

SECRETARIAT GENERAL

DIRECTORATE GENERAL OF DEMOCRACY AND
POLITICAL AFFAIRS

DIRECTORATE OF DEMOCRATIC INSTITUTIONS

PROJECT “**GOOD GOVERNANCE IN THE INFORMATION SOCIETY**”



Strasbourg, February 2008

**Compliance of the BeVoting Study with the
Recommendation (2004) 11 of the Committee of Ministers of
the Council of Europe to member states on legal, operational
and technical standards for e-Voting**

TABLE OF CONTENTS

1. Preliminary remarks	3
2. Overview	3
2.1 General Comparison	3
3. The first scenario- Ballot Booklets	4
3.1 Key issues	4
3.1.1 Paper Trail	4
3.1.2 Audit and Certification	5
3.1.3 Security	6
3.1.4 Counting of the Votes	6
3.1.5 Camera-based reader as barcode reader	6
3.1.6 Multi-polling station computer	6
3.1.7 Voting Urn	6
3.2 Detailed analysis of the Council of Europe's Recommendation	7
4. The second scenario- Optical Scanning	7
5. The third scenario- Thin Client System	8
6. The fourth scenario- Remote Internet Voting	9
7. The fifth scenario- Kiosk Voting	10
 Appendix- Article-by-Article Assessment of the Belgian Study in comparison with Recommendation Rec(2004)11 of the Committee of Ministers of the Council of Europe to member states on legal, operational and technical standards for e-voting	 12

1. PRELIMINARY REMARKS

This report intends to assess the compatibility of the five scenarios presented in the Belgian Study Consortium's "*BeVoting study of electronic Voting Systems*"¹ with Recommendation Rec(2004)11 of the Committee of Ministers of the Council of Europe to member states on Legal, operational and technical standards for e-voting (hereafter the Recommendation).

The Council of Europe was asked to examine the overall coherence of the Study and the extent in which it complies with the Recommendation. The following report has been prepared with the assistance of an independent researcher commissioned by the Directorate General of Democracy and Political Affairs, Dr. Jordi Barrat Esteve.

This report will first present some general remarks on the Study, followed by a general overview of the five proposals' compliance with the Recommendation. Like the Study, it will also focus on the first system and highlight its key issues. The appendix to this report contains detailed elements of comparison between the preferred scenario and the Recommendation on e-voting.

N.B. The numbers in parenthesis refer to Articles in the appendices of the Recommendation.

2. OVERVIEW

2.1 General Comparison

Although there are five different scenarios, some of them share similar patterns or basic principles that mean they can be classified together where others stand alone. For instance, the fourth scenario must remain distinct as it is the only one to accept voting from unsupervised locations and is consequently faced with questions regarding the secrecy of the vote and voter freedom.

The first three scenarios are very similar, given that the voting process takes place in a traditional polling station and includes a paper-based procedure - ballot tickets, ballot booklets or normal paper ballots uploaded onto a computer with a scanning device; presumably introduced as a means to strengthen citizen confidence in the procedure. Optical scan voting, in which paper ballots are recorded by an optical-scan machine, may not alter the electoral routine of the citizens, but can nonetheless be subject to concerns about their technical accuracy. In a thin client system, in which electronic voting machines are connected to a local network (with a paper trail option), clarity is paramount, so as to ensure that all voters can actually verify their vote before the final electronic confirmation. However, the use of eID cards and the creation of an internal network could increase the danger to the anonymity and integrity of the votes. The ballot booklet proposed in the first scenario contains a human readable part that could easily be used to verify the vote cast if need be. However, this division of a single vote into two components creates a dilemma as to which part of the booklet represents the genuine will of the voter. The usability issues for this scenario are similar to those of the current e-voting system.

The fourth scenario, internet voting, clearly poses the greatest number of legal and security challenges. Its implementation can only be considered when its necessity and goals have been clearly established.

Finally, the fifth scenario, kiosk voting, mixes some features of internet voting such as the use of an external network, with traditional voting carried out in a supervised environment. In the absence of a paper trail, public confidence in this system needs to rest on the proper organisational and technical measures being taken.

¹ BeVoting, Study of Electronic Voting Systems. Part I and Part II of the "Studie Geautomatiseerde Stemming Def. Vs 18122006". Versions 1.1, 15 April 2007 (Part I) and version 0.9999999, 12 October 2007.

