E-voting handbook

Key steps in the implementation of e-enabled elections

Council of Europe Publishing

Acknowledgements

The author of this document is Susanne Caarls. However, it could not have been produced without contributions from a number of individuals and experts in the field of e-voting including: Michel Chevallier, Ardita Driza Maurer, Andreas Ehringfeld, Pierre Garrone, Ben Goldsmith, Robert Krimmer, Manuel Kripp, Henrik Nore, Michael Remmert, Patrick Trouveroy, Michel Warynski and Peter Wolf.

All Internet sources cited in the references were accessed in October 2010.

Directorate of Democratic Institutions
Directorate General of Democracy and Political Affairs
Council of Europe
Strasbourg
France
www.coe.int/democracy

Cover design and layout: Documents and Publications Production Department (SPDP), Council of Europe

Council of Europe Publishing
F-67075 Strasbourg Cedex
http://book.coe.int

ISBN 978-92-871-6948-8

Printed at the Council of Europe

Contents

Introduction

E-voting refers to an election or referendum that involves the use of electronic means in at least the casting of the vote. The introduction of e-voting raises some of the same challenges as are faced when applying electronics to any other subject, for example e-government. Politicians or administrators may perhaps expect that a paper version of a certain service or process can simply be taken and put on the Internet. Unfortunately, the reality is more complex, and nowhere more so than with e-voting.

There have been many developments in the application of e-voting since the Council of Europe Recommendation on legal, operational and technical standards for e-voting (Rec(2004)11) was adopted by the Committee of Ministers in 2004. Some countries no longer use e-voting; some have conducted pilot e-voting schemes and decided not to introduce it. At the same time, there are other countries which are continuing to conduct pilot schemes and introduce e-voting. It has been used in other elections, for example student councils or youth councils. There are also countries or organisations[1] which would like to launch pilot e-voting schemes but have not yet examined all the options. This document has been written with them in mind.

This document reflects the findings from several meetings at which the development of e-voting has been examined. These include the second review meeting on Recommendation Rec (2004)11 which took place in Madrid in 2008, and the sessions of the Forum for the Future of Democracy in 2008 and 2009.

This paper does not set out to argue either for or against the introduction of e-voting; it is designed to provide assistance and guidance to those who are considering introducing it.

1. The target groups of this document are governments and organisations wishing to know more about e-voting. Although specific reference is made to countries and governments, it should be noted that the same principles and advice apply to organisations responsible for elections other than governmental elections.

One of the central themes highlighted here is the issue of trust and confidence. Over the years, it has become clear that e-voting systems cannot be introduced unless citizens trust their political and administrative systems. Another important aspect to consider is that e-voting must not result in the exclusion of certain groups, for example the socially disadvantaged or people with disabilities. Furthermore, it takes time to develop a robust and secure system, and the necessary research and development time must be set aside before any e-voting system is actually introduced.

This document can be used as a stand-alone handbook, but governments or organisations would benefit most by consulting it in conjunction with the Council of Europe recommendation. Statements and recommendations already made in the recommendation are not repeated in this document. Users are also advised to consider the ongoing work of the Council of Europe in the field of e-voting, especially with regard to certification of e-voting systems and the transparency of e-enabled elections.[2]

The first chapter provides a brief account of the different kinds of electronic tools that can be used for e-voting or e-counting. Chapter two deals with the various aspects of e-voting which need to be carefully dealt with before conducting pilot schemes or experiments. The following chapters are structured in terms of the electoral cycle[3] developed by International IDEA in co-operation with the European Commission. The cycle comprises three main stages – the pre-electoral period (preparations), the electoral period (operations) and the post-electoral period (strategies) – and e-voting issues are discussed in that framework.

It should be noted that any reference to elections also includes referendums. Explanations can be found in Appendix I.

---

2. Information can be found on the website: www.coe.int. Also, a recently published study by IFES, "Direct Democracy: Progress and Pitfalls of Elections Technology" could be of interest.

3. www.aceproject.org/ace-en/focus/focus-on-effective-electoral-assistance/the-electoral-cycle-approach.

Chapter 1 – Different types of electronic tools

It is important to distinguish between the different types of electronic tools which can be used in elections.

– Direct Recording Electronic computers (DREs). These are machines or computers normally installed at a polling station, which record and simultaneously store the vote. This can be done using a touch screen (with or without a specific pen) or through a device which involves pressing one or more buttons.

– Voting via the Internet. This can be done in a controlled area like a polling station or in a non-controlled area such as a kiosk or the home.

– Optical and digital scanning devices which can be used in polling stations or in a designated counting area to scan ballot papers. These are normally used to improve the accuracy of the counting process and reduce potential manual counting errors. However, the quality of the count depends on the correct marking of the ballot paper and the quality of the ink used by the voter.

– At a polling station, use of one medium to record the vote, which is then registered in a ballot box on another device. This system differs substantially from a DRE in that nothing is stored in the DRE and it is impossible for a voter to manipulate the memory containing the vote.

It is important to examine the reasons for introducing e-voting in order to decide which type of electronic means best suits the purpose. Channel neutrality is also very important. The manner in which citizens cast their vote should not influence the content of their vote.

Before any decision is taken to introduce e-voting as part of the official electoral process, it is important to begin with feasibility studies in order to establish what one is trying to achieve. Moreover, e-voting systems must be thoroughly piloted and trialled before any introduction. Pilots or experiments can be conducted with a specific group of voters (those living or working abroad or students), in a specific area (a (part of a) town) or during specific elections (for example, local elections).

Chapter 2 – Points to consider before introducing e-voting

There are several major issues which need to be dealt with carefully before conducting pilot schemes or experiments or introducing e-voting. Aspects linked to the principles of free and fair elections, as well as general and technical points, need to be considered.

2.1. Principal points to consider

2.1.1. Voter verified paper audit trail

A paper trail can be added to voting computers in a polling station. A voter verified paper audit trail (VVPAT) can provide physical, unalterable evidence of how the voting computers interpreted each vote. This is done by showing the result to the voter on paper. Thus the voter casts his/her vote on the computer and a printed version of the vote is either shown to him/her behind a glass screen or given to the voter, who then puts the printed version of the vote in a ballot box. The problem with the latter option is that the printed version could disappear, accidentally or otherwise, and this could potentially lead to "vote selling" or to the need for the voter to show proof to another person of how he/she voted (family voting). This could lead to voters being coerced.

One of the reasons for introducing a paper trail is to enhance confidence in the system. The voter can check that the printed version matches his/her electronic vote. A further reason for introducing a paper trail is that it permits a manual recount if necessary. Before introducing this option, arrangements have to be made to deal with any discrepancy that may arise between the paper version and the electronic version. To whom can the voter complain if the paper version is different from the electronic version? What will happen to the election if his complaint is legitimate? What is the consequence if it is false (for example, a voter complaining out of mischief)? Furthermore, there must be a rule to stipulate which type of vote (electronic or paper) takes precedence if there is a discrepancy in the result. One argument for giving precedence to the electronic vote is that voters have cast their votes electronically. However, a counter-argument could be that the paper vote is preferable because it is "visible".

There are also people who argue that a paper trail will not work because voters rarely look at the printout and therefore do not check their votes. Others claim that it gives voters false confidence, since it shows a printout of the vote but provides no evidence that the computer actually stored the vote as cast. Moreover, this method could be difficult for people with disabilities to use because they might have difficulty in reading the paper version. Member states should also be aware that it is a costly system and a source of potential failure. For example, what should be done if the printer fails so that printouts of the votes become unavailable?

A paper trail should, therefore, be combined with a mandatory count of paper votes in a small, statistically meaningful number of randomly selected polling stations. However, it is important that polling station officials are not told in advance which polling stations will conduct the paper count. Any discrepancies between the paper and electronic results should be subject to further investigation.

The purpose of adding a paper trail is to give the voter the opportunity to verify his/her vote and leave open the opportunity for a manual recount. The paper trail is the most common example of this "software independent" medium for storing the vote. Another example is the storage of the vote as a PDF file on a smartcard. If it is needed, this PDF can be printed which would then allow for a paper ballot count.

2.1.2. End-to-end verification

A paper trail should not be added to the voting system in uncontrolled areas such as home voting, since this could lead to "vote selling". A solution to this problem might be end-to-end verification, a procedure which often uses cryptographic methods to create receipts enabling voters to verify *post facto* that their votes have not been altered, without revealing which candidates they voted for. The voter would then, for example, after casting his/her vote, receive a 23-digit number and use it after the election, via a website, to check that the vote has been counted.

Another possible solution is the "reversible vote", of which there are two types:

– The voter may vote via the Internet as many times as he/she wishes, but only the last vote cast will be counted.

– As above, with the added possibility of the voter going to a polling station (on election day). The vote cast at the polling station is the one which will be counted, since this is the only vote which can be guaranteed to have been cast in secret.

Estonia

Internet voting from home is possible for all elections. Estonian legislation gives voters the opportunity to cast their vote via the Internet from the 10th to the 4th day before election day. A voter may change his/her electronic vote during the advance voting period by casting another vote electronically or by voting at a polling station by paper.

Source: www.vvk.ee/internetvoting

The latter option presents a difference in voters' rights. Some voters have the right to revoke their votes, while those who vote on election day do not. A legal solution must be found for this specific situation.

