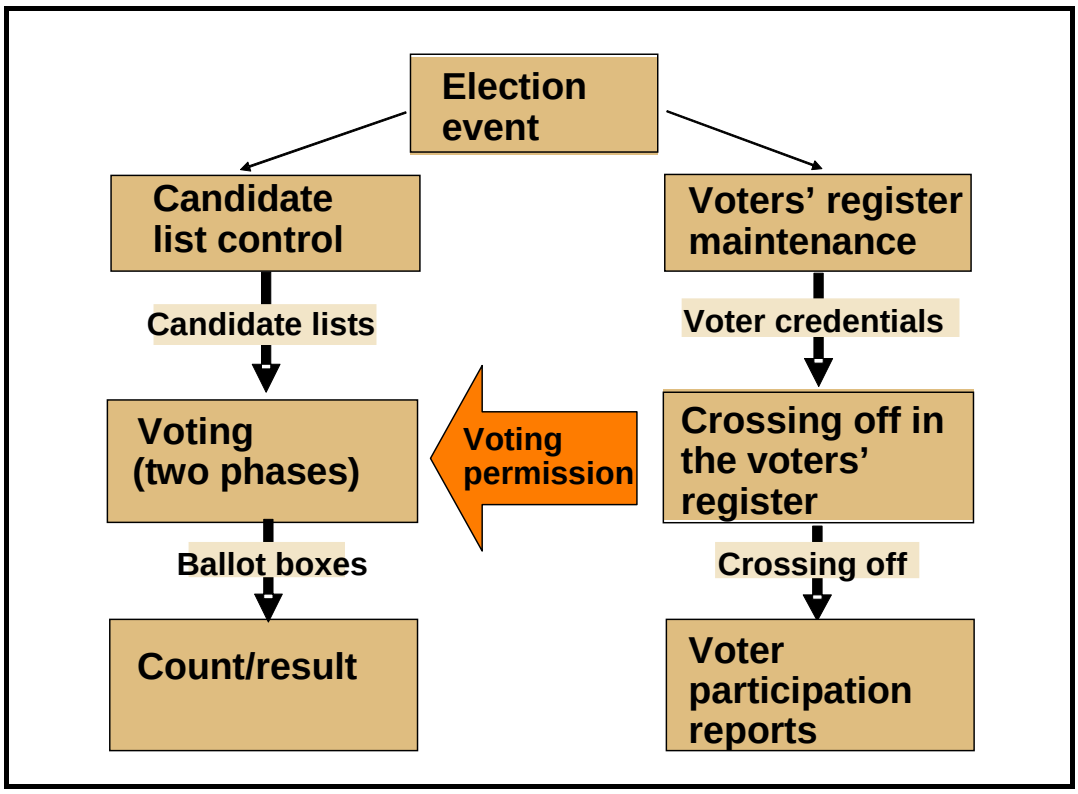


Figure 8.5: The Voting Process

8.4.2 Electronic voting requires a voter credential

E-voting in uncontrolled environments requires very different procedures. The voter must have a voter credential to be given permission to vote. The credential is also meant to prevent any voter from submitting more than one counting vote cf. the EC Recommendation on e-voting, Standards no 5, 6 and 94.

The voter credential may be anything from a voting card containing a secret code to an advanced smart card solution. One possibility may be that the voter makes use of an ID card which may also be used for general purposes, and which may be controlled against the voters' register before the voter is permitted to submit his or her ballot.

A voter may only insert one counting vote in the ballot box. This can be ensured either by making the voting credential unusable for voting once the ballot has been inserted, or by giving the voting credential a unique ID number which is recognisable by the voting system.

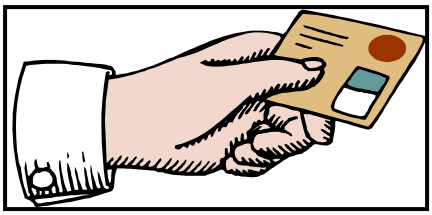


Figure 8.6: Electronic voting requires a voting credential

The first solution requires that in one way or another, the system can write into or modify the voter credential. Precautions should be taken for possible system break downs during the voting process, which means that the voting credential should be changed only after the submitted ballot has been registered. This again does not prevent voting fraud, as the voter may cut off the power supply just at the critical moment. In the second solution, the system has an overview of the credentials used. If a second attempt is made to use a credential, the system may either refuse the attempt, or accept a second ballot and annul the first one. The working committee recommends the second solution since it alleviates many of the problems related to undue influence and the buying and selling of votes and at the same time does not require considerable extra expenditures. Hence, an electronic ballot is not accepted as a valid e-vote and the voter not crossed off in the voters' register until the e-voting period is ended.

It is interesting to consider how, or to what extent, the ID number of the credential should be linked to the voter's identity, (i.e. the voter's birth certificate number). In order to enable the voter to re-cast an e-vote and also cancel it on Election Day, the connection between the voter and the vote must be directly or indirectly available until the polling stations are closed on Election Day. It is an absolute requirement, it should be remembered, that the voter be able to annul an e-vote submitted by submitting a new ballot by traditional means on Election Day.

Let us take a look at the alternatives.

Voting permission by an anonymous credential
One thinkable way is to make the voter completely anonymous before the ballot is cast by sending him or her a random voter credential for use in the casting of his or her ballot. The voter may receive or pick up a credential from a trusted system, or pull a credential from a box of some sort, in which case there will be no link between the voter's identity and his or her ballot.

The solution suggested here takes care of the voter's anonymity. However, it also has considerable disadvantages. The voters' register must be informed that the voter has received a voting credential. A new credential should not be issued if, for example, the voter claims to have lost his or her credential, because such an arrangement would at the same time permit the same voter to cast more votes by different credentials. If the voter decides to vote on Election Day, and there is a note in the voters' register that the voter has received a credential, the credential must be presented by the voter in order that the electronic advance vote is annulled. An anonymous voting credential is also not to be recommended since it allows the buying and selling of voting rights, and the credential may be considered a negotiable good

Even though this method guarantees absolute anonymity, for security reasons or for practical purposes it is not a viable solution.

Deriving the identification of the credential from the voter's ID.
To restrict the number of modules that can recognize the voter's real identity a system may be used which derives the voting credential from the voter's ID. A separate module of the e-voting system, or a trusted third party is used to generate an ID credential (pseudo identity) based on the voter's birth certificate number. If the same birth certificate number is submitted, the same pseudo identity is received but any attempt at reversing the operation will fail, i.e. it will not be possible to receive a birth certificate number by submitting a pseudo identity number.[57]

The use of a pseudo identity supports repeated voting since the same identity is used each time. If a voter's credential attached to the pseudo identity is lost, a new credential may be generated on the basis of the voter's true identity (since the same pseudo identity may be generated again).

If the voter wants to vote in the polling station on Election Day, and it has been checked off in the voters' register that the voter has received a voter credential, there are two options. One is to have the voter present the credential in order that the pseudo identity may be used immediately to annul any electronic votes submitted by that voter. If the voter cannot present the credential, the second option is to register the voter's birth certificate number and have a "trusted" system compute the pseudo identity again.

The credential has the voter's identity
In this solution the voting system knows the identity of the voter, but he system must be designed in a way which guarantees that no connection can be traced between the content of the vote and the voter. One way to do it is by means of "sealed electronic envelopes" – see 8.4.3 below for a detailed description. If the voter decides to cast an advance vote electronically, it must be crossed off in the voters' register. The voter may also cast his or her vote on Election Day, either by presenting his or her voter credential or by giving his or her true identity.

From a technical point of view the simplest solution is to have the voter use his or her real identity (birth certificate number) when casting his or her vote. Even if these solutions require that special attention is paid to designing the central systems in such a way that it is impossible to connect the content of the ballot to the voter, this disadvantage is balanced off with the advantages of this system. One very important advantage is that the voter credential is not required for a re-casting in the polling station on Election Day, which makes the voter credential a non-asset for potential buyers.

The working committee recommends the latter solution. In the following we therefore assume that the voter communicates with the voting system using his or her real identity. The question then is how the voting system can identify and authenticate the voter

In principle identification and authentication is based on:

- Something possessed by the voter (a passport, ID, smart card, eID or something similar).

[57] The national prescription register at the Norwegian Institute of Public Health has adopted this solution, Statistics Norway is the trusted third party providing a pseudo identity before a prescription is registered. A person's total prescriptions over time are thus collected, yet the person's real identity may not be traced.

- Something known by the voter (password or PIN code).
- Something biometrically identifying the voter (facial features, finger print, retina pattern).

At present biometric methods are too complicated and too expensive to apply extensively, particularly for application in home computers. However, this may change over time with the technological development. The solution, therefore, should be based on a combination of what the voter possesses (e.g. a smart card) and what the voter knows (e.g. a PIN code). The working committee will advise against the introduction of separate ID mechanisms for e-voting, as such systems will be expensive and cards and their PIN-codes may be used for trading.

The working committee would rather suggest using publicly accepted PKI solutions[58] like the ones being introduced in Norway at the moment. It reduces cost, the voter has to keep fewer cards and PIN codes and a potential buying and selling of voter credentials are kept to a minimum. A voter would hardly want to lend a PKI card and its PIN codes to somebody else when the borrower may use the card for a number of other purposes than casting a vote.

A PKI solution employs the technology of asymmetric encryption. The technology is based on an electronic pair of keys, i.e. two bit patterns created by help of a special algorithm. One key is used to encrypt an electronic message to make it illegible. The only way to decode the original, legible message is to decrypt the message by means of the other key of the pair. The key pair is used by making one key publicly known ("the public key") while keeping the other key strictly secret ("the private key"). If A sends a message to B and this message is to be legible to B only, A may encrypt the message with B's public key. If on the other hand B wants to make sure that the message actually comes from A, A may encrypt the message (or a number computed on the basis of it) with his own private key. This is a *digital signature*. If the message is decrypted by means of A's public key, it must come from A personally, and not from anyone pretending to be A.

To confirm that a public key actually belongs to a particular person or institution, a *digital certificate* may be used. Such certificates are often issued by a trusted third party. For example, the voting system may ensure that user A is in fact user A (or at least ensure that the user has access to the electronic ID of user A) through the PKI accessible BBS security gate[59]. A detailed description of the system is found in chapter 3 of NOU 2001:10 "Uten penn og blekk" ("No more pencil and ink")

In Norway it has been suggested that PKI identities are issued, validated and maintained by private agents (as opposed to Estonia, for example, in which ID cards with PKI identities are issued by public officials.) The Norwegian Post and Telecommunication Authority is the Supervisory Authority responsible for controlling qualified-certificate-providers, and all such providers have to register with the Post and Telecommunication Authority[60]. Services like

[58] http://odin.dep.no/filarkiv/234033/Kravspek_PKI_v102.pdf is a requirement specification for the public sector.
[59] http://www.brreg.no/sikkerhetsportal/ - The purpose of the Security gate is to make it simple for the civil service or the local government administration to offer electronic services to users which require e-identification or e-signatures. The security gate is designed to integrate PKI solutions from different system suppliers and is meant to offer Single Sign-On options in several services, whether they are accessible through the Security gate or directly from the municipal and civil service web pages.
[60] See http://www.npt.no/pt_internet/sikkerhet_teleberedskap/digital_sign/tilbydere.html

"MinSide" ("MyPage"), to be launched in the first quarter of 2006, may contribute to help people see the value of acquiring a PKI identity.

Two levels have been defined for personal certificates in the requirement specification for PKIs in the public sector: "Person-Standard" and "Person-High". Person-High means that the certificate has been stored in a smart card and it is necessary to appear in person to get it. Person-Standard means that the certificate may be downloaded to a file in a personal computer. The Working Committee recommends that the level "Person-High" is set as the standard requirement for electronic voting.

Alternatively, for computer-based e-voting the mobile phone may serve as a "trusted device". Today a great number of people own a mobile phone whose SIM card may have PKI functionality.[61] When a person logs on to cast a ballot over the Internet, a verification message may be sent to this person's cell phone. The message is signed by the private PKI key in the SIM card (the password is entered on the cell phone) and the voter is thereby identified. The problem with this is the possibility of buying and selling votes: the buyer may agree with the seller to approve such a transaction, and the person inserting the ballot (the buyer) and the voter registered (the seller) do not even have to be in the same place. If a one-time password is sent to the voter's cell phone and this password has to be entered into the voting client, the voter's identity is secured, at least to some extent. It is also possible to ask the voter for advance registration of the mobile phone number to be used for submitting a ballot.

8.4.3 How to avoid any link between the content of the vote and the voter

It is the working committee's intention that a ballot cast in uncontrolled environments may be withdrawn, either as a new electronic ballot is cast by the same voter or as the voter submits a new ballot in the polling station on Election Day. To achieve this, each electronic ballot cast must be linked to the voter as long as a new ballot may be submitted, but during this period the ballot must be sealed. Standard no 35 of the EC Recommendation states that "votes and voter information shall remain sealed as long as the data is held in a manner where they can be associated".

The general solution to this problem is the double envelope system as we know it from paper based advance voting and voting outside the voter's assigned district on Election Day. The ballot is inserted in an anonymous envelope which is then inserted in a cover envelope having the voter's identity written on it. During counting, the voting card and the ballot paper envelope are separated and the ballot paper envelope is inserted in the ballot box along with the other ballot paper envelopes.

An electronic voting system is constructed with a double envelope system by means of asymmetric encryption (see section 8.4.2) and at least two key pairs – one to protect the ballot (the inner, ballot envelope) and one to verify that the ballot has been cast by the given voter (the outer, cover envelope). When the voter has made his or her choice, the chosen electronic ballot is immediately encrypted by the public key of the election. This encryption seals the ballot envelope. The content of the ballot is only readable after it has been decrypted by means of the voter's private key, seen as the opening of the ballot envelope. A security module generates the key pair at the start of the election event. The public key of the election is distributed to the voters through the software used for the casting of the ballot. The

[61] All the SIM-cards fromTelenor Mobil have PKI-functionality as of 1May 2002

accompanying private key is kept in the security module and is only made accessible by a procedure in which a given number of people from the electoral authorities have to "unlock" the security module by means of a set of keys (physical and/or digital keys)[62].

The messages to be encrypted in an election are to a large extent standardized messages, i.e. unmodified ballots. For this reason the unmodified ballots may not be asymmetrically encrypted in a direct way – otherwise an attacker could easily get hold of the content of the ballot. Some random data must be attached to the ballot. One obvious solution is to use hybrid encryption by means of a randomly chosen session key.[63]

Before the encrypted ballot is sent from the voting client, it must be inserted in a sealed electronic cover envelope. The cover envelope is given the voter credential's identity and is encrypted by the voter's private key, which means that the ballot is given a digital signature. The cover envelope is opened, i.e. decrypted by means of the voter's public key which may be obtained by the voting system from an electronic voters' register or from a national PKI system, depending on the solution chosen. This way it may be verified that the ballot is received from the given/stated voter. Figure 8.7 below illustrates the principles for securing the secrecy of e-votes as just discussed.