Despite their differences on issues of usability, integrity and confidentiality, the five scenarios share one common feature: the final results of the election are always generated by electronic means. Transparent procedures, audit measures and certification mechanisms are therefore important to ensuring a trustworthy system.

At this point, attention should be drawn to the risk of detectable radiation from the voting machines. It has been proved that radio emanations from certain voting machines can be detected from several meters distance and be used, by means of a device, to reveal who has voted for which party or candidate. The Belgian authorities should look closely into this matter, before introducing new voting machines.

As regards the compliance of the different scenarios with the Recommendation on e-voting, the conclusion is that in their present form, the scenarios do not fully comply with the Recommendation. In the first scenario for example, special attention needs to be given to auditing and certification and the recount. However, following some adjustments to the first scenario, the Belgian authorities should have no problem complying with the Recommendation. The other scenarios would require some more modifications in order to comply with the Recommendation.

3. THE FIRST SCENARIO – Ballot Booklets

The first proposal is quite similar to the current electronic voting scheme in Belgium. However, it introduces some key changes to both update the technology and to increase transparency (e.g. paper trail). In spite of these and other minor changes, the new system will not require a significant adaptation in the electoral routine of Belgian e-voters under the present system. This is a key advantage.

However, there remain several sensitive areas in need of analysis. The next section outlines some of these key issues.

3.1 Key Issues

3.1.1 Paper Trail

(i) General Remarks

In the current scheme, a two-step procedure is employed; the voter inserts their token (a magnetic card without a human readable part) into a voting machine inside a booth, selects their candidate/ party on that same machine, and afterwards deposits their token into a ballot box outside the booth. The ballot box counts the votes and produces another magnetic card containing the results. This second token is then sent to the first totalisation centre to be aggregated with the others.

The proposed system is quite similar: a two-step voting procedure including a token given to the voter by the polling station staff. The introduction of a paper trail is the major innovation of this scenario. After the voter has cast their vote, a ballot booklet is printed and inserted into the ballot box by the voter. This ballot booklet contains not only a barcode that will be processed through a computer, but also a human readable part, comprehensible to the citizen.

The introduction of paper trails is a recurrent demand of those groups concerned by the opacity of e-voting systems; citizens, and even electoral authorities, who do not understand how the voting machine really works cannot properly scrutinise the electoral procedure. In order to counter the preeminence of computers in an e-voting system, a VVPAT (Voter Verified Paper Audit Trail) can be an effective way to re-empower the citizen in the electronic electoral domain. However, the Recommendation does not address this issue directly.

(ii) A Computer-less Recount

The Recommendation accepts different types of recounts (article 26), including those carried out by the same devices, those carried out by different equipment and, finally, a manual recount based on the paper trail. However, it is worth noting that the same article of the Recommendation stresses that these solutions are of varying complexity and offer different levels of accountability. This being the case, although different types of recount may be accepted, the explanatory memorandum on article 98 explains that "*to gain confidence, it is most important that the counting process can be reproduced and that this can be done with a different system from a different source*" (p.162). It is clear, therefore, that a recount carried out with the same devices, the same decoders and readers, would finally be less acceptable than, for example, the use of different electronic devices.

(iii) Which Is the Genuine Ballot?

The Study rightly raises this issue: although a single vote should not be divided, the ballot booklet contains two parts. The voter inserts the whole ballot booklet into the ballot box, yet it is the barcode that will be used to carry out the first and perhaps the only tally.

The problem is perhaps best viewed through the procedure for disqualifying a marked booklet. Although the returning officer inspects all ballot booklets for external marks, he or she must not unfold them to check for internal marks, thus rendering it possible for a voter to legally cast a vote with a marked booklet. Should a recount occur in which the human readable content of the ballot booklet is checked, the mark will be discovered. Under the normal circumstances of a democratic election, such a ballot would be disqualified for violating the principle of secrecy. In this case, however, the problem arises as the vote in question has already been accepted in the previous, official, electronic tally. Invalidation would generate a mismatch between paper and electronic results. An easy though provocative solution would be to simply ignore these marks, despite the threat to vote secrecy. If procedure clearly stresses the importance of the returning officer's inspection of the booklet before accepting it, there is arguably little point in attributing much importance to a mark discovered inside the book later on.

Unfortunately, at the time the Recommendation was drafted, ballot booklets were not an option, therefore it does not express a preference. However, from a legal standpoint one could argue that the human readable part should prevail, because it is the only part comprehensible to the voter. In order to avoid any dispute at a later stage, the Belgian authorities should decide on this matter before the new system is introduced.