These solutions should solve problems of family voting, because anyone who is being coerced should have several other possible ways of casting his/her vote in private or on election day at the polling station. However, there is no firm guarantee that these solutions will eliminate family voting when remote e-voting is used.

There are arguments for enabling the voter to check the content of the vote online, this being the only way in which a voter can be certain that his/her vote was counted and stored correctly. Although this would contribute to the transparency of the process and thereby reinforce confidence in the system, it can also encourage "vote selling", since the voter's choice may be disclosed to a third party. Another consideration is that this option does not exist in a paper election.

2.1.3. Family voting

Family voting refers to one family member deciding or influencing the voting choices of other family members. This situation is more likely to occur when a vote is not cast at a polling station, under official supervision and in private. Thus, in the case of remote voting in an uncontrolled environment such as Internet voting or postal voting, the secrecy of the ballot cannot be fully guaranteed.

In order to address the challenge this poses, there are two options.

– Before casting his/her vote, the voter could be asked certain personal questions such as his/her date of birth or mother's maiden name. Only if these questions were answered correctly would the vote be counted. In the event of incorrect answers, the voting process would continue but the vote would not be counted. The rightful voter, that is to say, the person who knows the correct answers, could then vote at another time in private.

– The introduction of multiple voting plus single vote counting might be envisaged. This reversible vote system has been discussed earlier in section 2.1.2. A voter could cast his vote via the Internet as many times as he/she wishes, and then go to the polling station on election day. The vote which would be counted is either the last vote cast via the Internet or the vote cast at the polling station.

In both cases there must be provision to ensure that the votes cast earlier are cancelled before the final vote is counted.

2.2. General points to consider

2.2.1. Confidence

In recent years it has become clear that an e-voting system can only be introduced if voters have confidence in their current electoral system. If it is trusted, voters are very likely to have confidence in new e-enabled elections. However, confidence should not be taken for granted and states need to do their utmost to ensure that it is preserved, all the more so as once trust and public confidence are eroded, they are exceedingly hard to restore. A trusted system gives scope for citizens and other stakeholders to ask critical questions.

Fostering transparent practices in member states is a key element in building public trust and confidence. Transparency about the e-voting system, the details of different electoral procedures and the reasons for introducing e-voting will contribute to voters' knowledge and understanding, thereby generating trust and confidence among the general public.

Although transparency, with documentation available to voters and other stakeholders, is important, it will not be possible for everybody to understand the e-voting system. If they are to have confidence in the electoral

process, some voters need to rely on others who are in a position to understand the equipment and the processes. It is therefore essential that domestic and international observers as well as the media have as much access as possible to relevant documents, meetings, activities, etc. Acting in a transparent manner towards these specific and important groups will boost public trust and confidence, because without transparency states cannot guarantee that an e-enabled election was conducted according to the democratic principles of free and fair elections.

Some people argue that the introduction of e-voting can also boost public confidence. However, building trust should never in itself be a reason for introducing e-voting.

2.2.2. Public debate

Before deciding to pilot or introduce e-voting, there should be sufficient public debate on the subject. This is also a good way of finding out what voters want with regard to elections. For example, are they in favour of Internet voting or would they prefer to keep the current system? A public debate can foster the electorate's confidence in the system and provides transparency to the decision-making process. However, if not handled well it may produce the opposite result. Political parties or other stakeholders may argue against it because they think they would stand to lose if e-voting did not engage their own voters.

One also has to be prepared to deal with unfounded allegations. People may claim that the system does not work, or that they can hack into it (or have already done so). "An attack does not have to be successful technologically to be successful publicly".[4] One has to decide in advance how to deal with untrue or unfounded statements.

2.2.3. Accessibility

E-voting can provide great opportunities for improving certain groups' access to the election process. The following groups could benefit:

– the visually impaired could use headphones connected to DREs and PCs if using Internet voting;

4. Statement by Andreas Ehringfeld, Vienna University of Technology, Research Group for Industrial Software, to the EVOTE2010 Conference in Bregenz, Austria, 21-24 July 2010.

– citizens who are not normally able to go to a polling station to cast their vote can now vote via the Internet from their own home;

– the use of electronic media can also facilitate the use of official minority languages, and this could lead to increasing involvement;

– military personnel overseas find it difficult to vote while on duty, so that e-voting might make it easier for them to participate in elections;

– citizens living and working abroad face some of the same challenges as military personnel, and so could similarly benefit from the introduction of e-voting.

E-voting should result in inclusion, never exclusion, of certain groups.

2.3. Technical points to consider

2.3.1. Open-source or proprietary software

Proprietary software is software which is licensed under exclusive legal rights held by its owner. The buyer acquires the right to use the software under certain conditions, but not for other purposes such as modification or further distribution. Open-source software has freely available source codes which can grant users the right to use, study, change, improve, expand and distribute the source code.[5]

An important decision when defining an e-voting strategy is whether to use open-source or proprietary software. This is especially relevant to the issue of confidence. Several e-voting companies use proprietary software, which has the disadvantage that in most cases the rights holder does not make the source code available to the general public (or makes it available only partially or temporarily). In some cases a few selected experts are given the possibility to review the source code. However, this is most likely to be governed by strict rules, for example non-disclosure agreements barring the electoral authority from revealing anything about the content of the source code, or its conclusions or recommendations. This is not a very transparent process and will, therefore, not contribute to building confidence.

5. More information can be found on: www.opensource.org.

One advantage of open-source software is that it can increase the confidence of the population and other parties involved in the e-voting system. This is reinforced by the fact that the suppliers are independent and there is no vendor lock-in. Furthermore, information security is increased because the source code is available to all, and the future stability of the chosen e-voting solutions is strengthened as the source code can also be supported by third parties. Moreover, licence fee costs are lower because open-source software is generally made available free of charge and the use of open standards often means that fewer problems of connection to other software are encountered. Proprietary systems also can, should and do use open standards like Election Markup Language (EML)[6] to increase interoperability, in conformity with whatever requirements are set.

A third option is for a proprietary source code to be owned by the government, which means that the government controls the source code and its distribution. This approach allows the government, independent bodies and citizens to examine the source code and to propose improvements if they wish. It is important, however, that governments refrain from using ownership of the source code as an excuse to restrict distribution to a select few or to not share it with others at all.

2.3.2. Identification and authentication of the voter

When e-voting is used at a polling station, the voter identification process can stay the same, but it can also change if an electronic voter register is used. In this case, arrangements need to be in place to ensure that the voter's identity cannot be linked to his/her vote (see 2.3.3). If biometric features have been used for the registration process (see 3.4.1), these same features can be used for voter authentication.

Internet voting from home[7] is different and a remote electronic identification system must be developed. Voters could authenticate themselves with an electronic ID card or, where no such system exists, authenticate themselves by using a combination of username and password with a control question

---

6. For more information see www.oasis-open.org.

7. Internet voting from home refers to the fact that voters can vote from anywhere and at any time – for example, from their workplace, from a hotel, from the office, etc.

(for example, date of birth). It is important to realise that without a physical token, voter authentication is less reliable and it is much easier to sell one's vote by disclosing username and password to a third person.

It should be noted that when voters have to make up their own username and/or password (for example, when registering to vote), they may forget or mislay the username and/or password. So a system needs to be set up to provide a new username and/or password at very short notice whilst at the same time ensuring that the voter can only vote once.

2.3.3. Removing the link between vote and voter

In order to respect the secrecy of the ballot as one of the main principles of democratic elections, it is important that at some point in the voting process the link between the identity of the voter and the vote itself is broken. This should preferably happen immediately after the voter has cast his/her vote. Since the vote and the voter must not be linked, it is important to establish a procedure governing who has access to the voting register and the voter registers (preferably managed by different authorities), when and under what circumstances they will have access, how long the registers will exist, and how and by whom they will be deleted. In the case of reversible voting (see paragraph 2.1.2), specific technical solutions must be put into place.

2.3.4. Design of the electronic ballot paper

Decisions have to be taken about the design and layout of the electronic ballot paper. There are two possibilities:

– the electronic ballot is exactly the same as the paper ballot;

– the electronic ballot has a different layout, for example because the paper ballots are too large and their design does not lend itself to computer use. In this case a two-stage approach may be necessary. The voter would first choose a party and then, on the next screen, vote for his/her chosen candidate. The need to scroll down the screen should be avoided, because it would jeopardise the equality of the candidates: those whose names are only visible when a voter scrolls down would be disadvantaged.

In particular in cases when electronic media are used alongside paper, one has to decide how to deal with any difference in design, since this could also have legal repercussions for the election.

Austria

For binding elections to the student bodies in 2009, the law provides in Article 43 HSWO that the electronic and paper ballot should both resemble as closely as possible the original template in the law. As e-voting was conducted in the week before the paper-based elections, a data entry error was found on the electronic ballot (one student party's name was not complete) which could only be corrected on the paper ballot. This problem can be overcome by certifying the e-ballot before the election starts.

Source: www.oeh-wahl.gv.at (in German only)

The introduction of new voting technology could also serve as an opportunity to improve the current design.