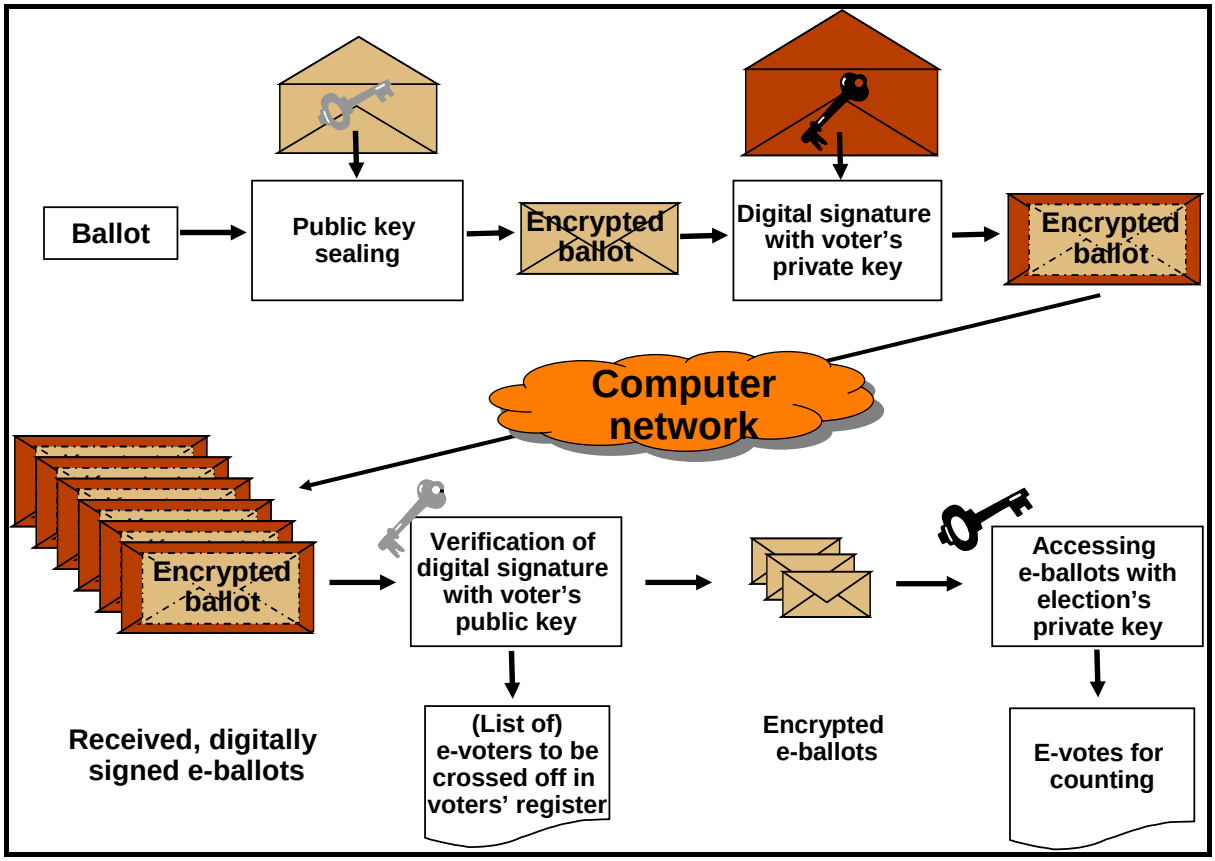


Figure 8.7: Principles for securing e-ballots

[62] This solution is identical with the solution used for e-voting in Estonia,see The National Election Committee: E-Voting System – Overview at http://www.vvk.ee/elektr/docs/Yldkirjeldus-eng.pdf

[63] In hybrid encryption symmetric encryption is used for the real message, i.e. it is encrypted and decrypted by the same key. However, this key is a randomly used session key which is transferred from sender to receiver by means of asymmetric encryption. Since asymmetric encryption requires more computer power than symmetric encryption, and considerably less work is required to encrypt a session key than a whole message, hybrid encryption may be a very efficient solution. Furthermore a wanted element of randomness is introduced.

In order for this solution to ensure that the content of the ballot cannot be associated with the identity of the voter, it is an absolute requirement that nobody involved in the voting process has access to the digitally signed e-votes and the private key of the election *simultaneously*.

8.5 The functionality of the voting system

From the previous chapters we have seen that the working committee recommends that paper based and possible electronic voting solutions should co-exist on a long term basis. It is therefore required that we come up with some good solutions on how to integrate the two means of casting a vote. In the present section we sketch a system for routines to be followed in elections with traditional paper ballots as well as electronic ballots. The routines are described by means of Use Cases in accordance with the UML standard (Rumbaugh, Jacobson & Booch 2004)[64].

Use Cases are mostly self explanatory, yet a definition of certain terms may be useful:

- *Agent*: A special type of user – humans or other systems playing a role in the system and having a goal which is reached by following the Use Case.
- *Pre-condition*: A condition that must be satisfied in order for the Use Case to be performed**.**
- *Post-condition*: The state of the system and the agent after the Use Case has been performed**.**
- *Basic course of events*: The sequence of events achieveing the agent's goal without any hindrances or exceptional situations
- *Variants*: Deviations from the basic course of events.

[64] See http://www.uml.org

8.5.1 The electronic voting procedure

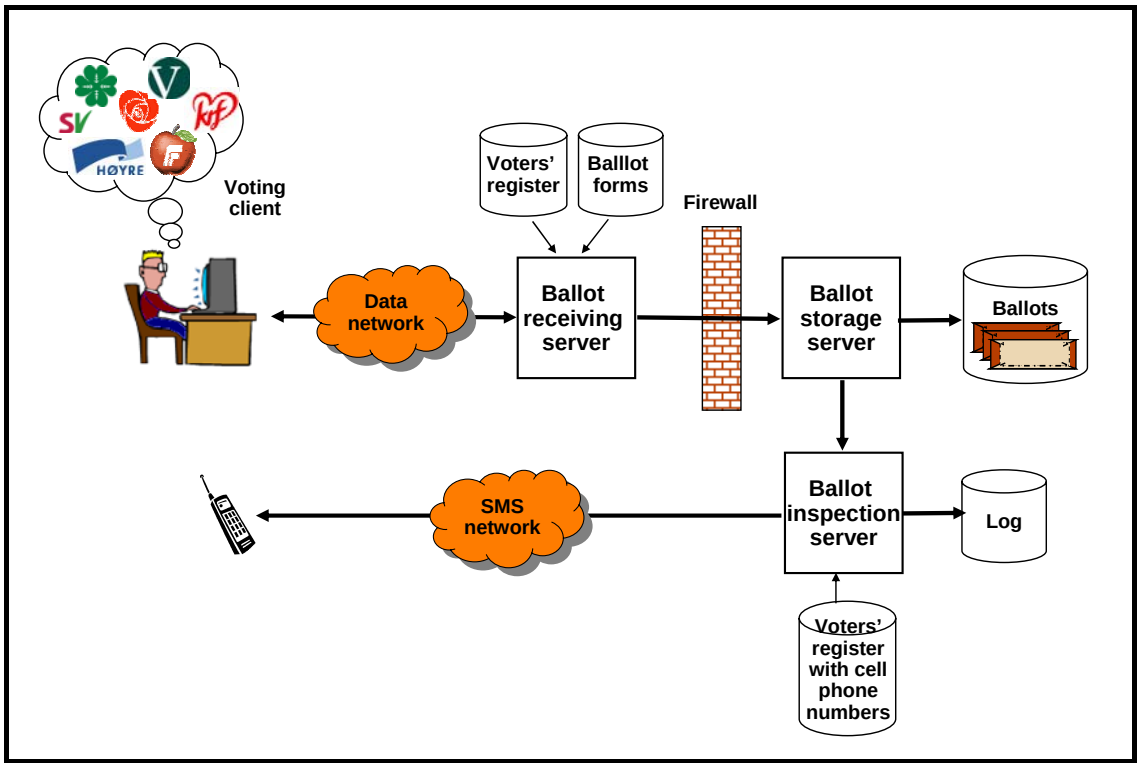


Figure 8.8: Architecture of the voting system

The central functionality of any e-voting system is the very submission of the ballots. The functionality described in the present section is based on the architecture illustrated in figure 8.8. The ballot receiving server must have *reading access* to the voters' register as well as the ballot forms, not only to verify that the voter has the right to vote but also to send the voting client the correct ballot forms. The ballot receiving server passes the cast ballots on to the ballot storage server through a firewall. The ballot storage server writes the received ballot onto a "write-once"-medium, and then passes it on to the inspection server.

For security reasons, the software receiving the finally modified ballot from the client and passing it on to the ballot receiving server and the ballot storage server must be as simple as possible. This part of the software must be kept separate from the software that downloads and presents the ballot forms and allows the voter to modify them, since the security requirements differ, and since the programs easily end up being too large and too complicated.

Use Case Description
Agent: The Voter
Pre-condition: Voter client with a browser is ready for use
Post-condition: The voter's ballot has been registered in the ballot data base.

Basic course of events:

1. The voter accesses the voting system and identifies himself/herself to the system.

2. The system verifies that the voter is registered in the voters' register and grants the voter permission to cast his/her ballot (voting permission granted). The right ballot forms are presented to the voter, i.e. in accordance with the voting district of the voter.
3. The voter decides on the ballot of his or her choice, modifies it in accordance with his or her preferences and submits it to the system. In a zero trust system the cast ballot may be given a pseudo identity at this stage.
4. The system receives the ballot and stores it in a safe place for the counting stage.
5. The voter receives confirmation from the system that the ballot has been received. Confirmation is preferably sent over a different channel (SMS, for example).
6. The voter checks the receipt/confirmation and exits the system.

Variants:

2a.

1. The system finds that the voter is not registered in the voters' register. The system returns the message that the voter is not registered and terminates the Use Case.

4a.

2. The system finds that an error has been made in the modification of the ballot. The system returns the message that an error has been detected and goes back to 3.

The functionality must be based on a client/server architecture by which the voter operates the voting client and the ballot receiving server receives and transfers the ballot to other parts of the overall voting system. Each step in the Use Case is described in detail in the following paragraphs.

The voter contacts the voting system and is given access by means of the voter credential
The user interface should be designed as a web application or web page to make as many client platforms and operating systems as possible available for voting. An alternative is to have "voting programs" that may be downloaded in different formats for a PC, Mac, Linux etc. This alternative is less independent of a particular platform, and is more cost-sensitive. A client machine should not be required to have more than a standard browser (and selected security solution support) to be used for voting.

The voter follows the first step in the Use Case specifications by starting a browser and filling in the web address (the URL) given by the electoral authorities. The component governing the rest of the dialogue with the voter is then downloaded. This requires that the browser is configured to run such modules.

The voter is then given access to the e-voting system by means of the voter credential, see section 8.4.2. The credential automatically identifies and authenticates the voter to the system.

The system verifies that the voter is registered in the voters' register, fetches the ballot forms based on the voters' voting district and grants the voter permission to cast the ballot of his or her choice
Voter identity is sent to the ballot receiving server. The server reads the voters' register and checks that the voter has the right to vote. If the voter is not found eligible in the register, a message about this will be returned to the voter.

The server then finds the voting district of the voter and returns the ballot forms (candidate lists) available to the voter. In other words, the server machine must have *reading access* to an electronic voters' register and a data base containing the ballot forms. The system may be split into several servers, each of which having access only to certain parts of the voters' register and candidate lists/ballot forms.

The voter picks the ballot form of his or her choice, modifies it according to his or her preferences and submits it to the system
The voter is now ready to pick the ballot form of his or her choice. In this connection it is important that the user interface is not designed in such a way that it favours any of the ballot forms to the disadvantage of any other forms.

The voter may now modify the ballot form according to the rules for modifications by using the available input units (pointing screens or keyboard/mouse). Candidates may be given a personal vote or eliminated from the form, and danglers may be added from other parties' candidate lists which may be displayed on pull-down-lists, by using search functions, or by similar methods.

The system should continuously validate the modifications made by the voter and alarm the voter of invalid or erroneous modifications by returning informative error messages. It should not be possible to cast ballots that will not be approved.

The voter submits the finished ballot by pressing a button which starts the transmission of the ballot to the ballot receiving server.

The system receives the ballot and stores in a secure place for counting
Before the ballot is transmitted, it is inserted in a sealed "electronic envelope" in the sense that the content of the ballot[65] is encrypted by the system's public key. This ensures that the content of the ballot submitted is readable only to the person or system knowing the system's private key. The ballot envelope is inserted in a cover envelope through an electronic signature inscribed by means of the voter's private key to make sure that the ballot has been submitted by the person he or she presents himself or herself to be, and to ensure that the ballot submitted may be withdrawn if the voter opts to vote by traditional means on Election Day. This double encryption procedure is described in greater detail in section 8.4.

The Recommendation from the European Council states that the EML format shall be used for the transmission of data as far as it is advisable. The working committee considers any communication between the voting client and the ballot receiving server to be "internal" communication between two logically interdependent systems which in all probability will be provided by the same system supplier. This implies that a considerably simpler raw data format may be put to use, not only to reduce the amount of the data transmitted, but, for security reasons, to make the programs in the two machines as simple as possible. However, the ballot receiving server should base any further communication with the core system on the EML format.

[65] The ballot may be transmitted as a whole (all the names on the list), including the voter's modification, or it may be transmitted in the form of a ballot paper indicator ("MyParty") followed by the voter's modifications. The latter principle will probably reduce the size of data transmitted, on the assumption that the voters do not make too many modifications.

The ballot receiving server passes the double envelope on to the ballot storage server as soon as the data are received. The ballot storage server enters the double envelope into a fire-wall protected write-once storage medium containing the cast ballots. This means that the only systems linked to the Internet are the voting client and the ballot receiving server.

The electronically cast ballots are stored in the ballot storage server until the counting phase starts.

The system confirms that the ballot has been received
The ballot receiving server sends a message to a log server, which is also a system for returning confirmation to the voter that the ballot has been received. The server logs onto a write-once medium that a ballot has been received from a voter with a given identity (but does not enter the *content* of the ballot in the log). When the ballot has been logged, the server must return a message to the voter confirming the reception and registration of the ballot, cf. Standard no 14 of the EC Recommendation. To enhance security, the confirming message may be sent over a different channel as well as over the channel used to submit the ballot, for example as a SMS over the cell phone network. This solution requires that the voter is registered with a cell phone number in the voters' register, or that the voter has given his or her number to the system before casting his or her ballot.

A confirming receipt may also prevent intruders from re-casting a vote in the name of the voter without the voter's knowledge, as the given cell phone number is automatically used to confirm the reception of a new vote (the phone number may only be entered once and may not be changed).

One central question is how the voter will know with at least some certainty that the registered ballot has not been changed or faked on its way in the system. One solution is that the client computes a "digital hash" (a number code) of the encrypted ballot and makes it visible on the screen before the voter sends it off. The ballot storage server computes the same "digital hash" and returns this to the voter along with the confirming receipt. The voter may then check that the two numbers are identical, i.e. they have been computed on the basis of the same ballot.

Another solution is to return the encrypted ballot in the confirming receipt. If hybrid encryption has been used (cf. section 8.4.3) and the client has saved or got access to the randomly chosen session key, the client may decrypt the ballot and spell it out[66].

The voter checks the confirming message before terminating.
The voting procedure has now been completed. At this point no residual data referring to the voting procedure or the voter's ballot must be left on the client machine, cf. Standard no 93 of the Recommendation.

Voting via SMS?
Voting via SMS should also be considered an alternative. The voter must register in advance with the mobile phone number that will be used in the casting of the ballot, and is then given a

[66] Given that the client machine keeps the session key, a function may be worked out, enabling the voter to inspect his/her ballot as registered on the ballot storage server. It is no obvious that this function is wanted: The voter's confidence that his/her ballot has been registered correctly is enhanced, but so is the unwanted possibility of undue influence and the buying and selling of votes. It may also be questioned whether this solution is in accordance with Standard 51 of the Recommendation.

personal code to be used for voting. The voter may then send "< name of party list chosen> <personal code>" to a given phone number. In receiving the SMS the ballot receiving server certifies that the given number code and the mobile phone number used for the casting of the ballot correspond. The ballot is then registered and an SMS is returned to the voter confirming that the ballot has been received and registered. The solution presented here does not allow ballot form modifications.

SMS voting may be extended to a multi-step procedure by which the first message: "VOTE <person ID>" is sent to a given phone number and a return message from the system must then be answered with a private key signature. The key is stored in the SIM card and protected by a separate PIN code. The ballot receiving server verifies the signature by means of the voter's public key and confirms that the ballot may be cast. The voter may then send the ballot of his choice and be asked to "sign" his ballot.

The security of the system is to a certain extent taken care of since the ballot is protected by a double authentication procedure: i.e. by something the voter possesses (a mobile phone with a SIM card with PKI functionality) and something the voter knows (a PIN code for the signature).

8.5.2 The ballot log

A central property of an election system is the verifiability of the results; cf. Standards no 107 and 108 of the EC Recommendation. Traditional elections with paper ballots are verifiable through the piles of ballots. If any doubt is raised as to the correctness of the counting results, the paper ballots may be re-counted.