3.1.2 Audit and Certification

Although a paper trail helps to promote transparency and confidence in the system, other audit and certification measures remain necessary. The VVPAT could guarantee the accuracy of the tally but not other key electoral issues, such as the secrecy of the vote. It is important that the whole set of principles are safeguarded and it is therefore imperative that the system's internal architecture includes adequate audit and certification mechanisms that will ensure the proper structure and performance of hardware and software

Currently, the organisational aspects of auditing and certification include two kinds of external supervision carried out by private certification companies and the College of Experts. These are the only two bodies that analyse the performance of the system and report on elections. The Interior Ministry relies on these reports and tends to accept and support e-voting platforms on their basis. Furthermore, the political parties receive a copy of the voting machine's source code in advance which is then published by the Ministry on the internet following the election.

The Consortium's Study mentions the current audit procedures, such as the certification of computer

devices, several times. It also stresses the role of the College of Experts and other independent auditors, but does not have a specific section devoted to this topic. The Study, whilst analysing in depth the advantages and weaknesses of the five e-voting scenarios, offers no similar analysis of the actual performance of the current supervision mechanisms in order to propose improved procedures. The implicit conclusion then is perhaps that the new e-voting system will be compatible with the current supervision framework. However, it remains advisable for the Belgian authorities to further evaluate the current auditing system in order to see whether it can be improved and if so, how.

3.1.3 Security

Many requirements in the Recommendation focus on the proper computer settings and organisational measures needed for a secure and stable e-voting system. The electoral authorities are obliged to establish a complex array of security mechanisms. A mistake by the supplier or system administrator in charge of such delicate operations could potentially jeopardize the introduction of the e-voting system. The Study rightly recognises this problem and stresses its importance, suggesting the use of access restrictions and controlled environments for procedures such as the installation and configuration of software.

The explanatory memorandum to the Recommendation also foresees that certification results be made available to political parties (article 50). The current system does not include this provision which would be worth integrating into the new voting system.

3.1.4 Counting of the Votes

It is unclear from the Study when a polling station is allowed to scan the ballot papers, effectively doubling-up as a Scanning Centre and when it is not. This creates confusion regarding Recommendation articles 1 and 20. It would be difficult for the voters to understand why one polling station is authorised to scan their ballots, while another is not.

If a polling station is authorised to scan the ballot papers, that office would require an internet connection in order to send its results to the Counting Centre. In the Study, there is no mention of any internet connection in the polling station, or how it should be installed. This issue, therefore, requires clarification.

3.1.5 Camera-based reader as barcode reader

It is difficult to concur with the Study that the introduction of a camera-based barcode reader would be a small change to the current laser pen. In particular, it would be an important change for the voters who currently vote by pencil and paper. In order to comply with the Recommendation's article 22 in the introduction of the barcode reader, the Belgian authorities should give greater consideration to the arrangement and degree of training that might be necessary for the use of the new barcode reader. This could also be a welcome opportunity to inform citizens about democracy and possibly raise curiosity about the topic.

3.1.6 Multi-polling station computers

It is unclear why the Study suggests the use of computers which could be used in more than one polling station. The Belgian authorities are advised to look into this further.

3.1.7 Voting Urn

One of the goals of the Study is to make the voting process as a whole more transparent. As such, the suggested use of a non-transparent voting urn is slightly contradictory. The Belgian authorities are

encouraged to take a closer look at ways in which the ballot booklet might be folded or closed, in order to permit the use of an open urn, thus creating more transparency.

3.2 Detailed Analysis of the Council of Europe Recommendation

In the Appendix to this evaluation, the reader will find a section intended to complement the table included in the Study. Comments under each Article of the Recommendation do not always mean that a contradiction exists between it and the proposed system. These comments are intended to provide supplementary information in that particular area and indeed to outline discrepancies where they occur.

4. THE SECOND SCENARIO- Optical scanning

Optical scan systems in which paper ballots are converted into electronic form by optical-scanning devices may seem like a conservative e-voting proposal given its full paper trail and the minimal changes required in electoral routine. This conclusion is not entirely accurate. First of all, the paper-trail does not reduce either the importance of the electronic tally in this system or its inherent dangers. Secondly, some versions of the optical scan system envisaged by the Consortium would indeed alter voting behaviour considerably, e.g. if the voters were to scan the ballot themselves. Finally, even an apparently straightforward optical scan voting system could pose unexpected threats, in the form of fake ballots for example.