2.3.5. Confirmation of the vote

It is advisable to have the voter confirm his/her e-vote. The procedure would be as follows: first, the voter votes for a party, a candidate, indicates one or more preferences, casts a blank vote or votes yes or no in a referendum. Next, the voter receives an overview of all his/her votes and is asked to confirm his/her choices. If the voter is not satisfied with the overview, he/she should be able to return to the election or referendum options and change his/her vote. The voter would then receive a new overview. Once satisfied, he/she should confirm his/her choices.

Since this is an additional, new step in the election process, special attention should be paid to informing voters about this new procedure, as it has been found that it is not always clear. Furthermore, it should be noted that if the confirmation stage is not completed the voting process is potentially open to fraud, with polling station personnel tempted to "finish" the casting of the vote.

Finland

The Finnish Ministry of Justice conducted an experiment with DREs in three municipalities during the local elections on 26 October 2008. Owing to a usability issue, voting was prematurely aborted for 232 voters.

The system required voters to insert a smart card to identify themselves, type in their selected candidate number, then press "OK", check the candidate details on the screen, and then press "OK" again. Some voters did not press "OK" the second time, but instead removed for reasons unknown their smart card from the voting terminal prematurely, with the result that their votes were not recorded. On 9 April 2009 the Supreme Administrative Court ordered that new elections be held in the three pilot municipalities.

Source: www.vaalit.fi/electronicvoting

2.3.6. Voting period

Citizens are generally accustomed to an election held on a single day, but this may be extended if e-voting at polling stations is used. However, when introducing Internet voting from home, consideration may be given to extending the voting period from a few days to a few weeks. One advantage of this is to reduce demands on availability and capacity. Note, however, that interest in the electoral campaign may wane if a significant number of voters have already voted long before election day.

As regards the end of the Internet voting period, there are two options. Voting can end:

– one or two days before election day. This would give the organisers extra time to update the voter register if necessary;

– at the same time as voting at the polling station. This requires that an online voter register be in place.

Chapter 3 – Pre-electoral period (preparations)

3.1. Legal framework

3.1.1. Constitution

Generally, the constitution enshrines the main principles governing the rights of citizens in elections/referendums is already mentioned in the introduction, so we can delete it here. Suffrage must be universal, equal, free, direct and secret. E-voting is a particular method of voting and should not influence these general principles. However, when remote voting from home is introduced, for example via postal or Internet voting, namely, in an uncontrolled environment, there may be particular problems in guaranteeing the secrecy of the vote.

3.1.2. Legislation

The question arises whether a legal basis is required for pilots or experiments. In the case of a pilot scheme where the test results of the vote are not binding, there is probably no need to establish a legal basis. However, conducting such a voting experiment with official, binding results probably requires a change to the legislation. In any case, it would be useful at this stage of the testing to start preparing for a possible change in the electoral system, without fundamentally changing the democratic foundations.

In most countries, existing electoral law does not envisage e-voting therefore new legislation needs to be drafted. This new legislation could take three different forms:

– a temporary law permitting e-voting experiments;
– a change in the existing electoral law or in the implementation of existing legislation;
– a temporary law on e-voting followed by changes in the existing electoral law.

Reform of electoral law is a complex undertaking, and so it is imperative to begin this process as early as possible. In most cases, legislation permitting experiments with e-voting is subject to a specific time limit or is geared

to one or more specific elections (for example, experiments may only be conducted during local elections). The advantage of a temporary law is that existing electoral legislation does not have to be amended, which would probably take more time and thus slow down the process. In the case of a temporary law, it is important to ensure that the time frame set is sufficient to allow for the possibility of further experiments.

The process of reforming existing electoral law would in all likelihood take more time, as it would not simply entail the addition of an e-voting provision. The entire electoral law would have to be reviewed in order to see where and how the different components of e-voting could be incorporated.[8]

Experiments and pilot schemes on e-voting are carried out in order to provide input for any decision on its introduction. One legislative option would be to prepare preliminary temporary legislation and, while conducting the experiments, begin preparing the amendments to the existing legislation. The advantage of this combined approach is that no time is lost once a decision to introduce e-voting has been made. The disadvantage is that certain findings of the experiments could lead to changes in the text which has already been drafted.

Legislation on e-voting should be technically neutral and details should be set out in lower legislation in order to achieve a simple, swift process of change. Information and Communication Technology (ICT) is a fast-growing area, and no one wants to be tied down by outdated ICT specifications.

Other legislation which impinges on elections, such as criminal law, also needs to be examined, especially if a paper trail is to be introduced. New provisions will have to be included to deal with any legitimate or non-legitimate complaints of discrepancy between the paper and electronic versions.

3.1.3. Electoral systems and electoral districts

E-voting can be used in any electoral system: there are no exceptions. It may, however, be more efficient in one system than in another. One of the reasons for introducing e-voting is that it facilitates vote counting: it takes less time

8. To introduce an exception for e-voting, one has to verify the suitability of the legislation for each electronic component. The advantage of separate legislation lies in the possibility of dealing with a given component without having to examine the entire legislation a second time.

and fewer mistakes are made. However, when introducing e-voting in the more complex voting systems one also needs to bear user-friendliness in mind. It may make it easier to count votes, but casting the vote still has to be simple and straightforward. One also has to make sure that e-voting does not make electoral fraud more likely.

With regard to electoral districts, it is vital when conducting e-voting experiments or pilot schemes to make it plain that the aim is not to review or question electoral districts. It must be clear in e-voting experiments that no party or candidate is favoured or disadvantaged.

Special attention should be paid to the number of voters at each polling station, bearing in mind that e-voting for the first time can take longer for some groups of voters (for example the elderly) than traditional voting systems. Moreover, polling station staff may lack experience and could have trouble with the usability of voting computers.

3.1.4. Electoral management body

In countries where an electoral management body (EMB) is not responsible for the organisation of elections but has a different role, for example a more advisory role, it is important for it to remain involved. The EMB can play an essential part in generating confidence. For example, if the EMB states publicly that the e-voting system to be introduced has shortcomings, the whole process will be undermined. It is therefore also important that the EMB has the necessary technical expertise for it to understand all the technical aspects of e-voting.

The responsibilities of an EMB should be clearly defined in legislation. In some countries, an EMB is the body responsible for the overall organisation of elections, whilst in other countries it is responsible only for the conduct of elections. In many cases the EMB is responsible for declaring the final result. This means that it is also involved in the electoral process, and may thus use electronic means to perform its functions. An example might be the tabulation of the different results coming in from different polling stations or municipalities. Where the EMB uses electronic means in its own work, it must also ensure that the issue of confidence is addressed: the EMB needs to have the confidence of all the players, namely citizens, political parties, media and observers.

3.1.5. Codes of conduct

Drawing up codes of conduct is good practice, regardless of the means by which the vote is conducted. It facilitates the clear communication of expectations regarding the behaviour of all those involved in the voting process, and indicates possible sanctions if the standards are not respected. So with e-voting it is highly advisable to draw up codes of conduct for all concerned, including the technical designers, testers, software architects and other technical staff who would not be involved in a non e-enabled election. A code of conduct could be given official status by incorporating it in the e-voting legislation.

3.2. Planning and implementation

3.2.1. Budgeting, funding and financing

One of the major issues with e-voting is the financial aspect. E-voting requires investment, but can lead to savings in the long run. It is important to generating confidence that the financing of the project be fully open and transparent.

There are four possible ways of acquiring an e-voting system:

– designing and building an e-voting system of one's own;
– buying an e-voting system in order to obtain the intellectual property for that system;
– leasing an e-voting system, and thus leaving the intellectual property of the system with the proprietor;
– sharing or purchasing the user rights from a seller as mentioned in points 1 or 2.

The first option, designing an e-voting system, has the financial disadvantage of being expensive. The first e-voting experiment will be very costly, especially in terms of cost per voter, but the system should produce savings in the long run. The advantage of building an e-voting system is control over the product, which should increase citizens' confidence in the system. It also affords the option of using open-source or other software. Being in control of a system means less dependence on suppliers and prevents possible vendor lock-in. A tailor-made e-voting system will meet all the requirements and will best satisfy specific national and local needs.

The same advantages and disadvantages of designing a system are applicable, *mutatis mutandis,* to buying one.

In the short run, leasing a voting system from a supplier is likely to be less costly since the system will only be used for one election at a time. However, in the long run this option could be more expensive. One disadvantage of leasing a voting system is that it could be difficult to review the source code. Reviewers, hired by the government, will often have to sign a non-disclosure agreement for the review process and in most cases will not be permitted to disclose their own findings. It is important to spend sufficient time on review certification (minimum six months) and evaluation reports, as well as the results of source code inspection. A second disadvantage is that people are less likely to have confidence in the system if the vendor is not transparent.

When establishing a budget, it should be kept in mind that funding is not only required for the software and/or hardware but also for storage, testing, communication, evaluation, research, auditing and training (Total Cost of Ownership (TCO)). As this budget will be a recurrent one throughout the period when the e-voting system is in use, it must be a flexible budget which can adapt, for example, to changes in legislation which might place new demands on the e-voting system in use. It should also be clear from the outset who is responsible for which costs.

3.2.2. Election calendar

E-voting can be applied at any statutory, legal or administrative point in the electoral process. It requires a range of working methods (organising election work and training, for example), and consequently it will be important to decide whether and in what respect an election timetable needs to be modified. Also, internal timetables will need adjusting in order to help observe deadlines and respect time limits.