It is hard to find a replacement for the paper ballots as a security measure once the ballot is cast electronically. It is a requirement that the voter be ascertained that the back-up ballot is a hundred per cent correct. American security experts have suggested voting machines which not only send the ballot off electronically, but produce a paper print version behind a glass screen for verification by the voter and for insertion in a ballot box untouched by the human hand (Mercuri's voting machine[67]). Another suggestion is to have the voting process divided in two steps, each on a separate machine (Bruck, Jeffeson & Rivest 2001). The voter at first submits his or her ballot on a machine which is not connected to a data network. This machine "burns" the ballot electronically on to an electronic chip called the "frog". The voter then walks over to the election official who registers the content of the chip in the voting system and inserts the chip in the ballot box. The pile of chips is now the back-up copy. More creative suggestions include creating a safety net by video recording the keyboard and the screen of the voting device in a way that does not recognize the voter.

Principles like the ones presented above are irrelevant for e-voting in uncontrolled environments since there is no safe way to handle the backup copies. Rather, a ballot log must be created on the central servers.

[67] See an account at http://www.notablesoftware.com/evote.html

8.5.3 Crossing e-voters off in the voters' register after phase 1

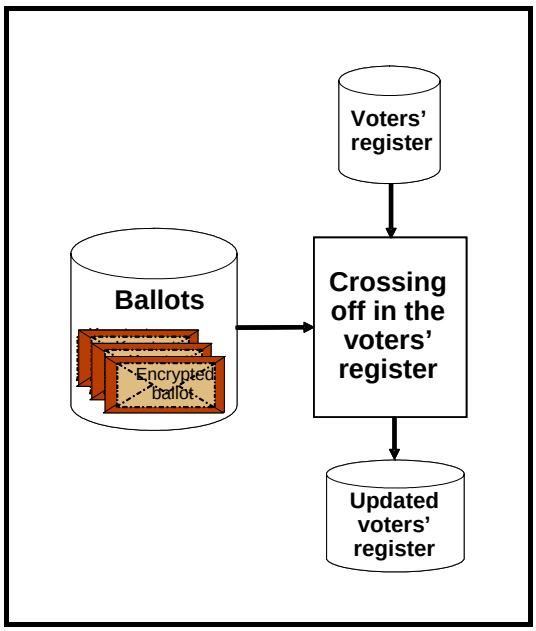


Figure 8.9: Crossing e-voters off in the voters' register after phase 1

For correct handling of voters who have submitted one or more electronic ballots in phase 1 but who opt to submit a ballot again in the polling station on Election Day, the election officials must have access to the voters' register for their districts. The voters' register does not have to be electronically available in the polling station, a paper version will do.The voters' register used in the polling station must have information about the voters' advance submissions. The updating with this information has to take place between phase 1 and Election Day. This requires that a trusted part of the system knows the connection between the identity of the voter credential and the identity of the voter in the voters' register.

Use Case for crossing e-voters off in the voters' register after phase 1
Agent: The electoral authorities

Pre-condition: e-voting in phase 1 is closed.
Post-condition: The voters who have submitted one or more electronic ballots have been crossed off in the voters' register.
Basic course of events:

1. The electoral authorities activate the crossing off system.
2. The crossing off system runs through all the e-votes in the ballot data base and crosses the e-voters off in the voters' register.
3. The crossing off system produces all necessary paper versions of the voters' register for use in the polling stations on Election Day.
4. The crossing off system creates all the necessary and/or interesting statistics.

8.5.4 Annulment of electronically submitted ballots on Election Day

If a voter who has already submitted a ballot electronically decides to vote again on Election Day, the election official has to inform the electronic system that all the ballots submitted electronically by this voter are annulled. If completely anonymous voter credentials are used, the voter has to present his or her voter credential to be granted permission to vote on Election Day. If the voter credential is derived from the voter's ID, this is unnecessary, since it may be

derived again. However, it is simpler to annul ballots if they are linked directly to the voter ID.

The routine requires online availability of the annulment system in the polling station – an expensive solution. An alternative is to have the election official communicate in one way or another to a central office that the electronic ballots from phase 1 are withdrawn. The very details of this procedure, as well as the question of whether the voter has to await confirmation of the annulment, have not been considered by the working committee. The annulment system must in any case be designed to prevent any outsider or unfaithful officer from being able to annul ballots without a warrant to do so.
When an electronic ballot is withdrawn, the annulment should be confirmed to the address first receiving confirmation that the ballot had been registered (see section 8.5.1)

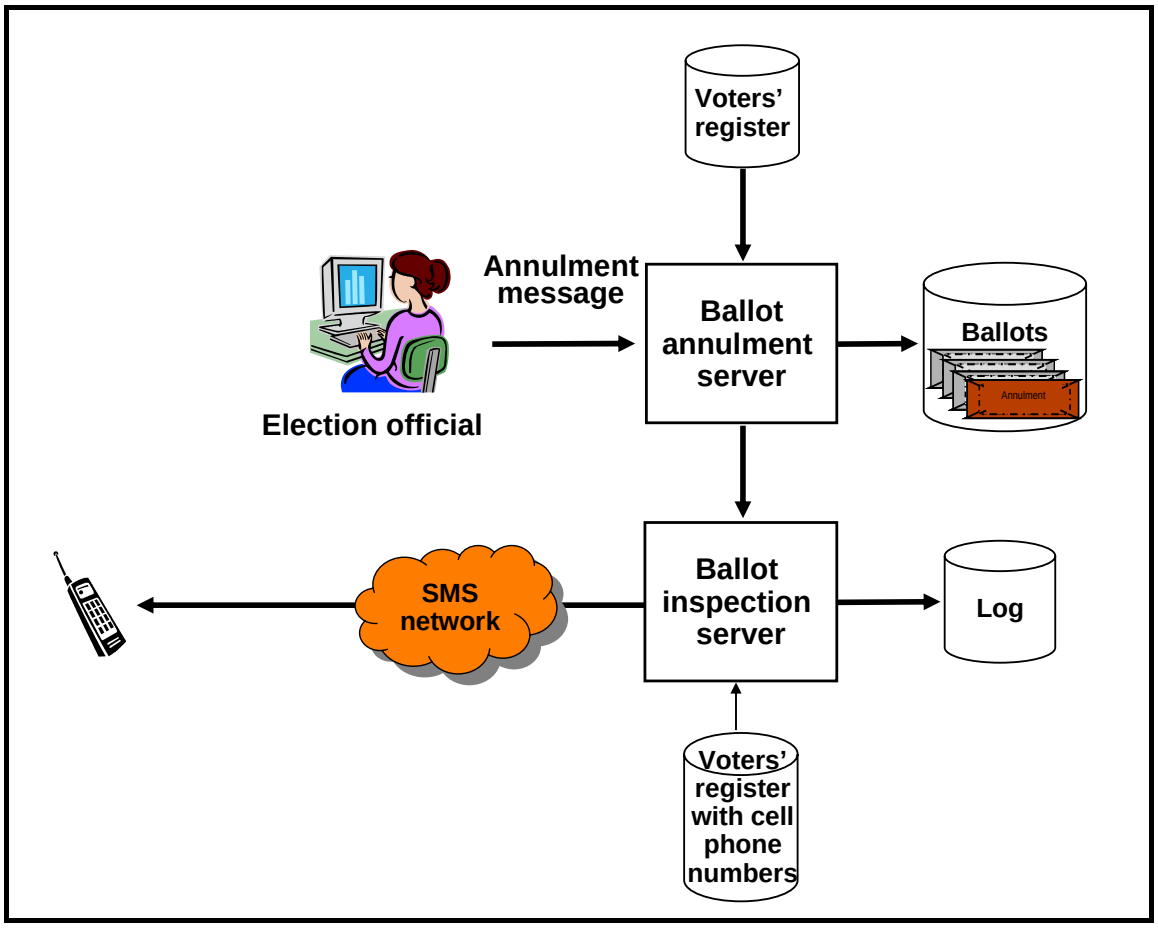


Figure 8.10: Ballot annulment

Use Case for annulment of electronically submitted ballots from phase 1 on Election Day
Agents: Election official, voter

Pre-condition: The election official has found the voter listed in the voters' register and noted that this voter has already submitted one or more electronic ballots.
Post-condition: The voter's electronic ballots have been annulled and the voter is granted permission to cast a paper ballot in the ordinary way.

Basic course of events:

1. The election official enters into the annulment system the identity of the voter credential presented by the voter (pseudo identity or birth certificate number, depending on the chosen solution, cf. section 8.4.2).
2. The annulment system annuls the ballots submitted in phase 1 by inserting an "annulment envelope" in the data base of the ballot storage server.[68]
3. The annulment system also registers the "annulment envelope" in the log.
4. The annulment system returns a confirmation message to the election official that all the electronic ballots attached to this identity have been annulled.
5. The annulment system also sends a message to the voter over the same channel that was used to confirm the reception of the electronically submitted ballot, to say that the advance votes have been annulled.

Variants:

1a. The voter does not have a voter credential but presents another ID with his or her birth certificate number. The election official registers the birth certificate number.

3a. For technical reasons the election official will not receive confirmation of annulment. In this case the election official must be confident that the annulment system has annulled or will annul the electronically submitted advance votes.

8.5.5 Counting the e-votes

This functionality consists of two Use Cases, one to extract the valid advance e-votes and the other to count them. The two processes should be kept apart to reduce the risk of connecting the content of the ballot to the voter's identity.

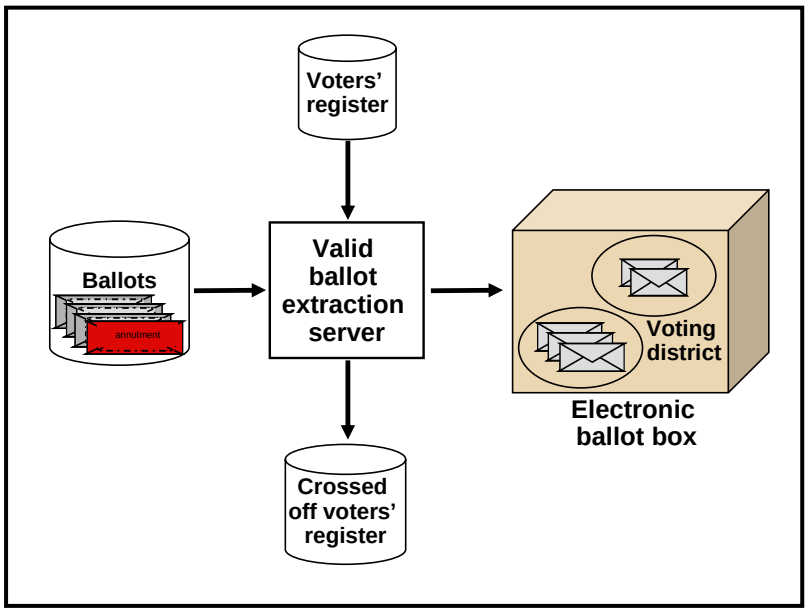


Figure 8.11: Extracting valid e-votes

Use Case for the extraction of valid e-votes
Agent: The Electoral Authorities

[68] This procedure is better than deleting the electronic advance votes or marking them off as invalid. In this way the vote storage in the ballot storage server may be designed as a "write-once"-medium. Which ballots count as valid ones, is determined during counting.

Pre-condition: The time period for cancelling electronically submitted ballots in the polling stations on Election Day is terminated.
Post-condition: E-votes in the electronic ”inner envelope” are ready for counting.

Basic course of events:

1. The Electoral Authorities start extracting valid ballots.
2. The extraction system sorts the ballots submitted (still in the electronic cover envelopes) on the basis of the voter credential identifier and on the basis of the registered submission time.
3. The extraction system extracts the last ballot submitted for each credential identifier. The last ballot submitted may be an “annulment envelope”.
4. The extraction system performs a last crossing off of e-votes in the voters’ register to take account of all the annulments made on Election Day, and then distributes the e-votes to the voting districts. (if a voting district has fewer than a given number of e-votes, the votes must be sent to a “aggregate voting district” to maintain the secrecy of the votes).
5. The extraction system then mixes the valid e-votes.
6. The extraction system opens the cover envelopes by means of the voters’ public keys, picked up from the voters’ register.
7. The extraction system enters the “inner envelopes” in a "write-once"-medium – which is the ”electronic ballot box”. In a ”zero-trust”-system the ballots must be assigned a pseudo-identity if they do not already have one.
8. The extraction system sends a report to say that the valid electronic votes are ready for counting.

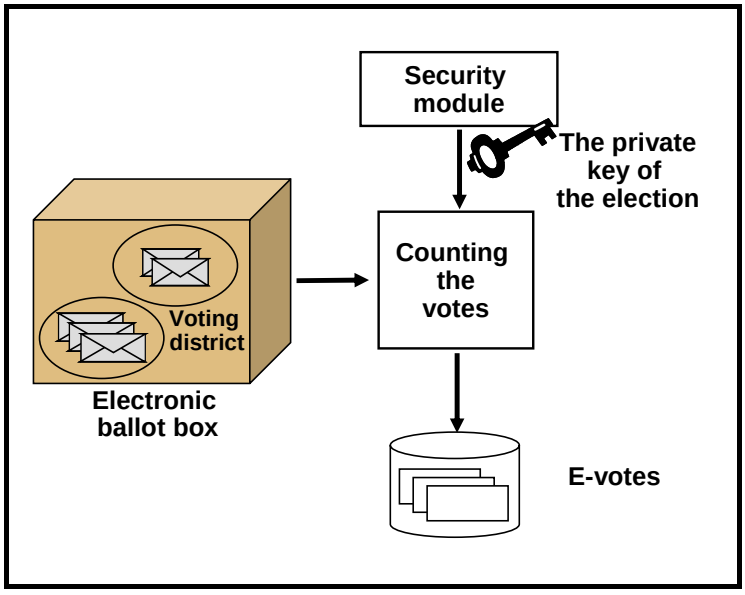


Figure 8.12: Counting valid e-votes

Use Case for counting valid e-votes
Agent: The Electoral Authorities

Pre-condition: Electronic votes in the electronic ”inner envelopes” are ready for counting.
Post-condition: Electronic votes have been counted and are ready to be merged with the paper ballots.

Basic course of events:

1. The Electoral Authorities open the security module holding the private key of the election.
2. The Electoral Authorities start counting the e-votes in the electronic ballot box.
3. The counting system reads the private key of the election and opens all the electronic inner envelopes. In a zero trust system the codes must be deciphered by means of a set of codes with the same pseudo identity.
4. The counting system lists the e-votes in a "write-once"-medium.
5. The counting system counts the e-votes and produces for each voting district a report which is well suited for integration with the results from the counting of the paper ballots.
6. The counting system sends a report when the counting is done.

It should be seriously considered what to do with the private key of the election when this Use Case is terminated. Security logs and copies of voter ballots in electronic double envelopes may exist in several places in the system, and given simultaneous access to the logs and the private key of the election it is possible to expose the content of the e-voters' ballots. If, on the other hand, the key is maculated, the voters' ballots will be illegible forever.[69]

8.5.6 Returning of Results

Paper based voting will probably make up the majority of the cast votes in many elections in the future. The electronic votes submitted should therefore be integrated into existing systems for counting in the counties. An "electronic ballot box" (printout) holding the electronic votes submitted, may be sent to each county on the Election Night (when it is clear who have opted to cast their ballots in the polling station and thus to annul their electronic ballots). These ballots may then be added to the counts of the ordinary ballots as a separate voting district or something of that sort.

8.6 The voters' register

From the preceding discussion it should have become clear how important the voters' register is in running an election. The voters' register is used in the following processes:

- The production of printouts of voters' registers for manual or electronic advance voting in controlled environments.
- The production of voter credentials.
- The presentation of district-based ballot papers on the voting client.
- The confirmation that an e-vote has been registered (to find the cell phone number or other suitable address).
- The checking off in the voters' register after e-voting in phase 1.
- The production of printouts of voters' registers for use in the polling stations.
- Annulment of electronic ballots from the polling stations on Election Day.
- Extraction of valid e-votes (for crossing off).
- Counting the e-votes (to find the voter's public key).

[69] In the electronic voting system in Estonia several pairs of keys are used in each election. The voters' ballots are duplicated and encrypted by means of the public keys from each pair, which is a security measure in case any private key is lost or does not function correctly. Unused private keys are protected in the security module.

