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.