3.2.3. Recruitment

When starting an e-voting project, it is important to recruit a project management team. This team should ideally consist of the following:

- a project manager who will have overall responsibility for the project;
- a communications specialist who will be responsible for keeping local authorities, citizens, political parties, civil society, media and observers informed;
- a technical specialist responsible for all technical aspects of the e-voting system and for all contacts with the vendor;

- a security specialist responsible for all the security features;
- an implementation specialist responsible for conducting the experiment and/or implementation of the e-voting system;
- a training specialist responsible for developing and organising training activities for electoral bodies and citizens and for others if necessary;
- a legal expert responsible for all legal matters;
- a testing expert who is responsible for the testing of the technical components;
- a usability expert who is responsible for user-friendliness;
- an accessibility expert who is responsible for convenience and availability;
- a "devil's advocate" who should be able to suggest different views to the rest of the team and to propose various constructive solutions. One aspect of this work is to detect as many system faults as possible and pinpoint any potential for attacks. System faults must be sought in both unintentional misuse and in deliberate attacks for the purpose of undermining public confidence.

This project team could be set up at any governmental level. It is advisable to set aside a ring-fenced multi-year budget for the entire project in order to ensure that the project is independent of financial fluctuations.

It is also advisable to set up an advisory board. Participants could be members of political parties, academics, representatives of local, regional and/or national authorities, and representatives of civil society. It should also include representatives of organisations which do not favour e-voting, if they have a constructive approach. The role of the board would be to give general advice on specific aspects of the e-voting project.

The project team should also take into account that the implementation of an e-voting system calls for the recruitment of IT specialists to electoral bodies in order to ensure that they understand the system in use. Lastly, in the case of e-voting experiments, it is advisable to set up an evaluation commission consisting of experts in the relevant fields, for example a security expert, an electoral expert and a member of the local authority.

3.2.4. Procurement

Procurement of e-voting can include hardware and software for electoral administration, voter registration, voting, counting and tabulation. Before starting, it is important to decide what kind of contract is required and for

how long. Long-term planning is essential: how many elections are to be covered by this procurement and what happens when the procurement ends? What are the different scenarios? Planning ahead will save time and money in the future.

In order to ensure transparency and confidence, all parties involved in the tender need to follow general procurement procedures. In order to guarantee an open and competitive bidding process, an official call for tender should be organised. One way of ensuring transparency is to use Internet services such as live webcasting.

Norway

Norway is planning to conduct an experiment with home voting via Internet on the occasion of the local elections in 11 municipalities in 2011. The tender process used life webcasts in order to provide transparency over the whole process. Furthermore, an account of the workshop on observation of e-enabled elections which was co-organised with the Council of Europe can be found in the Norwegian multimedia archive.

Source: www.valg.no

In this process, the government does not bear sole responsibility: vendors are equally responsible. They should therefore do their utmost to be as transparent and reliable as possible and ensure that they comply with all existing local, regional, national and European recommendations.

United Kingdom

The United Kingdom conducted numerous experiments during local elections in England and Wales in the period 2002-07. DREs, kiosk voting, Internet voting, text messaging, electronic counting and postal voting were all experimented with. The Electoral Commission evaluated the experiments and advised in their evaluation report on the 2007 experiments that "sufficient time must be allocated for planning e-voting pilots. This should be approximately six months between the time the supplier contract is awarded and the elections."

Source: www.justice.gov.uk/publications/docs/gov-response-elec-comm.pdf

3.2.5. Logistics

The general logistics of e-voting concern equipment at polling stations, organisation of technical support services, communication issues and storage.

E-voting at a polling station

Once it has been decided to conduct an experiment or to introduce e-voting at polling stations, it is important to put a logistics plan into place. This plan should cover the following aspects with regard to voting.

– If computers are used: the number of computers required at each polling station and the equipment necessary to run them (cables, printers, etc.); how to prepare, distribute and install them; how to ascertain that the ballot box is empty; how to collect the computers after the election and how to store them between elections.

– Where to position the standby computers and standby technical personnel so that they can reach a polling station if required urgently.

– How to prepare computer activation keys for voters (or for polling station personnel); how to distribute these cards to the different polling stations; how to collect them after the election; how to delete them; and when and how to store them safely between elections.

– If a media device will be used to store the results of the election: how to transport this media device to the central tabulation point; how long and where to store the media device; and how and when to delete the contents.

– If the election results are to be printed at a polling station: how to transport the printed results to a central tabulation point; how long and where to store these results; and how and when to destroy it.

– If a paper trail is used: how to deal with the printed votes; in what circumstances and when to count them; how to transport them to a central tabulation point; where and for how long to store them; and how and when to destroy them.

– If paper ballot papers and a ballot box are used, as a backup: how many ballot papers and ballot boxes are needed in each polling station; how to prepare and print the ballots; how to distribute the ballot papers

and ballot boxes; when to use them; how to collect them after the election; how to transport them to a central tabulation point; where and for how long to store them; and how and when to destroy them. If paper ballots and electronic voting are used simultaneously, it has to be decided beforehand how to deal with any discrepancies which might arise between, for example, the total number of voters and total number of votes cast.

– If the Internet is used at a polling station: how to arrange the Internet link at each polling station; how to set up this link and how to ensure its safety; who will be responsible for setting it up; and what to do if the connection fails. For more information on Internet voting logistics, see below.

Special attention should to be paid to storing the voting computers between elections. For more information, see 3.2.6 Security.

Voting via the Internet from an uncontrolled environment

If voters are given the opportunity to vote from home, the following logistical aspects should be considered.

– If a voter is required to use a special tool to vote, such as a polling card with a certain code, disc, card or card reader: how many will be needed; how these are to be prepared; how they will be distributed; and how the voter should install them.

– Where to locate the main server and the standby server. It would pose a problem for some countries if servers were in another country. Servers could be located on Ministry of Defence premises or in a specially secured location.

– If voting from outside the country: not all websites can be viewed in every country because specific cryptographic tools do not always conform to national legislation. Also, certain countries can block the voting website. The latter situation is highly regrettable, but unfortunately nothing can be done about it.

– The system should not include a printing functionality and it should not display the voter's identity on the screen in order to prevent vote selling and undesirable pressure on the voter.

Kiosk voting

Some electoral authorities use public kiosks where citizens can cast their votes. These kiosks can be situated in various places – in the street, in town halls, in universities, etc. The same logistical aspects apply to kiosk voting as outlined at the beginning of this section. It should also be noted that outdoor kiosks must be weatherproof and tamper-proof. Generally speaking, constant supervision cannot be guaranteed and it is a prerequisite that the kiosk cannot be tampered with.

Polling station management

Technology can also be introduced to manage the polling station. Logistical aspects include the following points.

- If a voting machine is used: deciding on the number of voting machines required at each polling station; how to prepare, distribute and install them; how to collect them after the election; and how and when to store them between elections.
- If specific electronic cards are used for polling station personnel to identify themselves on a computer: deciding how to prepare these cards; how to distribute them; how to collect them after the election; and how and where to store them between elections.
- If a scanner is used to count ballot papers: deciding on the number of scanners required in each polling station; how to prepare, distribute and to install them; how to collect them after the election; and how and when to store them between elections.
- If connections need to be set up between the voting machine and the computers used by the polling station personnel: decide who will be responsible for these connections; the distribution of different equipment required; how to install and uninstall it; how to collect the equipment after the elections; and how to store it between elections. Wherever possible, wired connections are preferable because the possibility of intercepting data is greater with non-wired connections.
- If polling station personnel are required to use the Internet to perform their tasks: deciding how to arrange the Internet link at each polling station, how to set up this link; who will be responsible for setting it up; and what to do if the connection fails (for example, mobile telephones present at the polling station).

Risk management plan

For e-voting a risk management plan should also always be envisaged. This backup plan should include the action to be taken and the distribution of responsibilities in the following situations:

- when equipment is late or missing;
- when equipment breaks down;
- if the Internet connection fails;
- if access to the voting website or the voters register fails due to firewalls or other security measures;
- if there is a software error;
- if polling station personnel do not arrive;
- if there is a power failure;
- if there is a natural disaster or other emergency.

3.2.6. Security

Security is an essential part of e-voting. Not only are technical security and the security of data important, but so also is the security of procedures and personnel. For example, many things can go wrong if polling station officials are required to install software on a computer. In addition, threats due to viruses on computers of persons who vote from home are challenges which need to be considered. The legal aspects of security must also be considered, for example dealing with a hacking attempt on an Internet voting system from a country other than the one where the election is held.

This chapter deals with current security, and it is not possible to predict when, where and how these matters may change in the near future. It is therefore recommended that anyone envisaging e-voting make use of the information below, but also create their own risk model which can be applied throughout their project.

Security considerations vary between paper-based elections and electronic elections. For example, the latter entail many more technical security aspects. Electronic media call for strong safeguards against misconduct. Firewalls must be set up, votes must be encrypted and decrypted, any cyber-attacks must be countered, etc. It is important that a robust security system is in place at all levels. The paramount aim of secure procedures is to have

a system which can guarantee that all citizens who are entitled to vote can vote and that after the close of the election their vote is counted accurately.