Some of the functions listed are very time critical. It would be extremely unfortunate, for example, if the voters' register was not available during the counting of the electronic ballots. A good thing is that there is little need for updating in the processes listed above, which means that several identical electronic copies of the voters' register may be used (mirroring).

In addition to the information traditionally required in the voters' register, the question may be raised as to whether the voters' cell phone numbers (or other suitable address) and the voters' public keys should be included, since the register is needed to support e-voting of the sort described in this report. The working committee has not considered designing procedures for entering this information in the voters' register.

8.7 General requirements for the system architecture

This section discusses the working committee's suggestions for general, principal requirements for the system architecture of e-voting systems. The list of requirements should not be taken as a final list, as it may need elaboration and be made more specific to be used as a real requirement specification for an e-voting system.

8.7.1 The same technical solution in all environments

The working committee is of the opinion that technical solutions should be designed to accommodate voting in controlled as well as uncontrolled environments and through different channels. Control and certification procedures will then be simpler and technical barriers against changes are reduced in case of general technological and political change. Furthermore the voters will be able to bring their experience with voting in controlled environments to voting in uncontrolled environments. This means that the equipment in controlled environments should be of a kind that may be expected also to be in people's homes, or that it is reasonable to believe people will buy.

8.7.2 Solutions independent of platform

The software solutions should be designed to be as independent of particular platforms as possible, and be able to run on computers from different manufacturers and with different operating systems. This applies in particular to the voting clients. The number of servers will be very limited, which means that it is acceptable for a software provider to be bound to a particular platform.

8.7.3 A standard format for the exchange of data between components

A complete voting system consists of a number of relatively separate components, such as a voters' register system, a ballot receiving system, a ballot storage system and a counting system. It is a great advantage if the transmission of data among these components takes place in a standardised format. The different components will know exactly the format of the data to be sent and received, the distribution of tasks among the components is clear, and it will be an easy task to replace a component with a corresponding component. These matters are important not only to have different components produced and delivered by different software and hardware providers, but also to process the same data in parallel by different components(N-version-systems, see section 8.7.9).

In transmitting data among different components, considerations must be made as to what extent the data should be self-descriptive, i.e. to what extent the data should include

information about themselves. If the data are not self-descriptive, all the components sending and receiving the data must know the format of the data and what they mean. Self-descriptive data have the advantage that the components processing them can adapt/adjust to the data they receive. It is also possible to generate the sub-components which send and receive data on the basis of the data descriptions. Self-descriptive data have the disadvantage that the descriptions often are repeated, which has the consequence that more data are transmitted among the modules than are strictly necessary.

A format for self-descriptive data which has become generally accepted is the XML format (Extensible Markup Language)[70]. A specialized variant of this language, the EML (Election Markup Language) has been developed for e-voting[71]. Standards 66 to 68 of the Recommendation of the European Council state that data transmission among different components in an e-voting system shall take place by means of standard transmission formats, such as the EML, which shall be used whenever possible.

The EML is an extensive standard, and it is hard to say off hand whether it is suitable for Norwegian elections. The working committee has had a prototype of a complete e-voting system constructed for Norwegian elections. The transmission of data in this system is in accordance with the EML standard (Aas 2005). Our experience is that with a few extensions and adaptations of the EML standard (version 4.0) it may be used for Norwegian elections. The Working Committee recommends that initiatives should be taken as soon as possible to integrate these changes in the next version of the standard.
One of the circumstances that make Norwegian elections special is the option for the voter to modify the ballot before it is cast. This requires the system to transmit more data to the ballot receiving server than what is the case in other countries. Capacity restrictions on the transmission of data between the voting client and the ballot receiving server, and processing capacity restrictions in the ballot receiving system must be paid particular attention to.

8.7.4 Security log

The voting and all other significant events related to the use of the voting system must be logged properly to ensure that the whole operation is open to audit and control (cf. Standards no.102 and 103). The log comprises extra copies of the ballots submitted, identified attacks on central components and functionalities, all voting-related actions performed by the election official, such as opening and closing the ballot receiving server, opening the electronic ballot box, decrypting received ballots and opening the counting and calculation system. The EC Recommendation also requires protection of the log against attacks (cf. Standard no 109).

8.7.5 Certification

Highly security sensitive, specialized modules must be certified by accredited certification agencies (see chapter 9 below and Standards no 111 and 112 of the Recommendation of the European Council). Highly security sensitive modules which must be inspected thoroughly should be clearly separated from less security sensitive modules. The highly security sensitive modules must be designed and programmed in such a way that the inspecting body can infer their correctness by inspecting the program itself ("white box testing"). The design should not be based on extensive, over-complex software libraries which may contain security loopholes.

[70] See http://www.w3.org/XML/
[71] See http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=election

8.7.6 Solutions based on well tested software

To the extent highly security sensitive elements of the system are based on software from a third party, this software should be generally used, well tested and open to inspection. Examples are encryption and decryption modules

8.7.7 Open code?

Using an open source code is one way to protect system solutions from fraudulent as well as unintended codes. Traditional open source code projects have been based on a cooperation of several collaborators for development and functionality. This philosophy contributes to making it very difficult to build in security loopholes and fraudulent codes. One of the advocates for using open source codes and collaborative system development in voting applications used to be Jason Kitcat. In his 2004 article, however, he withdraws his standpoint (Kitcat 2004), but mainly because he thinks open source codes do not affect the fundamental problems related to electronic voting.

The working committee is of the opinion that it is neither realistic nor preferable to develop a highly security sensitive application such as an election as a traditional open source code project. A voting system requires a step by step development with strict deadlines, strict delivery schedules and well defined responsibilities and roles. An open source code may also expose very important security measures in unfortunate ways.

The requirements of verification generally and certification procedures as sketched above specifically, demand that the source code be available for inspection. This entails that all system providers must commit themselves to giving access to the source code for audit and verification.

8.7.8 User Interface

The user interface is central in e-voting, and should follow a standard or be subject to strict specifications or instructions (Standards no. 61 to 65 of the Recommendation of the European Council spell out some such requirements). The objective is to have a product-independent design in the sense that the user interface, as far as possible, is the same from one election to the next.

8.7.9 Distributive server structure

Figure 8.13below is an overall illustration of the computer based subsystems of a voting system built in accordance with the principles sketched in the present chapter. In this section we discuss to what extent the different core sub-systems should be distributed and duplicated.

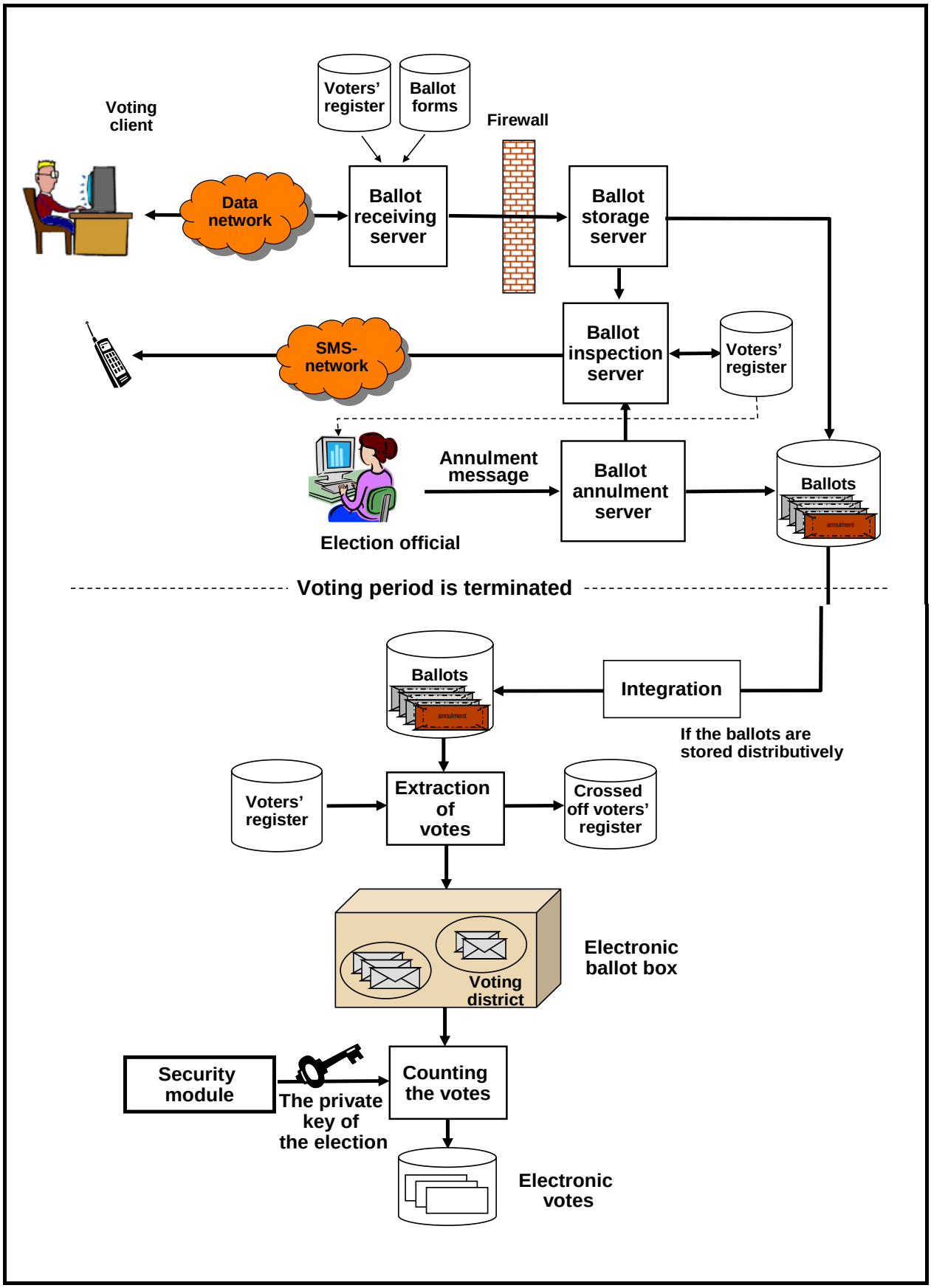


Figure 8.13: Overall illustration of the voting system

Ballot receiving servers
The availability of ballot receiving servers is very important. In a national, fully developed e-voting system several ballot receiving servers must be available and distributed over the country. The probability is then very low that all the servers break down at once, due to a denial-of-service attack, some technical problem, operational problem or power failure.

Ballot storage servers and ballot annulment servers
The working committee recommends that all the incoming ballots are stored in one or a very limited number of ballot storage servers, mainly to accommodate the security requirements and the "uptime". The risk of deviations and operational disturbances increases with the number of different storage servers used. Another thing to consider is that in a distributed system incoming ballots and "annulment envelopes" from the same voter may reside on different servers, although they must be coordinated before ballot extraction. A voting system based on hundreds of "electronic ballot boxes" collecting ballots for subsequent transfer to the counting system is considered less relevant.

Other core sub-systems
With respect to the other core sub-systems (ballot extraction and counting) the working committee recommends that they are placed in one or a few sites for security reasons. These processes must be under surveillance and the transaction must be logged with minute precision.

The hardware and the infrastructure must be designed to avoid any single point of failure. This means that all critical components/elements must be duplicated, several network connection and several physical servers running in parallel. The power supply must be secured. Spare installations must also be available and accessible, preferably in a different place geographically, in case some core sub-systems are out of service.

To increase the level of security it may be a good idea to duplicate the core solutions to establish what has been called an N-version system (Liburd 2004). The principle is that the critical processes run in parallel on several computers, preferably computers manufactured by different producers and designed with different operating systems, as well as software produced by different software suppliers using different methods in their system development. If parallel processes yield the same results, we are quite certain that the results are correct. N-version systems very close to guarantee that there are no unpremeditated errors or any consciously programmed "back doors" in the core systems. Such solutions are expensive, but will to a large extent prevent insider sabotage or unpremeditated faults leading to erroneous results.

8.8 Recommendations

- The technical solutions should be designed to be easily adjustable to voting through different channels in controlled as well as uncontrolled environments. This simplifies the audit and certification tasks, removes the problem of technical barriers against changes if the technological or political conditions change, and helps the voter feel confident under the new conditions.
- Incoming ballots should be registered on a "write-once" medium to preclude deletions or overwriting of the ballots.

- Highly security sensitive components must undergo certification by an independent certification body.
- To make the software solutions secure and certifiable, highly security sensitive components must be kept separate from the other components, and must be designed and programmed as simply as possible to enable the inspecting body to infer their correctness by inspecting the program itself (white box testing).
- Highly security sensitive software libraries, for encryption and decryption purposes, must be open, generally available and certified by security experts.
- To enable white box testing, the manufacturer must give the certification bodies free access to the source code.
- Data exchange among components must take place in a data format specified in the EML code, with the exception of data transmission between the voting client and the ballot receiving server.
- The voters' access to the voting system should be regulated by using publicly approved PKI solutions at level "Person High". No special voter credential should be issued for voting purposes only.
- The voter should have a receipt confirming that his or her ballot has been received and registered in the core system, preferably through a different channel than the channel used for the casting of the ballot.
- To strengthen security, N-version systems and the duplication of systems and storage units should be considered.
- Politically binding elections should not be run on technical equipment which is outside the control of the electoral authorities as long as the security level is not higher than at present.

9 Control and approval of an electronic voting system

9.1 Introduction

The present chapter discusses ways to make the technical solutions used in electronic elections as safe and trustworthy as today's manual procedures. Three tasks formulated in the mandate are dealt with in particular:

- Consider effects of changing control routines, from that of the layman to the professional expert, including effects on the voting system with respect to the audit and administration of the election and the competence of the administrators. (14)
- Consider the responsibilities related to electronic voting, from a local, regional and national perspective. (15)
- Consider how an approval of electronic voting systems should be conducted. (16)

Although the three tasks relate to different aspects of e-voting, they have one thing in common: they are all concerned with the task of maintaining the voters' confidence in political elections. If we give up layman control, we risk that the heritage of democratic institutions in Norway is stirred. Does the change mean that the "computer experts" take over the control of the election?

These are important and complicated questions, which will be taken up and discussed in turn. The first question is whether the introduction of e-voting will involve changes in the system of layman control (9.2). A general section follows on system certification (9.3), the most relevant solution (possibly the only relevant solution) for meeting the challenges outlined above. The most central types of certification are accounted for (accredited certification bodies, certification of activities and technical solutions). We then go on to discuss the Norwegian solution (9.4), emphasizing in particular the exploitation of existing arrangements related to information security. A short section follows on the need for a national requirement specification for electronic voting. In the last section, some concrete points of recommendation are put forward.

The main conclusion arrived at in this chapter is that the introduction of e-voting will entail a partial transfer of the control to the professional. An e-voting system will have certain consequences for the election system, with respect to functional requirements, control procedures as well as election administration and competence requirements. However, the working committee recommends that current control and approval procedures are maintained for a period of time. Great changes are not to the purpose, yet new solutions for control and approval should be developed, and should be included as an important task in the mandate for the recommended project group cf. chapter 10. An interim solution is to grant this project group the responsibility for approving the technical solution.

9.2 From the layman to the professional?

A system for electronic voting changes the conditions for election control and approval in many ways. Three conditions are particularly important in this respect. First of all, the local

administrators can not be expected to have the technical competence required to control and approve an electronic voting system. Certain parts of the electronic solutions are very complicated and the availability of computer competent resources is very limited in many municipalities.

Secondly, e-voting entails changing procedures for control and approval. Control comprises manual control of the voter's identity in the polling station, control of all ballots and ballot submissions, the registration of personal changes on the ballots and ballot counting. In today's system, this control is taken care of by the polling committee and the electoral committee. In a manual system the officials counting the ballots have to record all the results in accordance with a detailed protocol specified by the Ministry. The election records are presented to the municipal council/ county council before a resolution is passed to approve/disapprove the election. The council thus passes a resolution on the basis of meeting protocols kept by people who have personally controlled the counting of the actual ballots. In an electronic system the validation and counting of the ballots are automated. The election records are presented in the form of a print-out from the computer system. Also, the voter identity is controlled by an automated system. Automation of the process reduces the election officials' control tasks, but at the same time restricts layman supervision and inspection, to the effect that the election procedure is no longer transparent.