A realistic appraisal of this voting scenario, previously viewed as a tentative and conservative first step towards e-voting, reveals further risks that must be properly evaluated. For example, the actual usability (Article 1) of these ballots is not at all clear. The Consortium rightly analyses the feasibility of multiple sheet ballots, double sided ballots and/or abbreviated ballots given the limited capacity of the relevant hardware.

The layout of these documents obviously needs to be extremely accurate and transparent so that no voter finds it difficult to vote for their preferred candidate. The current electoral system uses a one-sided ballot which, although very large at times, provides clear information to the voter. The technical requirements of the optical scan process however, could mean that the ballots cannot be in the clear one-sided format. Instead, voters may be confronted with a new and perhaps less user-friendly system. Furthermore, this being the case, the system offers little room for improving accessibility for people with disabilities (article 3).

Finally, usability could be called into question should voters be required to scan their own ballots. Even the simplest scanning device is bound to be misunderstood and misused by a certain number of voters. Such devices could also risk contradicting other parts of the Recommendation, for example article 14 which states that every voter must receive a clear message when the voting process is concluded, a message which the self-scanning process may render distinctly unclear. In order to avoid confusion and disruption, the device ought to include a clear display, or perhaps an audible message, to inform the voter as to the correct procedure and its successful completion.

Regulations should also provide accurate information as to whether the voting procedure may be broken off (article 11) during the scanning process. Given that the Study only foresees these changes during the marking stage, prior to scanning their ballot, the voter should receive a message informing them that it will not be possible to change their vote later on, or to cancel the session.

The optical scan voting system faces yet another challenge in terms of the equitable presentation of candidates (article 47). As mentioned, traditional paper ballot systems meet this requirement with the one-sided ballot, whereas other e-voting solutions employ a two-step procedure, political party followed by individual candidates, to these ends. Optical scan systems, however, are unsuited to both of these methods.

In the case of numerous candidates for example, a one-sided format would be too small or, were an abbreviated layout used, possibly too difficult to understand. In this case, if a candidate's name were placed on the back of a double-sided ballot or on a different page entirely, they could legitimately argue that the electoral conditions were not sufficiently fair.

Undetected multiple voting is another potential problem (article 5) with the self-scanning optical scanning system. Given that the returning officer at the polling station has no control over the actions performed in the booth, only secure computer settings can guard against multiple voting with the same ballot or even fake ballots. Normally the ballot inspection by the returning officer acts as the main guarantee against multiple voting as they ensure that only one ballot is inserted into the ballot box. E-voting systems with a paper trail, like the first scenario of the Consortium's Study, maintain this guarantee.

Numbering ballots has been suggested as a solution to this problem. However, such a solution clearly engenders a new threat to voter secrecy if the chronological sequence of votes is reconstructed when counting votes at the polling station: the voters could theoretically be identified (article 16, 17). Obviously, randomizing computer settings could avoid this problem though this is unlikely to inspire the same degree of confidence as the sight of the returning officer inspecting the ballot.

Finally, it is worth noting that a paper recount in this system will produce the same dilemmas as in the first scenario, for example the question of what to do with a ballot discovered to be marked and whether it should be discounted, generating a mismatch with the first tally. If an electronic recount is used, the problem remains that the citizen's confidence must once again rest on the perceived reliability of computers.

Optical scan systems share similar problems, and indeed solutions, with the other four scenarios: information and training needs (articles 21, 22, 36, 38, 46), secure computer settings (articles 5, 7, 15, 18, 28, 29, 30, 31, 34, 53, 54, 55) and the implementation of open audits and inclusive observation procedures (articles 23, 25, 31, 32, 33, 56, 57, 58, 60). The findings included in the previous pages are therefore equally valid for the optical scan system, although they should be modified accordingly. This applies to the following chapters which analyse the third, fourth and fifth scenarios as well.

5. THE THIRD SCENARIO- Thin Client System

The third scenario, unlike the first and second, is a one-step electronic procedure. In optical scan voting and ballot booklet systems, ballots are marked during the first stage and put into the ballot box in the second. The thin-client voting system reduces the process to a single, purely electronic step; the voters' final decision will be made at the touch of a button.

Consequently, this system may be contrary to Council of Europe principles such as the voters' clear understanding of the voting process as a whole (article 1, 20) if the voting machine's layout is not suitably clear. Confirmation of the vote through a printed ticket is certainly a useful measure to promote clarity and voter confidence, but it should nonetheless be made very clear that the real confirmation, the real vote, has already been cast through the machine; the ticket is never in the possession of the voter who verifies that its details are correct before it drops into the urn.