With regard to the other aspects of the electoral system, procedures must also be put into place. Insider fraud is an example of a threat which needs to be dealt with: who will be authorised to carry out maintenance on the e-voting system during the election, and how many people should be allowed access to the system? Such interventions need to be laid down in protocols and submitted to the supervisory authorities. Rapid checks on accreditation of maintenance personnel are likewise important.

Security procedures should be put into place in respect of the persons authorised to perform particular tasks and ways of addressing the following situations:

- access to the security system of the e-voting system;
- authority and competence to modify system security;
- access to software;
- authority and competence to modify software;
- access to hardware;
- authority and competence to modify hardware;
- storage of software and hardware (location, duration, security arrangements);
- access to media devices (modification and storage);
- access to activation keys (modification and storage);
- distribution and collection of software, hardware or other election material;
- access to the server;
- testing the system;
- maintaining the system;
- counting votes;
- recounting votes;
- security checks on persons working on the e-voting system;
- authorisations and allocation of responsibilities regarding all above-mentioned issues.

Special attention must be paid to ensuring that voting computers are stored safely to prevent any kind of tampering. This applies to the computers between elections, but also during the period between configuration of the computers and the election day itself. One solution to this problem might be to install the software in an auditable way. This concerns not only the voting computers themselves but also those used on election day to receive, collate and compute Internet voting results. There have been a few cases where illicit access to voting computers has proved quite easy, which means there may be a risk of tampering with the software or hardware. Furthermore, some of the newest e-voting equipment also requires a climate-controlled environment.

Certification

The purpose of certification is to verify independently that an e-voting system complies with all the specifications and requirements established at the outset. Certification applies to hardware, software and operational issues. It is important that certification be carried out by a body independent of political parties, government and suppliers. It must be realised that the certification process takes a minimum of six months. It could even take a year or more if numerous adjustments have to be made.

Since certification is part of confidence building, it should be carried out in the most transparent way possible. Unfortunately, most certification processes take place behind closed doors, thereby producing the opposite effect and leading to mistrust and doubt. Finally, it should also be noted that certification needs to cover all aspects of e-voting, and this includes the people involved in all the processes and systems as well as the software and hardware.[9]

In some cases one may decide that an integral part of the certification cannot and must not be made public; this is in conformity with Recommendation Rec(2004)11 on legal, operational and technical standards on e-voting. An example would be all the particulars of security processes. In such cases full transparency will be hard to achieve.

---

9. *GGIS(2010)1 Report of the Meeting and Conclusions,* workshop on the certification of e-voting systems, Council of Europe (2009). More information can be found on the website: www.coe.int.

For more information on certification of e-voting systems, please refer to the work of the Council of Europe on this subject.[10]

Testing

An important part of the preparation for an e-enabled election is testing the software, hardware and processes. Sufficient time must be allocated to the testing phase; all too often delays in the development and building phases mean that there is no longer enough time for testing. Testing an e-voting system involves the following stages.[11]

– Acceptance testing
  This is a method of testing software that tests the functionality of an application performed on a system (for example software, batches of manufactured mechanical parts, or batches of chemical products) prior to its delivery.
– Performance testing
  This test is used to determine the speed or effectiveness of a computer, network, software programme or device. This process can involve quantitative tests done in a laboratory, such as measuring the response time or the number of MIPS (millions of instructions per second) at which a system functions. Qualitative attributes such as reliability, scalability and interoperability may also be evaluated. Performance testing is often done in conjunction with stress testing.
– Stress testing
  This is a form of testing used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often to breaking point, in order to observe the results. Stress testing may have a more specific meaning in certain industries, such as fatigue testing for materials.
– Security testing
  This is a process to determine that an information system protects data and maintains functionality as intended. The six basic security concepts that need to be covered by security testing are: confidentiality, integrity, authentication, authorisation, availability and non-repudiation.

---

10. www.coe.int.

11. For more detailed explanations please refer to www.wikipedia.org.

– Usability testing
  This is a technique used to evaluate a product by testing it on users. This can be seen as an irreplaceable usability practice, since it gives direct input on how real users use the system.
– Review of the source code
  This is a systematic examination of the computer source code intended to find and rectify mistakes overlooked in the initial development phase, improving both the overall quality of the software and the developers' skills.

Ideally, a small test election should be conducted before the real election, thereby providing feedback on the process from potential voters and the election commission. It is also advisable to invite representatives of civil society to participate in such tests. During this test phase, potential voters should be invited to test the system as it would be used in the real election.

3.3. Training and education

3.3.1. Operational training for election officials

All election officials should receive training on the e-voting system, whether for a pilot scheme or an experiment or when introducing e-voting. During such training sessions, all election officials should be able to practise working with the system and experiment with it. This will give them a better idea of how it works and will also enable them to answer questions about the system.

Before selecting people to participate in the election as election officials, the level of ICT knowledge they possess needs to be established. It is advisable that at least one polling station official has the required knowledge of ICT. It is also important that officials in other phases of the election process (for example, members of the EMB) have the required level of ICT knowledge or, if not, that they receive appropriate training.

3.3.2. Civic education

Civic education deals with the continuous development of civil society. It aims to educate citizens in the knowledge and skills they require to participate in the community, government and politics. This concept is therefore very broad and does not specifically apply to e-voting. This topic will not therefore be discussed further in this document.

3.3.3. Voter information and training

E-voting has an impact on how, when and where people vote and it is therefore essential that sufficient time and funding be allocated to extensive voter education. This is a very important aspect to achieving the confidence of citizens, political parties, academics and representatives of civil society. Wherever possible, use should be made of social networking sites like Facebook and YouTube, because these forms of media have the potential to inform a large group of people at once, especially the young.[12]

This being a quite new method of voting, citizens should be able to practise e-voting. For example, a test version should be available before and during the election on the voting district website. Special attention should be paid to the elderly and other groups of people who may not be familiar with modern technologies and the Internet.

It is also important to set up an information desk, either at national or local/regional level, where citizens can ask questions about the method of voting, security, what to do if they have lost their access codes or polling cards, etc. Ideally this desk should be staffed 24 hours a day during the election period, especially for voters who are voting from abroad, if applicable.

When an e-voting experiment is conducted or e-voting is introduced only for a specific group of people (for example, voters living abroad), targeted voter education will be required. Examples of voter education materials include brochures with graphics, a website, videos, banners and posters. All the information should be available in at least all official languages.

Canton of Geneva, Switzerland

Since 7 January 2003 it has been possible for citizens of selected municipalities to cast their votes via the Internet from home. In order to provide the population with all the information it needs, a specific website has been designed where voters can find information about e-voting and also try it out. This online demo is a good way to test the system.

Source: www.geneve.ch/evoting/english/welcome.asp (at the bottom of the page)

12. For more information on the use of social media in democracy please see the Council of Europe recommendation on electronic democracy (e-democracy). Recommendation CM/Rec(2009)1.

3.4. Registration and nominations

3.4.1. Voter registration

ICT can be used in the registration system, irrespective of whether a country uses a periodic list, a continuous register or the civil register. It can be applied in gathering, recording, storing, filing and printing voter information. Registration can also be effected by the voters themselves, for example via the Internet. It is important to ensure that the system complies with the guiding principles of voter registration. An electronic register must not lead to the disenfranchisement of voters.

Biometric systems have also been used in voter registration because they could reduce voter impersonation and multi-voting practices. Before deciding on using biometric features, one has to consider the cost and time aspects. It takes time and a large budget to register all eligible voters by biometric means.

When using ICT in connection with the voting register, the following aspects should be taken into account.

– Making the preliminary voter list available to the public: this can be done via the Internet, but a paper version of the register should also be available, for example at the town hall. Citizens should be able to contact the organisation responsible for the register in person, by mail, via the Internet and by telephone.

– A procedure must be set up to allow changes to the voter register and guidelines drawn up to identify how and when this should happen. This could be the case when citizens discover incorrect information or if persons have to be added to or removed from the list.

– It is in the best interests of some citizens not to have their personal information publicly posted on the voter register. Therefore, a procedure of the kind prescribed in data protection laws must be put into place to protect those who need this.

– If early voting is applicable, a procedure should be put into place for deleting the names of those who have already voted. Clarification is needed on who is entitled to amend the register and when this should happen.

- How will the final voting register be produced and distributed to each polling station? An encrypted electronic version of the register could be sent via the Internet or downloaded on to a laptop and thus distributed to the different polling stations. Alternatively, a media device could be produced and distributed and then installed on the computer in the polling station. The latter option could result in complications if polling station personnel are unable to upload the software. More information can be found under 3.2.5 Logistics/Polling station management.
- An online register accessible from the polling station via the Internet could be used. Special attention should be paid to the availability and accessibility of the system. It should be available throughout the entire election period. Questions of access to the register should be made clear – in particular, who has access, when and how will the software needed for access be installed? More information can be found under 3.2.5 Logistics/Polling station management.
- If legally required, an audit trail can be used to justify any changes or decisions made by electoral officials to the electronic voter list, if changes are allowed to be made.
- A backup plan must be drawn up. This plan should address any problems which might arise with the electronic voting register, including a malfunction in the system, problems with distribution and problems with the audit trail.
- As regards an electronic register at the polling station in particular, polling station personnel should be trained to work with the new technology. Other election officials who work on electoral registration will also need to be trained.