Thirdly, the *EC Recommendation* on e-voting has a number of control and validation requirements which are strongly supported by the present working committee. Most important of these, perhaps, is the requirement that e-voting solutions "shall be assessed by independent bodies" (Standard no 85), but the Recommendation also requires that the Member states "introduce certification processes that allow for any ICT (Information and Communication Technology) component to be tested and certified as being in conformity with the technical requirements described in this recommendation". This means that if e-voting is introduced on a large-scale or national basis, certain changes in the distribution of responsibility and administration of elections seem inescapable.

9.3 About certification

Competence requirements, information security considerations and the EC Recommendation on e-voting all point to the need for some kind of *certification* of the e-voting solutions, as illustrated above. But what exactly does this entail?

The intention behind certification is that the buyer (the electoral authorities in this case) is assisted by a "trusted third party" to create trust in the system. A "trusted third party" is a certification body or an independent agency whose competence in the field of information security is so high that they are considered the best to assess whether the system supplier delivers on its promise. Certification is a type accreditation of a product or system, based on a thorough evaluation analysis (www.sertit.no). The evaluation is made by computer experts (usually an accredited security system firm) and comprises technical analyses and tests to verify that the solutions provided satisfy the functionality and security requirements specified. The requirements are normally formulated by the authorities or by internationally accredited standards. Certainly, such certification systems can not guarantee absolute security of an e-voting system, but by means of adequate methods they can try to detect possible security

loopholes, control the correctness of the computed results, the trust of the service providers, etc. Certification, in other words, implies a risk reduction for the buyer.

Three different kinds of certification are needed for controlling an e-voting system adequately:

- Approval of *the certification procedures* (accredited certification bodies).
- Approval of system suppliers' *routines and procedures* (certification of operations).
- Approval of *technical equipment and solutions* (product certification).

The first kind – approval of certification procedures – relates to finding firms or agencies with sufficient competence to control the suppliers and their products. In the area of information technology there are several such agencies, some of which specialize in IT Security. They are sometimes called "accredited certification bodies" or evaluation agencies. Normally the agency is certified for a clearly defined standard – typically a Norwegian standard (NS) or an international standard (ISO). For example, the assessment body may satisfy the criteria for testing laboratories as formulated in Standard NS ISO/IEC 17025:2005.[72] Other accreditation systems also exist, some of which have no definite standard for the operation to be certified, but a set of established criteria, often based on some form of requirement specifications, in accordance with which the agency or firm has the required competence to perform control operations and recommend the approval of the products and operations. This is a somewhat weaker form of "trusted third party" than the accredited certification bodies. It is important, of course, that agencies set to test and certify e-voting solutions designed by other companies can document thorough knowledge and understanding of the requirements specified for the solutions as well as an in-depth understanding of the practical procedures of political elections.

The second kind of certification relates to the approval of the system suppliers' routines and procedures (certification of operations). What is at issue here is that the suppliers of e-voting solutions have gone through certification procedures securing that the requirements specified are actually complied with. Such requirements may be that the suppliers have defined contingency plans, responsibilities, guard arrangements, routines for the detection and correction of errors, access controls, documentation, training, etc. Vulnerability tests and risk analyses are usually also required. For e-voting this means that a set of specified requirements is defined which ensures that the election system as a whole and in part (in broad terms) is designed on the basis of thorough analyses of possible threats against successful operations. Based on their risk analyses the agency must be able to document that the solutions are sufficiently protected to overcome potential risks specified in the analyses, such as for example pre-defined limits for service failure. The risk analyses must be documented and made available to the certification authority. Furthermore, the analyses or other necessary requirements specified for potential system suppliers must have a set of domain specific legal provisions to comply with, cf. chapter 6 of the present report. The routines and procedures of the system suppliers may be tested for approval before an offer is made for a system solution, and should be in principle independent of the technical voting solution design. A certification of the operational standards may only be made by accredited certification bodies or evaluation agencies. Cf. the above discussion. To say it in plain words: *the electoral authorities may not decide on technical voting solutions from suppliers whose systems have not been already certified*.

[72] NS-EN ISO/IEC 17025:2005: General requirements on the competence of testing and calibration laboratories. For further information about the standard, see http://www.standard.no

A couple of standards have been defined for the certification of system suppliers' routines and procedures. In addition to the Recommendation on standards for e-voting, the 2005 Standard NS-ISO/IEC 17799[73] and the 2005 Standard ISO/IEC 27001[74] are both relevant in this context. The standards relate to information security management. In simplified terms, the NS-ISO/IEC 17799:2005 focuses on measures to improve the security of information and provides a multitude of measures that relate to different aspects of the operations. This standard furthermore provides relatively clear guidelines for establishing a security strategy, administrative engagement, delegation of responsibilities, physical security systems, access control, implementation, operation, disposal, etc. The ISO/IEC 27001:2005 standard, on the other hand, focuses on the very management of information security: the ISMS - Information Security Management System. Examples are routines for establishing, operating, monitoring and maintaining as well as documenting control and administration management. A list is also provided with central objectives and measures that must be selected as part of the tasks specified for establishing a management system for information security. (www.standard.no).

The third and final kind of certification relates to the approval of the technical solutions (product certification). The most central requirements have been discussed already in the previous chapters and in the Recommendation on e-voting. There is no need, therefore, to go into detail on these matters in the present chapter, only emphasize a few points of particular relevance for control and certification measures. First of all, quality measures must be defined for the individual technical modules that together make up the voting system. This enables us to make a clear division between secure and insecure modules. Next, as a minimum requirement the solutions must protect the source code against the possibility of being changed after inspection; physical measures, version control, check sums and digital sealing**.** Critical technical solutions shall under no circumstances be used unless they have been tested and approved. Moreover, a log must be provided which keeps records of all changes in the system. Transparency is an overall requirement, which means that all modules in the system must be available for control and certification on demand – at least for the competent electoral authorities and the trusted third parties. The conditions for access to the source code must be clearly defined, and the technical change of any sort must be documented and reported to the electoral authorities. In short, the technical solutions must maintain the quality, availability, integrity and confidentiality of the votes. Finally, the solutions must also keep the votes sealed and secret until counting. Encryption is necessary if the votes are stored or communicated outside controlled environments. This includes a requirement that any information about voters and their cast ballots must remain stored and sealed as long as any link is maintained between the voter and the vote.

9.4 Details about Norwegian certification systems

Two different and partly complimentary certification systems exist in Norway. Both of them deal with information security and are thus considered competent environments able to support or assist the suppliers as well as the authorities in their efforts to provide operative e-

[73] NS-ISO/IEC 17799:2005: Information technology, Information security management. For further information about the standard see http://www.standard.no/

[74] ISO/IEC 27001:2005: Information technology -- Security techniques -- Information security management systems – Requirements. The standard replaced the British standard (BS) 7799-2 as of the autumn 2005. For further information about the standard see http://www.standard.no

voting systems in Norway. It is of vital importance that the different certification environments are supplemented with specialized competence in the area of elections, as that seems to be missing.

One of the environments is Norwegian Accreditation (NA) appointed by the Ministry of Trade and Industry to perform technical accreditation analyses and inspection in compliance with the OECD regulations on ”Good Laboratory Practice” (GLP). Accreditation is a “public recognition of the competence and ability of an organization to perform given tasks in compliance with given requirements” (www.akkreditering.no). The function of the arrangement is to define certain agencies, controlled and approved by Norwegian Accreditation, as “accredited certification agencies”. Several such agencies exist in the field of IT, although only three companies have been certified as accreditation agencies in the field of IT security in compliance with the international standard ”Information Technology-Security Technology – Information Security Management” (NS-ISO/IEC 17799:2005). The three companies are:

- Det Norske Veritas Certification AS
- Nemko Certification AS
- Teknologisk institutt Sertifisering AS.

The strength of this arrangement lies primarily the management of information security in organizations. It relates to good practice for information security and comprises more or less all aspects of importance for managing comprehensive information security operations. Some agencies also offer assistance in defining requirement specifications for the buyer and certain other services related to information security systems. The weakness, in the opinion of the working committee, is that the environments are not formally or explicitly certified to perform technical analyses, including evaluations of individual modules in a voting system.

The other system is the National Security Authority (Nasjonal Sikkerhetsmyndighet, NSM), the Certification Authority for IT security *(SERTIT)* in particular. The arrangement of a national body for the certification of IT security in technical products and systems came about as the result of a recommendation by the Council for IT Security (Rådet for IT Sikkerhet, RIS) in 1997. SERTIT is currently a public certification authority for IT security placed under a cross-institutional management committee consisting of members from the following bodies:

- The Ministry of Defence (leader)
- The Ministry of Government Administration and Reform
- The Ministry of Justice and the Police
- Norwegian National Security Authority
- The Data Inspectorate
- Norwegian Accreditation
- Abelia
- Standards Norway.

The tasks defined for SERTIT, which also functions as the Secretariat for the Management Committee, consist in issuing certificates and certification reports to private and public agencies, formulating the conditions and regulations for IT security in Norway and ensuring that the regulations are followed by the involved parties. Furthermore, they are responsible for certifying and inspecting private firms as evaluation agencies. Specified criteria must be

satisfied and testing laboratory accreditation in accordance with NS-ISO 17025 must be obtained for an agency to be certified as an accredited evaluation agency. The company must make a test evaluation to demonstrate their understanding of the *Common Criteria* and the *Common Evaluation Methodology (*www.sertit.no). SERTIT is furthermore the Norweigan representative in the "*Arrangement on the Recognition of the Common Criteria Certificates in the field of Information Technology Security (CCRA)",* which is relevant in view of the Recommendation of the European Council being founded on the security measures defined in Common Criteria (CC). The following two companies have been recognized as accredited evaluation agencies by the SERTIT:

- NorConsult AS
- SeCode Norge AS

The greatest advantage of the SERTIT arrangement is that the evaluation agencies (?) also certify technical components. The disadvantage is that the arrangement is based on a rather comprehensive (and expensive) set of criteria. The agencies, therefore, can refer to a very limited set of assignments and references. But their portfolios are growing nationally as well as internationally. There are also different modules and levels, which create certain flexibilities. A final, but essential consideration is that this environment knows and is updated with respect to the routines (and procedures) forming the basis for the CC security methodology laid down in the Recommendation (Common Criteria/ ISO/IEC 15408:2005).[75]

9.5 The need for detailed requirements specification

Irrespective of any particular certification regime it is a fundamental requirement that some form of "standard" or requirement specification is formulated for electronic voting procedures in Norway. This specification should base its formulation on the most relevant documents discussed in the present report (security standards, the Recommendation on e-voting from the European Council, legal acts and provisions, etc.). Some flexibility is considered acceptable for such specifications, but in the opinion of the working committee they should typically include the following:

- Functional requirements
  - *Laid down in the Recommendation of the European Council on e-voting including its explanatory memorandum(see Appendix A)*
  - *Requirements as specified in the legal considerations, cf. chapter 6 of the present report*
  - *Requirements related to the technical solutions as specified in chapter 8 of the present report*
- Requirements related to the system suppliers
  - *Certified in accordance with NS-ISO/IEC 17799:2005:Information technology, Information Security Management*

[75] The standard is divided into three parts. Part 1 (ISO/IEC 15408-1:2005) consists of an introduction followed by a general framework for the evaluation of Information Security. Part 2 (ISO/IEC 15408-2: 2005) has a long list of functional security requirements for IT systems. Part 3 (ISO/IEC 15408-3:2005) specifies the requirements on quality management of the solutions etc. Further information on the relation between the Standard and the EC Recommendation is found in the explanatory memorandum related to the Recommendation. Further information on the ISO/IEC 15408:2005 is found on the following web pages: www.iso.org/http and www.commoncriteriaportal.org.

    - *Certified in accordance with ISO/IEC 27001:2005: Information technology -- Security techniques -- Information security management systems – Requirements*
    - *Conditions for the sub-suppliers*
    - *Response time in cases of error and user support*
    - *Future developments*
    - *Assistance related to possible change of suppliers (acquisitions, bankrupcies, etc.)*
- Requirements related to the delivery
    - *Training*
    - *Documentation*
    - *Testing*
- Requirements related to version control
    - *Change procedures*
    - *Auditability*
    - *Check sums, etc.*
- Requirements related to operations and maintenance
    - *Performance requirements (availability (uptime), capacity, service quality)*
    - *Error handling*
    - *User support in different phases*
    - *Contingency (crisis – catastrophies)*
- Local adaptations (options)
    - *Definite access points(buildings)*
    - *Infrastructure*
    - *Integration of existing technology*
    - *Guard arrangements, training, etc.*

The above is not a comprehensive list. It is meant to exemplify certain central requirements that must be stated in a Norwegian requirements specification for e-voting. Further details must be defined. The working committee has considered and recommended a technical solution which may form the basis for drawing up such a document. However, the committee has neither considered it possible nor to the purpose to set up a complete requirement specification within the framework of the mandate. Yet a complete requirement specification is considered necessary for any future development of an e-voting system. We would like to emphasize three areas of application for such specifications: First of all the requirement specifications are necessary for the system suppliers to develop a system and to have their activities, their sub-suppliers and their technical solutions approved. Secondly, the requirement specifications will be used by the certification bodies as criteria for certifying suppliers and technical solutions. Last, but not least, the requirement specifications are needed for reference (with possible local options) by the electoral authorities in the consideration of tenders.

9.6 Recommendations

The general question taken up in this chapter has been how we can best ensure the security and integrity of the technical solutions for e-voting. This is a very difficult task, yet essential for maintaining the confidence in Norwegian election procedures. The central argument is that before an e-voting system is introduced, and at regular intervals after that, an independent

body, appointed by the electoral authorities, is set to control the correct functionality of the system and to ensure that the system suppliers have taken the necessary measures for securing the system. The following recommendations result from the above considerations:

- Pre-certification should be made of the human resources and the operations which on behalf of the electoral authorities approve the system suppliers and technical solutions for e-voting (accredited certification bodies or evaluation agencies).
- Pre-certification should be made of the routines and procedures to be followed by suppliers of e-voting solutions in order to secure the voting solutions. Accredited certification bodies are responsible for the certification of system suppliers. The electoral authorities are obliged only to accept system providers who are certified with respect to the critical elements of the e-voting solutions.
- Pre-certification should take place of the technical equipment and solutions. As a general rule non-certified products should not be used in the voting solutions. For critical parts of the solutions certification is an absolute requirement.

The recommendations stated above imply a considerable risk reduction for the electoral authorities, but do not guarantee the elimination of every risk. The recommended solution entails a certain change of control from that of the layman to that of the professional. E-voting will change the election system with respect to the control function, the administration of elections and the required competence of the people involved. A prerequisite for the recommended solution is that a good, detailed requirements specification for e-voting in Norway is formulated. Before a de facto standard or act or legal provision for e-voting is presented and approved by the authorities, the requirement specifications formulated must follow the legal, operational and technical standards for e-voting laid down in the Recommendation of the European Council. The specifications should also define and maintain the changes and amendments to the Recommendation proposed in the technical solutions in the present report (cf. chapter 8).

The procedure envisaged by the working committee consists in a formulation of the requirement specifications by the electoral authorities. This work may be outsourced to qualified agents. The main idea is that existing arrangements for the certification of agents and technical solutions are used in the area of information security. We would like to emphasize that we do not recommend an appointment of new certification bodies for e-voting in particular. When the requirement specifications are formulated, they should be made available for potential suppliers of e-voting solutions in Norway and abroad. Potential suppliers are thus informed of a need to have their system solutions, as well as the systems provided by sub-suppliers, approved by a certification body in order to be considered service providers on the Norwegian market. Through the requirement specifications the certification bodies will also have definite criteria to go by for the certification of system suppliers and technical solutions. During a pilot regime the electoral authorities may use the requirement specifications as a reference document in considering bidders/tenders, possibly supplemented by local options.

The working committee understands that a certification system for e-voting can only be built over time, and should be defined as a central task for the new project group recommended in chapter 10 of the present report. An interim solution is to make the suggested project group responsible for certifying technical solutions. Members of existing certification bodies in Norway should therefore be represented in, or at least consulted by, the recommended project group.