Online registration

More and more countries which allow voters to self-register (for example, voters who live abroad) are considering an online registration system. The most difficult aspect of such a system is identification. With paper registration, citizens sign the application form and provide a photocopy of their passport. With electronic registration, the equivalent would be for the citizen to use an electronic signature. However, a national electronic signature system for people who live abroad is not always available. An alternative could be for citizens to create their own electronic signature when registering online. This could be done by asking citizens for a secret code which they create themselves. This secret code could then also be used in the

voting process later on. Of course this still does not address the issue of proving eligibility to vote. If e-government is well developed in a country, eligibility can be checked online during the process. If no such system is in place, voters could be asked to upload a copy of their passport or ID card. Unfortunately, this still means there is no real check as to who was uploading or registering. It might for example be very easy to register using the identity of another person.

Polling cards

Changes may also need to be made to the polling card where one is used. When e-voting at a polling station is used, the polling card can be the same as with paper-based elections. With Internet voting, however, the polling card could also provide additional information. It could, for example, contain a code (whether concealed or not) which is required when voting via the Internet. If such a code is used, it is important to install the necessary security features on the polling card to protect it and make tampering impossible. In these circumstances it is also advisable to send the polling card to the voter in an envelope. One has also to decide whether to distribute a new polling card to the voter for each election or to use a more permanent card.

3.4.2. Observer accreditation

The accreditation of observers or the organisations they work for is not affected by the introduction of e-voting, and therefore this issue is not developed further here. However, in the case of e-voting, major changes in the manner of observation are required because it is more difficult to observe all aspects of the process than with a paper-based election.

The leading body of experts in the field of election observation is the Office for Democratic Institutions and Human Rights (ODIHR) of the Organization for Security and Co-operation in Europe (OSCE). In October 2008, ODIHR published a discussion paper on the preparation of guidelines for the observation of electronic voting.[13] This paper identifies several aspects to be considered when observing e-voting:

– the background to the decision to use e-voting and the comparison with the system being replaced;

13. www.osce.org/documents/odihr/2008/10/34647_en.pdf.

– legal frameworks;
– how the particular e-voting system was chosen;
– the certification and testing of the system;
– the secrecy of the ballot;
– the security of the entire system and its functioning;
– voter accessibility and education;
– the analysis of documentation relevant to the system;
– election administration and training of polling station officials;
– overall transparency and public confidence;
– audits of the system;
– recounts and challenges to the result.

Observers could also decide to observe the voting register. It is wise to involve observers as early as possible in the process, as the sooner they are involved the better they can carry out their task. Observation is a way of building trust and is therefore crucially important to the successful implementation of any e-voting strategy. More detailed information on observing e-voting can be found in the discussion paper.

3.4.3. Parties and candidates

E-voting does not have any impact on parties and/or candidates. ICT could, however, be used in the registration process of parties or candidates. The advantage of this is that fewer mistakes will be made when constructing the whole ballot and the process will be quicker. A precondition for this to work is that those involved in the registration process (political parties, candidates or the EMB) have a certain level of ICT knowledge.

3.5. Election campaign

When a voter is voting, he/she should not be interrupted by any campaign activity on the part of any political party. In the case of voting via the Internet, a voter should be able to make his/her choice unperturbed. The secure voting website must not be open to campaigning, although information about the different parties and relevant issues could be published on the

main website (namely, before the voter accesses the secure voting area). In this way the voter, if he/she so wishes, could acquire information about the views of the different parties and make his/her choice accordingly.

The use of e-voting has no effect on other parts of the electoral campaign and the subject of e-campaigning is beyond the scope of this document.

Chapter 4 – Electoral period (operations)

4.1. Voting operations and election day

4.1.1. Pre-voting period

Different operational tasks will have to be performed before the election can start. These include:

– sealing the software;

– opening the voter register;

– releasing the voting website (if applicable);

– opening the election;

– opening the electronic ballot box.

4.1.2. Voting period

If e-voting and a paper ballot are used at the same time and for the same election, the following will have to be decided before the start of the voting period.

– Will the voting period for each channel be the same?

– If not, when does the voting period of one channel open and close and when do the voting periods of the other channels(s) open and close?

– How is (are) the voting period(s) to be announced to the general public?

It is important that the counting of ballots does not start before all channels have been closed. Read more in 2.3.6 Voting period.

4.1.3. Post-voting period

Several operational tasks will have to be performed at the close of the election, before counting can start:

– the close of the election;

– the close of the voter register;
– the close of the electronic ballot box;
– the decryption of the votes.

4.1.4. Special and external voting

Special voting

E-voting, more easily than paper ballot voting, can assist physically disabled people to cast their vote independently. Voting computers at polling stations can be equipped with special apparatus so that, for example, visually impaired people can hear the ballot paper through a headset and also check if their vote is cast as desired. It should be clear which polling station official is responsible for assisting voters.

Internet voting from home can also have such advantages. People who have difficulty in getting to a polling station (and thus cannot vote or have to proxy somebody to vote for them) can vote independently via the Internet. Also the visually impaired could hear the ballot papers through a headphone and vote from home using their PCs.

When designing an e-voting system, it is desirable to involve a national organisation with experience in improving access for disabled people to advise on such matters. This organisation could be represented, for example, on the advisory board.

Voting from abroad

Currently, voting via the Internet is considered a good way to facilitate access to the polls for voters living abroad. The advantages of such a system for overseas voters are that it is simple and fast. In most countries, voters who live abroad are obliged to vote at an embassy or consulate in their country of residence (some voters having to travel a long way) or else they can send a postal vote. Among the disadvantages of postal voting versus Internet voting is that postal voting has long time frames, which are needed to mail out ballot papers and receive them back, especially when the election timetable is tight. Secondly, the reliability, speed and secrecy of the postal system vary greatly from country to country. Finally, Internet voting can be designed to prevent family voting/vote selling more effectively than postal voting.

The Netherlands

The Netherlands has conducted two e-voting experiments for voters living and/or working abroad on election day in order to facilitate the casting of their vote. The first experiment was held during the European Parliament elections in June 2004, and voters had the option of voting via telephone or Internet (as well as using the usual method of postal voting). 7 195 out of 15 832 registered voters used the Internet and telephone to cast their vote.

In November 2006 a second experiment was conducted. Voters living and working abroad on election day could cast their vote for the national parliament elections via the Internet (as well as using the usual method of postal voting). This time 19 815 of 34 305 registered voters cast their vote through electronic means.

As the result of controversy about the use of electronic voting machines at polling stations, no further action was taken.

Source: www.rijksoverheid.nl (Dutch only)

However, it should be borne in mind that a country's legislation may require a separate polling station to be set up for Internet voting for a specific group. If there is, for example, a polling station for "voters from abroad", that polling station will have to fulfil all the requirements of a regular polling station.

Voters resident abroad frequently have to register, and this procedure is often very lengthy. It is advisable to bear the registration process in mind when considering e-voting for voters living abroad. It can be contradictory for voters to register by paper and receive documentation by post and then vote via the Internet. Using ICT in the registration process will not only assist voters, but will also assist the organisation responsible for the registration of voters abroad because it will be less time-consuming and less prone to error. However, e-voting and electronic registration should not be made dependent on each other and should therefore be separate approaches.

4.2. Vote counting

The exact time of the close of the vote must be unambiguous, especially when dealing with a combination of different types of voting, including

Internet voting from abroad and e-voting at polling stations. Counting should not begin if one type of voting is still taking place. However, counting should start as soon as possible after the close of the polls.

There are several ways to determine the results of an election. When direct recording devices are used, the result can be counted at the polling station (for example by printing the results). Electoral law may require the count (also) to take place at a central local point (such as a town hall). This means that the electronic device holding the content (the votes) has to be transported to this location. Votes cast using the Internet need to be counted at a central office.

Counting at a polling station

Counting e-votes at a polling station is normally a simple process on a voting computer, the results then being known immediately. The results can be printed out and stored on a separate media device. It is imperative that these procedures are made known and written down in a clear and transparent manner in order to generate confidence. The relevant instructions should be publicly accessible.

After the result at a polling station is known, there must be safe procedures for transporting the results to the central polling station. When both a printed version and an electronic version of the results are available, it is advisable to transport them separately.

The results could also be transported via an (encrypted) Internet line or something of the kind. This line needs to be secure and protected from tampering. It is also advisable in this situation to use another means of transport for a second version of the results. A time limit within which a poll official is obliged to transport the results to a central place should be set, in order to prevent tampering with the results. And in all cases it is important to provide a mode of return transport to the central office.

Counting at a central local point

When votes are counted at a central local point, precautions should be taken with regard to the transfer of votes from different polling stations to this point. There are three different vote transfer scenarios.

– Where votes have been cast by paper ballot, the ballot papers will have to be physically transported to the central point where they can, for example, be scanned.

– When e-voting is used the results are printed out and then transferred, preferably in a secure envelope. The votes can (also) be stored on a media device. These media devices will be physically transferred.

– With e-voting, where votes are electronically transmitted, for example via the Internet, to a central point, a vote can be transferred to a central electronic ballot box immediately after it is cast. Alternatively, the vote can be stored at the polling station and transferred at the end of election day.

Precautions must be taken to prevent the loss of votes, alterations, failures, breakdowns, and combinations of all these which may lead to discrepancies. It is important to define which votes are used for the official count.

Recounting

As for all elections, the electoral process must allow for recounts. It is imperative that this is done in the most transparent way possible. Recounts should be used for the right reasons and not, for example, to solve problems of confidence.

Before any election, the recount procedure should be clarified.

– Under what circumstances will a recount be called for?

– Who will be responsible for the recount?

– Who will conduct the recount?

– Who will be present?

– What if the outcome of the recount is different? Which result prevails – the first or second (and, in some cases, the electronic vote or the paper vote)?

– How will the results of the recount be announced to the public?

Electronic votes can be recounted by:

- reprinting the results per voting computer;
- reproducing a new media device per voting computer with the results;
- inserting the media device which contains the results from one polling station into another computer with different software;
- resending the results from the polling station to the central tabulation point;
- inserting the media device which contains the results of the Internet votes into another computer with different software;
- in the case of a paper trail, counting the paper votes. If the paper count yields a different result, it must be clear which count prevails over the other;
- taking all the votes in the electronic ballot box and counting again on a new computer.

Cook County, Illinois, United States

Cook County uses two voting systems: paper ballots which are read by optical scanners and a touch screen DRE. 5% of the election day precincts are randomly chosen by the state board of elections for a recount after the election. Which precincts will be recounted is announced the day after the election. A losing candidate has the option of asking for a "discovery recount" of 25% of the precincts in his district. The candidate chooses the precincts to be recounted.

Source:
www.cookcountyclerk.com/elections/2010elections/Pages/DiscoveryRecountsElectionContests.aspx

4.3. Tabulation of results

4.3.1. Tabulation of results

Tabulation of the polling station results can be transmitted electronically[14] to the main tabulation centre. The main tabulation centre can use certain software to tabulate all results. It is important that this system is as transparent

14. This covers transmissions via the (public) Internet, private communication networks, phone connections, GSM connections, etc.

and reliable as e-voting. Indeed, much of what has been said throughout this document (for example, regarding transparency and confidence) also applies to the tabulation of results.

4.3.2. Complaints and appeals

The existence of a robust election complaints and appeals system is vitally important. Citizens, political parties and other organisations should have the right to file an appeal or complaint (either in writing or by telephone). E-voting should not have any effect on the existing complaints and appeals system, although electronic means could provide an additional way of registering a complaint which could be filed via the Internet. Furthermore, a list of all complaints could be published on the Internet.

4.3.3. Official results

Every country has its own way of presenting the official results of an election, and e-voting would not normally have an effect on the way the final results are presented. Election results could also be made available via the Internet.

Chapter 5 – Post-electoral period (strategies)

5.1. Post-electoral period

5.1.1. Audits and evaluation

Audits

Audit trails play an important role within electoral processes, and become particularly sensitive and controversial if the overall integrity of the electoral system is a topic of public debate. An audit trail needs to be established for all aspects of the systems used in the election so that all changes and decisions can be explained and defended.

Audits can be carried out by all parties involved. At least one independent body should be responsible for an independent overall audit. It is important that audit information is available in a human readable form.

One part of the audit process of an e-voting system is to verify that the systems used for the election were indeed based on the source code that was certified before the election. Other parts of the audit process of the e-voting system include review of other documentation, for example the functional and technical system design. It is important to audit every part of the e-voting process, including the electoral voter register (if this is used), compilation of the electoral voter register, voting, counting, archiving and destruction of votes.

Evaluation

Two evaluations need to be carried out, one of the election itself and one of the project. It is advisable to evaluate the following elements of the election:

– the citizens (voters and non-voters);

– the polling station officials (training, experience, etc.);

– the help desk;

– the information campaigns;

– the internal systems: the project itself and processes within the project;

– the registration procedure, if applicable.

Different statistical material should be collected, for example, the number of voters in this election and previous elections, the number of voters who chose to use e-voting, errors/problems and so on.

With regard to the project, it is important that conclusions can be drawn for the benefit of future pilot schemes, experiments and/or the implementation of e-voting. All the information used to evaluate the election should also be used in the evaluation of the project. Further, an independent body should be set up with responsibility for the organisation and outcome of the evaluation. It should be clear from the beginning who will be responsible and which explicit goals have been set. Again, it is important to undertake the evaluation in the most transparent way possible and inform the public of the outcomes. In this way, the evaluation is also an instrument for fostering trust and confidence in the electoral system.

5.1.2. Archiving and research

Archiving

The method of archiving e-votes, where applicable, should be decided before the election. With regard to e-voting computers at polling stations, this will include deciding whether, and if so for how long, the votes cast should be stored on the computer. Such votes need to be kept available for a certain time in case of a recount. Secondly, it has to be determined who will be responsible for deleting votes on the computer, who will carry this out and how and when they will be deleted.

It should also be decided whether the electronic votes need to be stored electronically for a longer period of time. Issues to be addressed include:

– do the votes need to be stored?

– how will they be stored?

– who will be responsible for the storage?

– how to ensure the security of the archived data?

– how long do they need to be stored?

– where will they be stored?

– who will be responsible for the destruction of the votes after the storage period has elapsed, and how will this be done?

Where a paper trail has been used, the same considerations as mentioned above with regard to paper ballots will apply.

Research

Research on elections is an important factor in improving electoral processes, in particular when examining e-voting, where it can provide much valuable information on the e-voting process. Research can reveal whether citizens would like to use e-voting or not, what they see as the advantages and disadvantages and, most importantly, whether they feel they can trust the system.

5.1.3. Voter register update

Some counties have a separate voter register; other countries use their civil register and base their voter list on this register or use voter lists which are based on specific population registers. In most cases a voter register can then be created within a few days. Whether an electronic system or a paper voter registration system is used for the voter list or the population register, it is always important to keep it up to date.

5.1.4. Legal reform

E-voting experiments and pilots could ultimately lead to electoral reform. Over-frequent reform of electoral legislation should be avoided, as it could be confusing for electoral officials, citizens and political parties.

It should be kept in mind that experiments and pilots on electoral procedures create expectations which need to be taken into account. For example, if people have been able to use the Internet in a number of experiments, expectations will have been raised that electoral reform is imminent and these expectations will have to be handled carefully.

5.1.5. Institutional strengthening and professional development

E-voting pilots or experiments also entail training all the people involved, including voters, polling station officials, civil servants and political parties. It is important that these skills are not lost once the test period is over. Ideally, the same group of people should be involved in subsequent pilots or experiments, thereby building up a nucleus of professional and experienced staff.

Knowledge can also be turned to good account by sharing the results of different pilots and experiments with other countries. Such a range of experience provides a wealth of practical information, knowledge and inputs. The Council of Europe offers a European forum for this purpose.

Appendix I – Glossary of terms

This document uses a number of e-voting keywords. The table below offers explanations of these terms as used for our present purposes. They are not to be considered as definitions:[15]

Accessibility	The degree to which a product, device, service, or environment is accessible by as many people as possible.
Activation key	An electronic card which can be used to activate a ballot paper on a voting computer.
Auditing	An independent evaluation of a person, organisation, system, process, entity, project or product which includes quantitative and qualitative analysis
Authentication	The confirmation of the alleged identity of a person or of data.
Ballot	The legally recognised means by which the voter can express his/her choice of voting option.
Candidate	A voting option consisting of a person and/or group of persons and/or a political party.
Casting of the vote	Entering the vote in the ballot box.
Certification	The process of confirmation that an e-voting system is in compliance with prescribed requirements and standards and that it at least includes provisions to ascertain the correct functioning of the system. This can be done through measures ranging from testing and auditing through to formal certification. The end result is a report and/or a certificate.

15. Most of these definitions derive from the Council of Europe Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting: www.coe.int. For other explanations please refer to www.wikipedia.org.

Decryption	The process of making encrypted information readable (that is, unencrypted).
E-election or e-referendum	A political election or referendum in which electronic media are used at one or more stages.
Electronic ballot box	The electronic medium by which the votes are stored pending the count.
Electronic ID card	An official electronic proof of identity, making it possible to sign electronic documents with a legal signature.
Encryption	The process of transforming information (referred to as plain text) using an algorithm (a "cipher") and thus render it unreadable to anyone not possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as "ciphertext").
E-voting	An e-election or e-referendum involving the use of electronic media in at least the casting of the vote.
Experiment	A trial in which the result of the election is binding.
Family voting	A process which refers to circumstances in which one family member decides or influences the voting choices of other family members.
Identification	The verification of a person's identity.
Kiosk voting	Stand-alone DREs. They can, for example, be placed in town halls or universities or at train stations.
Locking the electronic ballot box	A cryptographic process where the electronic ballot box is sealed just before the start of the election.
Paper trail (or voter verifiable audit paper trail)	An independent verification system for voting machines designed to enable voters to check that their vote was cast correctly, to detect possible election fraud or malfunction, and to provide a means of auditing stored electronic results.