10 Pilots - plans and frameworks

10.1 Introduction

The main objective of the working committee's recommendations is to make it easy for voters to exercise their democratic rights and to reduce the costs related to this exercise. To achieve this objective, one strategy is to make e-voting facilities in uncontrolled environments available for all voters. The introduction of an e-voting system will increase accessibility and, in the long run, reduce costs related to running an election, as well as ensuring faster and more accurate vote counting. One objection is that e-voting may reduce the formal atmosphere associated with the act of voting in a traditional polling station. The working committee would like to counter this objection by emphasizing that e-voting is only recommended as *a supplement* to traditional voting procedures. Traditional voting in polling stations will be maintained in the foreseeable future**.** This means that voters unacquainted with or unfamiliar with e-voting technology will have the right to cast their votes according to traditional practice. It is worth mentioning, however, that the extensive practice of submitting advance votes over the last years has already contributed to changes in traditional voting practice.[76]

One possible consequence of introducing the opportunity to vote in uncontrolled environments – whether the vote is cast electronically or manually (for example by post) – is that the right to secret suffrage may be threatened. The voter may be under undue influence (as in, for example, *family voting*) and the buying and selling of votes may not be prevented. By permitting multiple submissions of advance votes, as well as the right to cast a vote again in controlled environments at a polling station, the negative consequences will be reduced significantly, although not avoided completely.

An absolute requirement for e-voting in uncontrolled environments is that the system builds on very strict security requirements and that the methods developed do not reduce the voters' confidence in the system. Current technology cannot guarantee this. The working committee is therefore of the opinion that e-voting is not at present recommendable on a large-scale basis.

Notwithstanding, it is not inconceivable that in the not so distant future, considerable pressure will be brought to bear to introduce remote e-voting in uncontrolled environments over time. Such pressure may arise as the result of a constantly growing use of ICT in society as a whole, or because e-voting is introduced in other countries, or because voter turnout falls drastically. To prevent a situation in which e-voting in uncontrolled environments is introduced without prior testing, the working committee will emphasize the need for aggressive initiative by central government in this area. Systematic pilot studies and evaluations should be carried out as soon as possible.

[76] In the last three parliamentary elections in Norway approx. 20% of the votes have been submitted in advance. See fig. 5.1, ch. 5.

10.2 The purpose of pilots

There are many reasons for recommending a period of comprehensive testing before an electronic voting solution is put into general use in uncontrolled environments. The following are of particular importance:

- Ensuring voters' confidence in the voting operations.
- Clarifying problems related to the risk of undue influence and the buying and selling of votes.
- Establishing technical solutions that satisfy the fundamental security requirements.

Voters' confidence in the voting system is of utmost importance, not only for voter participation, but also for the democratic principles on which the system is founded. Confidence is fundamentally dependent on the voters' understanding of the system provided for casting a vote. Traditional voting procedures are simple, well known and well tested. Voters in Norway have great confidence in the elections. This confidence has been built over time, and relates to every step in the process. Confidence, however, can easily be lost if any element of doubt is raised as to the ways the system works. According to standard no. 20 of the EC Recommendation on e-voting, the member states "shall take steps to ensure that voters understand and have confidence in the e-voting system in use".

The general conditions for moving the voting procedure from controlled to uncontrolled environments have been discussed in chapter 5 of the present report. The challenges related to the problems of undue influence and the buying and selling of votes are complex, and it is very important that the implications and consequences of these challenges are considered in detail.

In the opinion of the working committee, current technical solutions are not good enough for recommending a general introduction of e-voting in uncontrolled environments at this stage. The most important problems with electronic voting over the Internet relate to the security of the voting client, i.e. the voter's personal computer. For other types of technical solution, such as SMS voting, the user interface is a key concern and requires extensive testing. Furthermore, it is very important that the technical solution is designed to ensure secrecy of the vote cast and to secure against any loss or manipulation of the ballots submitted.

Pilots are needed in order to gain experience on the success and failure of different technical solutions, to stimulate public debate and, not least, to create confidence in the systems over time. Pilots provide an opportunity to make small-scale tests with regard to different solutions before they are put into use on a national basis. It seems particularly useful to explore areas in which the consequences of the changes may be substantial. Pilots are also highly relevant where the differences among alternatives are not clearly defined, or the direction to be taken is somewhat unclear. The method of trial and error will give experience that may be used to specify alternative solutions. Moreover, pilots often have the effect of mobilising changes, since the participants are given the opportunity to try out something new and develop good exemplars. Pilots thus help counteract a certain resistance, provide knowledge and prepare the grounds for change. Finally, the working committee considers it necessary to draw experience from electronic voting pilots, as this experience in turn will form the basis for preparing possible amendments to legislation.

10.3 Plans for pilot projects

10.3.1 Organization

Experience drawn from pilots in other countries shows that e-voting pilots are comprehensive and require significant resources. Considerable resources must therefore be set aside in order to prepare, conduct and evaluate such projects. The tests should extend over several elections, gradually including more functionalities and step-by-step testing of different solutions.

Fundamental democratic principles are at stake in the election event. Pilot projects on e-voting must therefore include systematic testing that can form the basis for continued evaluation. Such evaluation is needed if the pilot runs over several elections. In our opinion, the pilots should be initiated and administered centrally and include active participation from local electoral authorities. The participation of local authorities should be on a voluntary basis.

The working committee recommends the appointment of a broadly composed project committee, which should be given the administrative responsibility for conducting the pilots. The project committee should have expert competence in computer science, electoral matters and legal matters. It should be organized by the Ministry of Local Government and Regional Development. Sufficient financial resources must be made available before the tests are started. In accordance with the preceding discussion, the working committee assumes that the pilot projects are financed by the central government.

10.3.2 The framework

Pilots should be conducted in selected municipalities on the basis of a central initiative. The tests may be run on a particular group of voters, such as, for example, the disabled. However, it is important that the pilots are organized in a way that does not violate the legal right to a secret vote. One relevant issue in this connection is that the arrangements are not tested on too limited a group of people in a voting district, as could be the case if the pilot is run on a group of voters residing abroad. Expatriates are spread all over the world, but their votes are sent to and counted in their respective home districts (i.e. the voting districts to which they are assigned, on the basis of the Population Registry).

Referendums are not regulated by the Elections Act. The local governments are free to conduct referendums and to establish a set of regulations for such referendums. A referendum can only be consultative, and there is no requirement that all the voters of a municipality have to take part. Local referendums, therefore, offer very favourable conditions for testing electronic voting solutions. However, the working committee recommends that such testing is organized and administered by central authorities, as this will ensure that they make up an integral part of an overall plan for testing different aspects of e-voting and may be integrated in the step-by-step evaluation intended for gaining knowledge about this form of voting.

Pilot projects in schools will be of limited value due to the special conditions for this form of election. Knowledge gained from pilots in school elections is only partially relevant for general elections. However, school elections may be relevant for testing certain important aspects such as user interfaces and performance.

10.3.3 General plan

The working committee recommends that the pilots be conducted in clearly specified steps within a well-defined framework as regards the extent and purpose of the tests. Each step must bring the project forward and yield real results. At the same time, the pilot should be conducted at minimal risks.

The pilots should start in controlled environments. In subsequent phases the voting act may be gradually moved to uncontrolled environments, as suggested below:

- Controlled — Electronic voting in the polling stations or other premises controlled by an election official.
- Uncontrolled (i) — Electronic voting in uncontrolled environments with controlled hardware and software. This procedure requires the distribution of a CD-ROM (or a corresponding device) to prepare the voting terminal for the voting act. The system ensures a controlled channel from the voter's keyboard to the ballot receiving server, thereby reducing the risk of virus attacks on the voting client. A controlled channel also makes a secure log/returning message solution possible.
- Uncontrolled (ii) — Electronic voting over the Internet on a standard, personal computer. The procedures also comprise voting through other channels such as cell phone messages. This alternative requires that considerable progress is made in the area of security solutions for personal computers and the Internet.

The first step, testing voting solutions in controlled environments only, may be considered too restricted for our goals. The working committee would therefore like to widen the extent of the first step to include different types of election:

- Binding — Binding political elections, such as elections for the national, regional and local governments as well as for the Sami Assembly. In this type of election the voting act may be complex, due to the comprehensive candidate lists and the opportunity to make personal modifications on the ballots. The consequences of error may be substantial. Binding political elections require very high security standards at all levels.
- Consultative — Consultative referendums and other non-binding elections at the local level. The consequences of error in this type of elections and referendums are not as serious as in traditional, binding elections, and the security standard requirements are lower.

Table 10.1: General plan for pilots

Environments	Type of election	Step1	Step2	Step3
Uncontrolled, Uncontrolled computer(i)	Binding			
	Consultative			
Uncontrolled, Controlled computer (ii)	Binding			
	Consultative			
Controlled	Binding			
	Consultative			

10.3.4 Initiation phase

Framework
Establish the organization of the project and prepare the pilots.

Objectives
The first step in the pilots is to establish a project organization with a mandate, a progression schedule and a budget. The project group should start off by working out a requirement specification for electronic elections. The requirement specification should be based on existing documentation and should comprise the following central areas: (see chapter 9 for details about the content):

- Overall requirements with reference to relevant statutory provisions and standards
- Functional requirements, including security requirements
- Supplier requirements
- Delivery requirements
- Version control requirements
- Operation and maintenance requirements
- Localization requirements (options).

The project committee should assist the Ministry in working out regulatory provisions for the pilots. One way would be that the committee formulates a proposal for regulatory provisions which may then be adopted by a resolution in the Ministry.

In the initiation phase, activities should also aim at establishing a formal certification system for voting solutions. It does not seem feasible to establish a comprehensive accreditation system for the pilot phase. The project committee must take responsibility for adequate security and quality through a comprehensive and structured test regime.

Timeframe
Following the Ministry's consideration of the present report, a project organization should be established by the end of 2006.

10.3.5 Step 1

Framework
The first step should comprise tests on e-voting in controlled environments for binding as well as consultative elections and referendums. Small-scale projects should also be conducted in consultative referendums to test e-voting in uncontrolled environments on a controlled voting

terminal, i.e. a client installed with software distributed by the pilot administration on a separate CD-ROM. This is also the natural stage for initiating the establishment of a control and certification system, in cooperation with existing certification environments.

Objective
The main objective of these experiments is to test user interfaces, performance capacity, user acceptance and basic security aspects focusing on authentication (PKI), logging and secure storage of cast ballots. In choosing arenas for the experiments, account should be taken of the right to a secret vote.

Timeframe
Step1 should be concluded by the end of 2009.

10.3.6 Step 2

Framework
The second step should extend voting experiments in uncontrolled environments from a controlled terminal to include voting in binding elections. With respect to consultative elections or referendums, the second step should include the opportunity to submit an electronic vote from a terminal that is not controlled by the voting system. At this stage it would be natural to establish a provisional control system in cooperation with existing certification environments.

Objective
The main objective is to test voting in uncontrolled environments on a scale and in an environment in which the consequences of errors and voting fraud are limited. User acceptance and security solutions are in focus at this stage. Extended voting in uncontrolled environments will provide an opportunity to evaluate the consequences related to our fundamental democratic challenges: undue influence and the buying and selling of votes. Throughout this phase, experience should also be gained with respect to certification solutions. Step 2 is expected to contribute considerably to the evaluation of technical solutions.

Timeframe
The timeframe for conducting the tests outlined in step 2 will depend very much on the experience gained from step 1, technical developments and general changes in society.

10.3.7 Step 3

Framework
If the pilots in Step 1 and 2 are run successfully, and if technical developments have succeeded in finding solutions that satisfy the absolute security requirements, Step 3 should consist in conducting binding elections based on voting in uncontrolled environments from the voters' individual platforms (computers and software) with a restricted number of eligible voters. In this phase of the project, a complete certification system should be established.

Objective
Step 3 will thoroughly test all aspects related to electronic voting, including the legal, democratic, economic, practical and technical aspects. The organization of a certification regime should also be in place for evaluation.

Timeframe
The timeframe for carrying out Step 3 of the project will depend on the results gained from Steps 1 and 2, on the technical developments and general changes in society.

10.3.8 Information scheme

The communication scheme is an important part of the whole project. Objective, relevant information about the pilots at all levels must be communicated to the election officials, the voters and the media. Reference is also made to relevant requirements laid down in the EC Recommendation on e-voting.

10.4 Statutory basis for experiments

In the working committee's opinion, there is a statutory basis for pilot projects on e-voting in the Experiments Act as well as the Elections Act in Norway. However, it is not within the working committee's mandate to express an opinion on the appropriate statutory basis for conducting experiments of this kind.

10.4.1 The Experiments Act

Act No. 87 of 26 June 1992 on Experiments in the Public Sector (the Experiments Act) regulates experiments in the national, regional and local administrations.

In compliance with Section 3 of the Experiments Act, pilot projects may be approved of that depart from relevant Acts and statutory provisions on how the public authorities shall organize their work and solve the tasks they are set to do. For a pilot to be approved by the legal authorities, its objective must comply with Section 1 of the Act. Furthermore, the experiment must be justifiable and professionally well founded. Other regulations are laid down in Section 4, in which it is stated that an experiment may not be approved if it represents a limitation of the rights or an extension of the responsibilities of a citizen in accordance with relevant legislation. It is our opinion that these regulations have definite consequences for the way the experiments on e-voting may be carried out. In accordance with these legal regulations, e-voting may only be offered as a supplement to ordinary voting practice, and the opportunity to change one's mind and re-cast a ballot must be given to voters who cast their ballots electronically.

In order for experiments to be conducted, a set of regulations must be laid down in special statutory provisions that can replace the provisions from which the departure may be made, cf. Section 5 of the Experiments Act. At the outset, regulations of this kind shall be formulated by the municipal council or the county council and be approved by the King. In accordance with Section 6 of the Act, the King may lay down further regulations regarding experiments under this Act, such as, for example, the number of experiment units in the project, the procedures for selecting the units and areas of the experiments, and the approval and initiation of the experiments.

10.4.2 Statutory basis for experiments in Section 15-1 of the Elections Act

When the new Elections Act was enacted in 2002, a provision relating to pilot schemes was laid down in Section 15-1 of the Act. Pursuant to Section 15-1 (1), the King may give his consent to "*pilot schemes in which elections under this Act are conducted in other ways than*

those that follow from this Act". In accordance with Section 15-1 (2), the King may lay down conditions for the pilots and determine from which statutory provisions any departure may be made.

The provisions in Section 15-1 were laid down in the Act only after the Act had been debated by the Storting, and are based on a proposal made by the Electoral Law Committee. The statutory provision itself does not place any restrictions on the kind of pilot that may be conducted. The working committee considers it natural that the restrictions stated in the Experiments Act should also apply to pilots under the Elections Act. Of particular importance is the requirement that pilots may not be conducted if they restrict the legal rights of the voter, cf. Section 4 of the Experiments Act.

Royal authority under Section 15-1 is delegated to the Ministry under certain conditions cf. Royal resolution of 14 February 2003. The background for this division is that several pilots related to elections involve legal, technical and practical matters that provide little room for political considerations. Such matters are best considered and determined by the Ministry. Pilots involving the more fundamental principles of the statutory provisions for elections must be considered and determined by the King in Council. It is stated in the delegatory resolution that cases representing a departure from the fundamental decisions in the Elections Act […], shall be resolved by the King in Council.

Literature

Ad hoc Touch Screen Task force (2003): Report to the Secretary of State.

Alvarez, R. Michael og Jonathan Nagler (2001): "The Likely Consequences of Internet Voting for Political Representation", *Loyola Law Review* 34: 1115-1154.

Alvares, Michael og Thad Hall (2004): *Point, Click Vote. The future of Internet Voting.* Brookings Institution Press

Ansolabehere, Stephen og Charles Stewart (2005): "Residual Votes Attributable to Technology", *The Journal of Politics* 67: 365-389.

Arbetsgruppen for e-röstning og demokrati(2002): *E-Röstning. En antologi.* Ju2002E.