Pilot	A trial where the result of the election is not binding. Can be limited to a specific time frame.
Polling card	A card entitling its holder to vote.
Remote e-voting	E-voting where the vote is cast via a device not controlled by an election official.
Sealing	Protecting information so that it cannot be used or interpreted without other information or means available only to specific persons or authorities. This restricts physical access.
Source code	A collection of statements or declarations written in a human readable computer programming language. The means most often used by programmers to specify the actions to be performed by a computer.
Token	A device used to authenticate the voter.
Transparency	The concept of determining how and why information is conveyed through various means.
Unlocking the electronic ballot box (after the ballot closes)	A cryptographic process in which the electronic ballot box is unsealed just after the election has closed and before the results are counted.
Usability	The ease with which people can employ a particular tool or other man-made object in order to achieve a particular goal.
Vote	The expression of the choice of voting option.
Voter	A person entitled to cast a vote in a particular election or referendum.
Voter register	A list of persons entitled to vote (electors).
Voting channel	The way in which the voter can cast his/her vote.
Voting options	The range of possibilities from which a choice can be made by casting one's vote in an election or referendum.

Voting period	The time frame within which voting is permitted (the fact that a vote has been cast within the voting period must be ascertainable).

Appendix II – Bibliography

1. Country experiences

Austria
www.oeh-wahl.gv.at
(only in German)

Belgium
www.elections.fgov.be
(only in French, Dutch or German)

Estonia
www.vvk.ee/internetvoting

Finland
www.vaalit.fi/electronicvoting

Ireland
www.electronicvoting.ie

Netherlands
www.rijksoverheid.nl
(only in Dutch)

Norway
www.valg.no

Switzerland – Federal Chancellery
www.bk.admin.ch/themen/pore/evoting
(only in French, Italian and German)

Switzerland – Geneva
www.geneve.ch/evoting/english

Switzerland – Neuchatel
www.neuchatelville.ch

Switzerland – Zurich
https://evoting.zh.ch

United Kingdom
www.justice.gov.uk/whatwedo/electoralmodernisation.htm

2. Organisations

Carter Center
www.cartercenter.org

Council of Europe
www.coe.int

Competence Center for Electronic Voting and Participation (E-Voting.CC)
www.e-voting.cc

IFES
www.ifes.org

International IDEA
www.idea.int

National Democratic Institute
www.ndi.org

Organization of American States
www.oas.org

OSCE Office for Democratic Institutions and Human Rights, Election Department
www.osce.org/odihr-elections

Sales agents for publications of the Council of Europe
Agents de vente des publications du Conseil de l'Europe

BELGIUM/BELGIQUE
La Librairie Européenne -
The European Bookshop
Rue de l'Orme, 1
BE-1040 BRUXELLES
Tel.: +32 (0)2 231 04 35
Fax: +32 (0)2 735 08 60
E-mail: order@libeurop.be
http://www.libeurop.be

Jean De Lannoy/DL Services
Avenue du Roi 202 Koningslaan
BE-1190 BRUXELLES
Tel.: +32 (0)2 538 43 08
Fax: +32 (0)2 538 08 41
E-mail: jean.de.lannoy@dl-servi.com
http://www.jean-de-lannoy.be

BOSNIA AND HERZEGOVINA/
BOSNIE-HERZÉGOVINE
Robert's Plus d.o.o.
Marka Maruliça 2/V
BA-71000, SARAJEVO
Tel.: + 387 33 640 818
Fax: + 387 33 640 818
E-mail: robertsplus@bih.net.ba

CANADA
Renouf Publishing Co. Ltd.
1-5369 Canotek Road
CA-OTTAWA, Ontario K1J 9J3
Tel.: +1 613 745 2665
Fax: +1 613 745 7660
Toll-Free Tel.: (866) 767-6766
E-mail: order.dept@renoufbooks.com
http://www.renoufbooks.com

CROATIA/CROATIE
Robert's Plus d.o.o.
Marasoviçeva 67
HR-21000, SPLIT
Tel.: + 385 21 315 800, 801, 802, 803
Fax: + 385 21 315 804
E-mail: robertsplus@robertsplus.hr

CZECH REPUBLIC/RÉPUBLIQUE TCHÈQUE
Suweco CZ, s.r.o.
Klecakova 347
CZ-180 21 PRAHA 9
Tel.: +420 2 424 59 204
Fax: +420 2 848 21 646
E-mail: import@suweco.cz
http://www.suweco.cz

DENMARK/DANEMARK
GAD
Vimmelskaftet 32
DK-1161 KØBENHAVN K
Tel.: +45 77 66 60 00
Fax: +45 77 66 60 01
E-mail: gad@gad.dk
http://www.gad.dk

FINLAND/FINLANDE
Akateeminen Kirjakauppa
PO Box 128
Keskuskatu 1
FI-00100 HELSINKI
Tel.: +358 (0)9 121 4430
Fax: +358 (0)9 121 4242
E-mail: akatilaus@akateeminen.com
http://www.akateeminen.com

FRANCE
La Documentation française
(diffusion/distribution France entière)
124, rue Henri Barbusse
FR-93308 AUBERVILLIERS CEDEX
Tél.: +33 (0)1 40 15 70 00
Fax: +33 (0)1 40 15 68 00
E-mail: commande@ladocumentationfrancaise.fr
http://www.ladocumentationfrancaise.fr

Librairie Kléber
1 rue des Francs Bourgeois
FR-67000 STRASBOURG
Tel.: +33 (0)3 88 15 78 88
Fax: +33 (0)3 88 15 78 80
E-mail: librairie-kleber@coe.int
http://www.librairie-kleber.com

GERMANY/ALLEMAGNE
AUSTRIA/AUTRICHE
UNO Verlag GmbH
August-Bebel-Allee 6
DE-53175 BONN
Tel.: +49 (0)228 94 90 20
Fax: +49 (0)228 94 90 222
E-mail: bestellung@uno-verlag.de
http://www.uno-verlag.de

GREECE/GRÈCE
Librairie Kauffmann s.a.
Stadiou 28
GR-105 64 ATHINAI
Tel.: +30 210 32 55 321
Fax.: +30 210 32 30 320
E-mail: ord@otenet.gr
http://www.kauffmann.gr

HUNGARY/HONGRIE
Euro Info Service
Pannónia u. 58.
PF. 1039
HU-1136 BUDAPEST
Tel.: +36 1 329 2170
Fax: +36 1 349 2053
E-mail: euroinfo@euroinfo.hu
http://www.euroinfo.hu

ITALY/ITALIE
Licosa SpA
Via Duca di Calabria, 1/1
IT-50125 FIRENZE
Tel.: +39 0556 483215
Fax: +39 0556 41257
E-mail: licosa@licosa.com
http://www.licosa.com

NORWAY/NORVÈGE
Akademika
Postboks 84 Blindern
NO-0314 OSLO
Tel.: +47 2 218 8100
Fax: +47 2 218 8103
E-mail: support@akademika.no
http://www.akademika.no

POLAND/POLOGNE
Ars Polona JSC
25 Obroncow Street
PL-03-933 WARSZAWA
Tel.: +48 (0)22 509 86 00
Fax: +48 (0)22 509 86 10
E-mail: arspolona@arspolona.com.pl
http://www.arspolona.com.pl

PORTUGAL
Livraria Portugal
(Dias & Andrade, Lda.)
Rua do Carmo, 70
PT-1200-094 LISBOA
Tel.: +351 21 347 42 82 / 85
Fax: +351 21 347 02 64
E-mail: info@livrariaportugal.pt
http://www.livrariaportugal.pt

RUSSIAN FEDERATION/
FÉDÉRATION DE RUSSIE
Ves Mir
17b, Butlerova.ul.
RU-117342 MOSCOW
Tel.: +7 495 739 0971
Fax: +7 495 739 0971
E-mail: orders@vesmirbooks.ru
http://www.vesmirbooks.ru

SPAIN/ESPAGNE
Díaz de Santos Barcelona
C/ Balmes, 417-419
ES-08022 BARCELONA
Tel.: +34 93 212 86 47
Fax: +34 93 211 49 91
E-mail: david@diazdesantos.es
http://www.diazdesantos.es

Díaz de Santos Madrid
C/Albasanz, 2
ES-28037 MADRID
Tel.: +34 91 743 48 90
Fax: +34 91 743 40 23
E-mail: jpinilla@diazdesantos.es
http://www.diazdesantos.es

SWITZERLAND/SUISSE
Planetis Sàrl
16 chemin des Pins
CH-1273 ARZIER
Tel.: +41 22 366 51 77
Fax: +41 22 366 51 78
E-mail: info@planetis.ch

UNITED KINGDOM/ROYAUME-UNI
The Stationery Office Ltd
PO Box 29
GB-NORWICH NR3 1GN
Tel.: +44 (0)870 600 5522
Fax: +44 (0)870 600 5533
E-mail: book.enquiries@tso.co.uk
http://www.tsoshop.co.uk

UNITED STATES and CANADA/
ÉTATS-UNIS et CANADA
Manhattan Publishing Co
2036 Albany Post Road
USA-10520 CROTON ON HUDSON, NY
Tel.: +1 914 271 5194
Fax: +1 914 271 5886
E-mail: coe@manhattanpublishing.coe
http://www.manhattanpublishing.com

Council of Europe Publishing/Editions du Conseil de l'Europe
FR-67075 STRASBOURG Cedex
Tel.: +33 (0)3 88 41 25 81 – Fax: +33 (0)3 88 41 39 10 – E-mail: publishing@coe.int – Website: http://book.coe.int