Auer, Andreas (2005): "The European Union and e-voting" i Trechsel, Alexander H. & Fernando Mendez (2005), *The European Union and e-voting : addressing the European Parliament's internet voting challenge*. London: Routledge.

Berinsky, Adam J., Nancy Burns og Michael W. Traugott (2001): "Who Votes by Mail? A Dynamic Model of the Individual-Level Consequences of Voting-By-Mail Systems", *Public Opinion Quarterly* 65: 178-197.

Blais, André og Agnieszka Dobrzynska (1998): "Turnout in electoral democracies", *European Journal of Political Research* 33: 239-261.

Bruck, Shuki, David Jefferson, and Ronald L. Rivest (2001). *A Modular Voting Architecture ("Frogs")* http://theory.lcs.mit.edu/~rivest/BruckJeffersonRivest-AModularVotingArchitecture-doc.pdf

Buchstein, Hubertus (1997): "Bytes that bite: The Internet and deliberative democracy", *Constellations* 4: 248-263.

Bullock, Charles S. og M. W. Hood (2002): "One Person—No Vote; One Vote; Two Votes: Voting Methods, Ballot Types, and Undervote Frequency in the 2000 Presidential Election", *Social Science Quarterly* 83: 981-993.

California Internet Voting Task Force (2000): *A report on the Feasability of Internet Voting*.

Caltech/MIT (2004): *Electronically*. Voting Technology Project Working paper # 12 http://vote.caltech.edu/media/documents/wps/vtp_wp12.pdf.

Castberg, Frede (1947): *Norges statsforfatning. Bind I.* Oslo: Akademisk forlag.

Choe, Yonhyok (1997): *How to Manage Free and Fair Elections. A Comparison of Korea, Sweden and the United Kingdom.* Göteborg: Göteborg Studies in Politics.

Christin, Thomas og Alexander H. Trechsel (2005): *Analysis of the 26th September ballot as held in four Geneva municipalities*. E-Democracy Center. Geneva University.

Christensen, Dag Arne, Rune Karlsen & Bernt Aardal (2004): *På vei mot e-demokratiet? Forsøkene med elektronisk stemmegivning ved kommune- og fylkestingsvalget 2003*. Rapport 2004. Oslo: Institutt for samfunnsforskning.

"Code of Good Practice in Electoral Matters" CDL-AD(2002)023rev
http://www.venice.coe.int/docs/2002/CDL-AD(2002)023rev-e.asp

van Dijk, Jan A.G.M (2005): *The Deepening Divide. Inequality in the Information Society.* London: Sage

Drechsler, Wolfgang og Ülle Madise (2004) "Electronic Voting in Estonia" i Norbert Kersting and Harald Baldersheim (red.) *Electronic Voting and Democracy: A Comparative Analysis*, London: Palgrave Macmillan, 2005, 193-225.

e-Voting security study. Issue 1.2 (2002):
http://www.samfunnsforskning.no/files/rapp_07.pdf/

The Electoral Commission (2003): The Shape of Elections to Come. A Strategic Evaluation of the 2003 Pilot Schemes. London: The Electoral Commission

Elklit, Jørgen og Palle Svensson (1997): "What makes an election free and fair?" *Journal of Democracy* 8 (3): 32-46.

Fairweather, N Ben og Simon Rogerson (2002): *Technical options report*. Centre for Computing and Social Responsibility School of Computing, De Montfort University, Leicester.

Fairweather, Ben and Simon Rogerson (2002): "Internet Voting – Well at Least it's Modern" *The Journal of Representative Democracy*, 39.

Franklin, Mark N. (1996): "Electoral Participation", i Lawrence LeDuc, Richard Niemi og Pippa Norris, red. *Comparing Democracies: Elections and Voting in global Perspective.* Thousand Oaks, CA: Sage.

Fridtun, Dag (2005): *Tillit til elektroniske valg.* Masteroppgave. Oslo:Universitetet i Oslo, Institutt for Informatikk.

Fund, John (2004): *Stealing Elections. How Voter Fraud Threatens Our Democracy*. San Fransisco: Encounter Books.

Funk, Patricia (2004): "Is there an expressive function of Law? An empirical analysis of voting laws with symbolic fines". Upublisert notat. Stockholm School of Economics. (http://www.hhs.se/NR/rdonlyres/5E4F6B09-D249-46A8-81D2-24F08FDE3D1E/0/PFExpressive_Function.pdf)

Geser, Hans (2004): Electronic Voting in Switzerland, kapittel 6 i Kersting og Baldersheim: *Electronic Voting and Democracy. A Comparative Analysis*, Palgrave, London, 2004.

Geys, Benny (2005). “Explaining voter turnout: A review of aggregate-level research”, *Electoral Studies* (under trykking).

Gibson, Rachel (2001): “Elections Online: Assessing Internet Voting in Light of the Arizona Democratic Primary”, *Political Science Quarterly* 116: 561-583.

Internet Policy Intstitute (2001): Report of the National Workshop on Internet Voting: Issues and Research Agenda. Mars 2001.

Jansen, Arild & Dag Wiese Schartum (2005): *Informasjonssikkerhet : rettslige krav til sikker bruk av IKT*. Bergen: Fagbokforlaget.

Jefferson, David, Aviel D. Rubin, Barbara Simons og David Wagner (2004): *Secure Electronic Registration and Voting Experiment* (SERVE). Rapport.

Jones, Douglas W. (2004): "Auditing Elections". *Communications of the ACM* Vol.47, issue 10. ACM Press.

Karlsen, Rune, Bernt Aardal og Dag Arne Christensen (2005): «Elektronisk stemmegivning. De første norske erfaringer». I: Jo Saglie & Tor Bjørklund, red., *Lokalvalg og lokalt folkestyre*, s. 122-141. Oslo: Gyldendal Akademisk.

Karp, Jeffrey A. og Susan A. Banducci (2000): ”Going Postal: How All-Mail Elections Influence Turnout”, *Political Behavior* 22: 223-239.

Kenski, Kate 2005. “To I-Vote or Not to I-Vote? Opinions About Internet Voting from Arizona voters”, *Social Science Computer Review* 23: 293-303.

Kersting, Norbert og Harald Baldersheim (red., 2004): *Electronic Voting and Democrazy. A Comparative Analysis.* London: Palgrave MacMillan

Kitcat, Jason (2003): "The uncertain nature of elections to come". Response and analysis to the electoral Commission’s evaluation of the 2003 electoral pilot schemes and the Government’s own response to the evaluation. The free e-democracy project (www.free-project.org).

Kitcat, Jason (2004): ”Source availability and e-voting: an advocate recants”.*Communications of the ACM* Vol. 47, issue 10. ACM Press.

Laver, Michael (2004): ”Analysing Structures of Party preference in Electronic Voting Data” *Party Politics* 10:521-542

Liburd, Soyini (2004): *An N-version Electronic Voting System.* Caltech/MIT Voting Technology Project Working paper # 17
http://vote.caltech.edu/media/documents/wps/vtp_wp17.pdf

Lijphart, Arend 1997. “Unequal Participation: Democracy’s Unresolved Dilemma”, *American Political Science Review* 91: 1-14.

Magleby, David B. (1987): "Participation in Mail Ballot Elections", *Western Political Quarterly* 40: 79-91.

McLean, Iain (1989): *Democracy and New Technology.* Cambridge: Polity Press.

Morris, Dick (1999): *Vote.com.* Los Angeles: Renaissance Books.
The National Election Committee: *E-Voting System – Overview* http://www.vvk.ee/elektr/docs/Yldkirjeldus-eng.pdf

Newman, Terry (2003): "Tasmania and the Secret Ballot", *Australian Journal of Politics and History* 49: 93-101.

New York Times (2001): *36 days. The Complete Chronicle of the 2000 Presidential Election Crisis.* New York: Times Books.

Niemi, Richard G. og Paul S. Herrnson (2003): "Beyond the Butterfly: The Complexity of U.S. Ballots", *PS: Political Science & Politics* 36: 317-326.

NOU 2001:10 *Uten penn og blekk.*
http://odin.dep.no/fad/norsk/publ/utredninger/NOU/002001-020005/index-dok000-b-n-a.html

Norris, Pippa (2001): The Digital Divide. Cambridge: Cambridge University Press.

Norris, Pippa (2004a): "E-Voting as the Magic Ballot? The Impact of the Internet on Electoral Particiapation and Civic Engagement." Notat. Boston: John F. Kennedy School of Government, Harvard University.

Norris, Pippa (2004b): "Will New Technology Boost Turnout?" i Norbert Kersting and Harald Baldersheim (red.) *Electronic Voting and Democracy: A Comparative Analysis*, London: Palgrave Macmillan, 2005, 193-225.

Nygård, Beate (2003a): *Frie og rettferdige valg? En normative-empirisk analyse av de første direkte stortingsvalgene i Norge.* Hovedoppgave. Oslo: Institutt for statsvitenskap.

Nødtvedt, Einar (2002): Stemmegivning og informasjons- og kommunikasjonsteknologi. Vedlegg til Ot.prp.nr.45. Rapporten kan leses på
http://www.dep.no/krd/norsk/publ/otprp/016001-050016/ved002-bn.html

Olsson, Anders R (2001): E-röstning – En lägesrapport. Stockholm, IT Kommissionen, Rapport 35/2001.

Qvortrup, Matt 2005. "First past the Postman: Voting by Mail in Comparative Perspective", *The Political Quarterly* 76: 414-419.

Pratchett, Lawrence (2002): The Implementation of electronic voting in the UK. De Montfort University, University of Essex.

Reynolds, Andrew og Marco Steenbergen (2005): "How the world votes: The political consequences of ballot design, innovation and manipulation", *Electoral Studies* (under trykking).

Rumbaugh, James, Jacobson, Ivar & Booch, Grady (2004): *The unified modeling language reference manual* 2nd ed Boston : Addison-Wesley.

Rønning, Wenche M., Astrid M. Sølvberg og Christin Tønseth (2005): "Voksnes bruk av PC og Internet: Digitale skillelinjer er der fremdeles", *Samfunnsspeilet* (SSB) nr. 3/05 (pp. 21-28).

Røsland, Geir (2004): *Remote Electronic Voting*. Hovedoppgave. Universitetet i Bergen.

Saby, R.S. (1918): "Absent-Voting in Norway", *American Political Science Review* 12: 296-300.

Schartum, Dag Wiese og Lee A. Bygrave (2004): *Personvern i informasjonssamfunnet: en innføring i vern av personopplysninger*. Bergen: Fagbokforlaget.

Schneier, Bruce (2004): *Secrets and lies : digital security in a networked world*. Indianapolis, Ind., Wiley

Schorn, Heiner (2002): *Säkerhetskrav för internetröstning – en analys av skillnader mellan konception och realisering*, Human IT 1-2/2002, s.163-188.

Selker, Ted & Goler, Jonathan: *The SAVE System: Secure Architecture for Voting*

Shuki Bruck, David Jefferson & Ronald Rivest (2001): *A modular Voting Architecture ("frogs")* Caltech/MIT Voting Technology Project Working paper # 3. http://www.vote.caltech.edu/media/documents/wps/vtp_wp3.pdf

Southwell, Priscilla L. og Justin Burchett (1997):"Survey of Vote-by-Mail Senate Election in the State of Oregon", *PS: Political Science & Politics* 30: 53-57.

SOU 2004:111, Ny vallag.

Sturgis, Daniel (2005): "Is Voting a Private Matter?" *Journal of Social Philosophy* 36: 18-30.

Wand, Jonathan N, Kenneth W. Shotts, Jasjeet S. Sekhon, Walter R. Mebane, Michael C. Herron og Henry E. Brady (2001): "The Butterfly Did It: The Aberrant Vote for Buchanan in Palm Beach County, Florida", *American Political Science Review* 95: 793-810.

Watt, Bob (2002): "Human Rights and Remote Voting by Electronic Means". *Representation The Journal of Representative Democracy 39 (3).* London: The McDougall Trust.

Westholm, Hilmar (2002): "E-Democracy Goes Ahead. The Internet as a Tool for Improving Deliberative Policies?", i R. Traunmüller og K. Lenk, red. *Electronic Government. First International Conference, EGOV 2002.* Berlin: Springer.

Aall, Jørgen (2004): *Rettsstat og menneskerettigheter.* Bergen: Fagbokforlaget.

Aardal, Bernt (1997): «Valg». I: Øyvind Østerud, Kjell Goldmann & Mogens N. Pedersen, red., *Statsvitenskapelig leksikon*, s. 280-281. Oslo: Universitetsforlaget.

Aas, Patricia (2005): *Evaluating the suitability of EML 4.0 for the Norwegian Electoral System – a prototype approach.* Masteroppgave. Oslo: Universitetet i Oslo, Institutt for Informatikk http://wo.uio.no/as/WebObjects/theses.woa/wa/these?WORKID=28266

Standards

- NS 7799:2005: Styringssystem for informasjonssikkerhet, beskrivelse med veiledning for bruk.
- NS-ISO/IEC 17799:2005: Informasjonsteknologi, administrasjon av informasjonssikkerhet.
- ISO/IEC 27001:2005: Information technology -- Security techniques -- Information security management systems – Requirements.
- NS-ISO 17025: Akkreditering av prøvings- og kalibreringslaboratorier.
- ISO/IEC 15408-1:2005: Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model
- ISO/IEC 15408-2:2005: Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements
- ISO/IEC 15408-2:2005: Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements

Appendix A EC Recommendation (2004) 11

Pdf version on our web site:
http://odin.dep.no/filarkiv/261413/Rek-e-valg(2004)-engelsk-versjon.pdf

Appendix B Security challenges

1 General overview of potential threats

Electronic voting solutions for use in elections have undisputable advantages, such as wide availability, simple voting procedures and efficient counting of the votes. However, the electronic solutions also face a number of challenges. Seen from the perspective of free and secret voting and the principle of one voter - one vote, the following challenges are fundamental:

- Ensuring that the voter is provided with the means to cast his or her vote.
- Ensuring that the voter is prevented from casting more than one valid vote.
- Ensuring that the cast ballot is confidential in the sense of not being linked to the voter who cast it.
- Ensuring that the vote may not be changed or faked.
- Ensuring that votes are not lost.
- Ensuring that no votes are entered which have not been cast by a voter.

Related to each of the six challenges listed above, a number of central threats have been identified and linked to the following parts of the system:

- The voting client (client)
  - Virus
  - Programming errors
- Data transmission/network solution (transmission)
  - Lacking security in the network
  - Fake server (Man-in-the-Middle)
- Central servers (server)
  - Denial-of-Service
  - Insider attack on a server
  - Sabotage
  - Unauthorized votes
  - Errors in the server software
- General threats
  - Technical breakdown
  - Human error

The challenges and threats related to the system have been set up in the matrix on the next page. The threat considered most serious has been marked in each column by a capital X in bold. To give an example, a virus attack on the client machine will primarily have the effect that the voter's ballot is "stolen", but an additional effect may be that he voter misses his or her opportunity to vote, or that his or her vote is unveiled or deleted/not registered.

The present appendix gives a description of the different threats, and provides a sketch of possible ways to counter them.

Table 1: Threats matrix

	Threat	The voter is prevented from voting	More than one vote from a voter is validated	The voter's cast ballot is disclosed	The voter's cast ballot is lost	The voter's cast ballot is changed/faked	Fake votes
Client	"Virus" attack on client	x		x	x	**X**	
	Programming errors in the client	x			**X**		
Transmission	Lacking security in data transmission			**X**	x	x	
	Fake server (Man-in-the Middle)	x		x	x	**X**	
Server	Denial-of-Service (DOS)	**X**					
	Inside attack on server			x	x	x	**X**
	Data forgery		**X**		x	x	**X**
	Sabotage	**X**			x		
	Error in server software	x	x	x	**X**		
General	Technical breakdown	**X**			x		
	Human mistakes	x		x			

2 Threats directed at the voting client

Virus attack on the voting client

A system of voting over the Internet requires extensive use of standard computers and computer programs to function according to the objectives. Current basic software has turned out to be very vulnerable to fraudulent attacks. The number of such attacks has surged over the last couple of years. Many attacks have exploited weaknesses, or security loopholes, as they have been called, in the software. Information about such loopholes may spread very fast, and the suppliers very often are not the first to detect them. This also means that a malicious intruder very often knows how the different programs may be exploited

An attacker can exploit security loopholes in different ways, not only by creating viruses or worms to intrude upon the electronic voting processes. This type of activity may ruin the voter's confidence in the electronic voting system.

Attacks of this kind make up a serious and multifaceted body of risks, including the following threats directed at the client:

- General virus programs attacking the hard disk and threatening to stop the computer from running.
- Spyware, i.e. software monitoring the user's keystrokes.
- Trojan horses taking control of part of the computer and making it behave against the interests of the user and without the user's knowing about it.

New threats are discovered every day. Security loopholes in standard software will be a constant threat.

So far, there is no absolute way of securing against such attacks. A partial solution is to invite all involved parties to install security updates as soon as they are made available. If the opportunity is not taken to install security updates for a given loophole, - because, for example, the updates are not yet accessible – it might be an idea to change certain configuration settings, as that will help prevent the exploitation of the loophole in the given system, or at least reduce the harm.

One way to guarantee clean client machines would be to ensure that the computer is started on a special version of the operating system distributed on a CD-ROM. This solution is complicated and expensive, however, and will not be accessible to all voters. It places certain requirements on the voter's computers and assumes a certain competence which may exclude some voters from being ale to use it.

Programming errors on the client
All software may contain errors. Voting client software is no exception. In a security critical and time critical application such as an election, programming errors can cause the cast ballot to get lost, or prevent the voter from being able to cast his or her ballot. The way to prevent such risks, like in the use of any type of software, is to establish comprehensive, controlled tests.

3 Threats directed at vote receiving servers and other central computer resources.

Denial-of-Service – DoS/DDos
Denial-of-Service means that a service, except for planned downtime periods (for certain maintenance operations, for example), is unavailable for a longer period of time. Directed DoSs occur when thousands of computers (e.g. a so-called Botnet) simultaneously attack a server machine (the target) with a lot of traffic. The processing capacity of several web services is dimensioned for normal use only, which means that the services are not able to process the extreme amounts of information flooding in during such DoS attacks. In all probability, this type of overflow attacks will be more common and more sophisticated in the future, which implies that there is a pressing need for new and improved protection measures against such attacks.

Depending on its comprehensiveness, a DoS may cause the voting system to be partially or completely blocked during the whole operation or part of it. DoS attacks may have the effect that the voter is unable to cast his or her vote.

The problem may be solved in one of the following ways:

- Terminating the e-voting period before Election Day. This solution will always give the voters the opportunity to cast their votes in the polling station if the e-voting system is blocked.
- Planning for a traffic volume far beyond what is expected in an e-voting event.
- Updating the security mechanisms and following up the installation of security patches on the servers as well as the home computers, which may reduce the harm caused by viruses and worms.
- Securing potential weak points (single-points-of-failure) in the e-voting solutions by providing for a redundancy by back-up servers. An attacker may re-direct his attack to the other system, but only at the risk of being detected, which means that it is harder for the attacker to succeed.
- Establishing routines for moving the relevant web pages to other IP addresses in case of an attack.

Insider attack on server software
To run an election, the servers need specially designed software to handle certain functions during the election event. Fraudulent software installed on the servers by the experts, is considered a major threat in the literature. This type of malicious code is hard to detect and its consequences are potentially very serious in so far as it can cause a lot of votes to be changed, added or deleted.

In the opinion of the working committee, if specially designed software, products or systems have to be used in the operation, they must be approved by national or international certification standards. Certification ensures that the electronic voting system has been tested and satisfies the relevant codes, standards and/or directives (see chapter 9).

Data theft (hacking)
Data theft implies that an unauthorized party gets access to data resources. It may occur as the result of pure vandalism, a personal ambition or a wish to manipulate the election results. Although an electronic voting system is supposed to be updated and correctly configured, an attacker may exploit vulnerabilities that are unknown to the responsible authorities or weaknesses that have not been countered. Examples are unfortunate passwords, or malicious software downloaded on the voter's computer, such as for example viruses installing backdoors in infected computers.

Data theft has the primary effect that a voter submits more than one ballot. Moreover, the voter's ballot may be unveiled, deleted or, at worst, one or more cast ballots may be changed.

Different measures may be taken, but it is hardly possible to guarantee absolute security against this type of attack. The following measures are considered for reducing the potential for data theft in electronic elections:
- Performing regular vulnerability searches and regular checks on personal computers in order to detect potential security loopholes that may be exploited by intruders.
- Keeping informed about known software vulnerabilities and installing security updates for relevant software (*patching*).
- Monitoring and filtering traffic by means of intruder detection systems (IDS) for possibly unveiling theft attempts.
- Controlling the integrity of important configuration files and system files for possibly detecting unauthorized changes, indicating theft.

- Keeping electoral authorities and system authorities informed and knowledgeable about proper security procedures, such as, for example, guidelines in the selection of passwords and rules for installing and running the software.

Sabotage
Technical solutions are vulnerable to intended sabotage directed at central resources such as data stores and processors. The attacks may also be directed at the power supply and actual premises. Attacks of this sort may prevent voters from being able to cast their votes. They may also delete or manipulate cast ballots.

To secure the system against this type of threats, solutions providing physical security of the central modules must be established and a redundancy must be built into the solution to provide a back-up system in case any of the central modules fall out. The power supply should be secured by means of UPS solutions.

Server software errors
Just as for the client, the server may also contain unknown errors in the program code. At worst, such errors may put the whole election at risk, as a large number of votes may be lost. Programming errors on the server may also have the effect that the voter is not able to cast his or her ballot. Comprehensive, structured tests and code verification by inspection are possible means to reduce such threats.

4 Threats directed at the transmission of data

Security failure during transmission
Transmitting data over an open network such as the Internet implies a certain risk that others may get unauthorized access to the voter's ballot, and at worst delete or manipulate this ballot. Very strict encryption routines or security protocols (https, for example) may be used to prevent this type of threats.

Man in the Middle/Domain name system (DNS)
Fraud in the form of fake servers must also be taken into account. Some server may pretend to be the official server by tampering with the DNS or by using a name very similar to that of the official server (Man-in-the-Middle).

Faking the DNS may cause traffic to be misdirected, to the effect that the original ballot is deleted or replaced, or counterfeit ballots are faded in. Thus, it is important that the source of information in the DNS is correct. The problems with verifying who has registered DNS-information imply a certain risk of fake information registration in the DNS, for example that somebody pretends to be somebody else.

Another problem is that the voter may not be able to get access to the DNS if it is disturbed. Without a DNS a given network address can not be translated into IP addresses used by the Internet to direct the traffic to the right place. Abnormal load on the DNS, caused by repeated requests to the DNS by a malicious party, may prevent normal DNS services from being maintained, which in turn may prevent the voter from getting access to the e-voting system. (cf. section above on Denial-of Service).

To protect the system against Man-in-the-Middle attacks, a digital signature may be applied to the ballot to ensure verification of the voter submitting the ballot. However, it is of utmost importance that the confidentiality of the vote is not threatened.

Security solutions and return message solutions must be developed to prevent the possibility of attacks. One solution may be that the registration of a voter's ballot is confirmed through a different communication channel (SMS, Internet, digital TV), or the voter's voting card includes control information that enters into the dialogue between the voter's computer and the central vote receiving server, as in the solution chosen in Geneva.

5 General threats

Technical breakdown

Continuous access to IT systems and the Internet is all important for the success of electronic elections. This means that all the central components of the infrastructure must be robust and secure. Complete physical protection of the Internet, however, is unattainable, partly because of the complexity of the network structure and partly due to the costs related to the various security measures. Physical protection is here defined as all security measures directed at the physical components of the infrastructure, such as cable connections, radio equipment, connection points, central resources, etc.

The security level needed depends on the agreed level of acceptable risk and the relevant security norms. In furthering the work on security, the principle of security profitabilty will be very helpful.

Establishing an acceptable risk level is a comprehensive task since there are a number of resources (equipment, systems, information, staff, etc.) and information processing procedures that need protection. Sufficient security not only involves securing the production of a system. The system must be secured through every phase of its lifespan, from the design and development phase through the production phase to the disposal phase. For other resources too, security must be maintained through their lifespan

Efforts are continuously made to develop better solutions for physical security. In operating an e-voting system definite requirements must be stated for the Internet service providers (the ISPs), comprising among other things:

- The requirement of periodic risk assessment.
- The requirement of a continuous upgrading of the technology and procedures for ensuring an acceptable level of robustness against relevant threats.
- The requirement of documented contingency plans.
- The requirement of a certain redundancy in the infrastructure.

User ignorance

One of the greatest threats – and challenges – related to running an electronic election is the individual voter's failing awareness about IT security. Insufficiently secured personal computers may be kidnapped and exploited as platforms for overloading and virus attacks directed at the infrastructure used in the electronic election. Overloading attacks directed at critical parts of the infrastructure may have serious consequences for electronic elections. A central condition for e-voting, therefore, is that the voters take personal responsibility for the security of their own voting environment. The problem is, however, that the security

problems related to IT are highly complex and require thorough insight and understanding for the user to take the necessary security measures.

To enhance the security of voting over the Internet, voter awareness and voters' attitude to Internet security must be strengthened. Efforts to this effect are time consuming and require a lot of resources. One approach may be to run information campaigns before an election, providing the voters with information about the actual voting procedures, the security mechanisms built into the architecture, and the security measures to be taken by the individual voter before and during the elections. For the information to reach everybody, the materials sent the voters must have detailed, user-friendly descriptions and illustrations of the voting process.

People do not always behave logically and predictably, as is well known. Consequently, it is hard to predict and control their behaviour. The human factor relating to the voters as well as of the people building, running and maintaining the electronic voting system must be taken into account when the electronic voting system is designed and the rules and regulations for use are spelled out.

Theoretically, unintended eventualities may take place anywhere. This makes it difficult to establish alert systems and routines that can capture all such eventualities. It takes longer to discover unintended events than planned events, which means that the harm may be hard to repair. Moreover, emergency and contingency plans are normally developed on the basis of predicted events. This means that, on the whole, the voters have to take personal responsibility for the security of the system by complying with the rules and regulations provided for electronic voting. The higher the number of voters using the system, the higher the risk that someone breaks the rules, whether intentionally or by accident. The wider the application, the higher is the risk.

Appendix C and D

These appendices will not be translated into English.

Appendix E Terminology

Asymmetric encryption	Encryption based on a key pair. One key is used for encryption, the other for decryption. Normally one key is publicly known (“the public key”), while the other key is kept secret ("the private key").
Authentication	Mechanism to prove claimed identity, i.e. to know with certainty that a party is in fact the party it passes itself to be.
Authorization	A process by which permission is granted to use specified IT electronic resources.
Backup	Security copy
Biometrics	Used for authentication: Measuring a person’s physical properties/attributes (typical features of finger prints, colour of iris).
Firewall	A collection of components placed between to networks, the collection having the following properties: - All traffic from the inside to the outside, and vice versa, must pass through the firewall - Authorized traffic only, as defined in the local configuration, can pass through the firewall - As far as possible the firewall should is immune to intrusion.
User interface	The collection of aids used by humans (the users) to communicate with a given machine, physical unit or computer program (i.e. a system), typically a keyboard, mouse, screen, loudspeaker and screen image, and the effect of using these units in particular ways.
Buffer/overflow problems	That data are written into a memory outside the area designated for the purpose. May occur as the result of plain programming errors or by missing control of data entered into the program.
Data integrity	Security mechanism enabling the detection of unauthorized data changes or data changes caused by errors.
Digital signature	A data element attached to an electronic message or document, connecting the document to an individual, a machine or a data system. The signature allows the receiver to prove the origin of the received document and to detect forgery. The data element is generated by running a hash function on the document to be signed, followed by encryption by the signer’s private key. The security of a digital signature depends on the trust that the private key is known only by its legitimate owner.
Digital certificate	Electronic identification for the owner of a private and public key pair. The identification certifies the ownership of the public key.
Domain name system (DNS)	An Internet service translating URLs (e.g. www.odin.no) into IP addresses (such as 195.225.0.230).
Duplication	Copying often used to make several electronic copies of the data or to multiply transmissions of the same data over parallel channels.

EML	Election Markup Language, XML-based markup language used to format data for transmission among modules in an electronic voting system.
”Family voting”	A voting procedure in which one or more family members are unduly influenced by other family members.
Hacking	Slang expression for making small changes in computer programs. Often used negatively about changes made by unauthorized persons with devious intentions.
Hash algorithm	A mathematical function which generates bit patterns with a defined number of bits on the basis of a lot of data. A hash function always generates the same bit pattern for the same set of data.
White box testing	Testing a computer program system on the basis of reasoning and formal proofs**.** Requires access to the program code. It contrasts with black box testing, in which the functionality of the computer program system is only tested as observed from outside.
Non-denial (non-refusability)	Mechanism securing that the sender of an electronic message can not deny that he or she has performed the act of sending the message or refuse that the message has been sent by him or her.
Infrastructure	Basic structures and systems necessary for an organisation, a group of organisations or a nation to operate efficiently.
Integrity	Cf. data integrity
IP address	The address for a machine connected to the Internet, in the form of four numbers separated by dots, for example 195.225.0.230.
Client system	A system using the services of another system (called the server system).
Confidentiality	Securing that only authorized persons have access to a piece of information.
Encryption	To deform a text (or bit pattern) to make it illegible or incomprehensible, i.e. a chiffer text, which may only be decrypted by means of a decryption key.
Encryption key	A special bit pattern used as in-data for encryption and decryption programs.
”Man in the middle attack”	Attack by which somebody (the man in the middle) intrudes upon an electronic dialogue between A and B and pretends to be B towards A, and A towards B.
N-version system	Program system yielding high level security by processing the same data in parallel in n different sub-systems and comparing the results. If the results diverge, there must be an error. The system is a special kind of redundancy.
Optical scanner	Machinery which reads printed and written symbols and possibly bar codes, from paper and transforms this type of data to bit patterns.
Phishing	Attempts to tease users to disclose sensitive data by pretending to be a trustworthy organization or authority.
PKI (Public Key Infrastructure)	Public Key Infrastructure. A collection of security services, security modules and agents enabling large scale use of digital signatures.
Redundancy	Duplication of technical equipment, programs or data used to

	ensure security and control.
Auditability	Auditability relates to the ability to uncover events and actions and link them to defined subjects.
Secure Sockets Layer (SSL)	Protocol for authentication and encryption of network communication, first developed by Netscape. The most frequently used protocol for establishing secure network links over the Internet.
Smart card	A plastic card - the size of a credit card - with an embedded small computer (chip).
Traceability	A principle used in public administration to ensure that the treatment of a case may be reconstructed after the case is closed. It must be possible to trail the course of the case.
Voter credential	Proof of the voter's identity, i.e. that the voter is in fact the person he or she passes himself or herself to be.
Voting permission	Proof that the voter has the right to cast a vote in the relevant elections.
Symmetric encryption	Encryption in which the same encryption key is used for encryption and decryption.
Vulnerability	The vulnerability of a system is an expression of the weaknesses and faults in the system and special circumstances that increase the probability of threats in a security event (special circumstances may be size, complexity, the involvement of many agents, geographic distribution, frequent changes and site exposure).
Accessibility	Securing that a service satisfies given stability requirements that make relevant information accessible on demand.
"Denial of Service attack"	Attack against a website by flooding it with nonsense requests,, to prevent other users from getting in touch with the targeted service. The worst-case scenario is that the attacked website breaks down. Denial of Service attacks may involve several high capacity computers used simultaneously (or a network of computers)
Trojan Horses	Fraudulent software disguised as a legitimate program
Non-refusability	See non-denial
UPS	Uninterruptable Power Supply – equipment ensuring power supply maintenance even if normal power supply fails
Virus	Self-replicating fraudulent software spreading from computer to computer
VPN	Virtual Private Network – software enabling the establishment of secure data communication channels through a public, sometimes insecure, data network infrastructure such as the Internet.
"write-once"-medium	A medium for saving data in a way that prevents the data from being over-written or deleted.
XML	Extensible Markup Language. A standard way of coding electronic documents to make content elements and formats contained in the document recognizable.