Usability (article 1) is a very important consideration for a ticket system. The layout of the ticket should mean that it is easy for all to read, including the visually impaired. The urns themselves might cause further problems for voter confidentiality, given that it would be difficult for the machine to fold the ticket before it drops it into the urn (article 16, 17, 52). Non transparent urns are a controversial solution but one which could perhaps only work if the voter was able to somehow check that their ticket is correctly stored. Finally, if the voter decides not to confirm their vote after the ticket is printed, the system should ensure the destruction of

this document in a manner sufficient to ensure that its content could not be reconstructed by any means (article 11). The use of false, duplicated or stolen ID cards should be properly prevented as well.

Although not specifically required for a thin client voting system, the Consortium foresees its use in conjunction with eID cards, that is, that citizens would identify themselves with their eID card and then cast their vote on the same machine. Clearly, merging identification and voting considerably increases the threat to vote secrecy and confidentiality (article 16, 17, 19, 35). Such a system would no doubt also hamper the growth of citizens' confidence (article 20) and require additional measures to control and secure the register (article 39).

It is important to note that the ticketing element of the thin client voting system allows for a paper recount (article 26, 59). However, as the Consortium Study points out, these receipts will also have a barcode to allow for speedier recount which, however, leads back to the same problem encountered in the first scenario.

Finally, it is worth noting that the list of candidates should be made available by non electronic means (article 43).

In chapter 4, the Study describes specific criteria for the new voting system. One of these is that citizens living in one municipality should be allowed to cast their vote in another municipality. This is especially important given that the Recommendation explicitly states that one of the purposes of introducing or using e-voting is to enable voters to cast their votes from a place other than the polling station in their polling district (p.6 Recommendation) which of course would help the Belgian voters fulfil their duty of voting. It is regrettable that this criterion is only briefly addressed in the presentation of the thin client voting system. The Belgian authorities should take this issue into consideration, especially in the framework of the preferred first scenario.

6. THE FOURTH SCENARIO- Remote Internet Voting

It is unfortunate that this scenario is not explored in greater depth in the Study, especially in light of the bill on the introduction of remote e-voting pending in the Belgian Parliament. Although it may be considered acceptable in the context of this kind of broad-ranging report, the complexity and delicacy of the internet voting scenario vis-à-vis the Committee of Ministers' Recommendation would merit a deeper analysis than it has hitherto received. More so than in any other scenario, the computer plays the central role in the voting process which means that procedural guidelines and secure computer settings become all the more important.

Internet voting is the most controversial topic within the e-voting debate. Only a handful of countries currently accept it in various forms and, although there are several projects underway, for example in Switzerland and Estonia, all agree that its implementation should be especially thorough if its inherent challenges are to be properly tackled.

The fourth system raises another important question regarding the universal availability of internet voting and the establishment of supplementary or alternative voting channels. Although the internet is a worldwide network that is theoretically open to everybody, this is not enough to meet the Council of Europe's Recommendations until it becomes "effectively available" to everybody (p. 30 memorandum). Therefore, remote voting channels should still be accompanied by traditional voting methods, like the paper ballot procedures for Belgians living abroad.

Greater consideration should be given to the identification mechanisms of internet voting. Moreover, if remote internet voting is accepted alongside paper voting, the identification mechanism must be protected against any temporal gap that might allow for multiple voting (article 5, 6). Some countries opt for a

diachronic method, and close remote internet voting before Election Day to ensure the electoral roll has been properly updated. As mentioned regarding the thin client system, this does not solve the problem that merging identification and voting into a single action constitutes a threat to the secrecy of the vote (article 16, 17, 19, 32)

Free suffrage includes the right to a clear and calm voting process (article 10). As the report mentions, the confirmation step is a key measure to ensure that the voter actually knows and acknowledges what they have done. This concern is equally important for remote voting and, furthermore, besides the confirmation stage, applies to the entire process beforehand; on-screen options must be especially clear when the general tendency is to simply glance over rather than properly check the confirmation screen.

As for the other scenarios, the clear and comprehensive presentation of information to the voter is vital in securing a sound voting process. In the case of remote voting, article 50 suggests the addition of a warning message alerting the voter that they are not merely participating in a pilot or trial but a real and valid voting session. Although the Study states that the confirmation step is enough to meet this condition, the whole process should be organised and presented in such a way as to ensure it is understood as an official and binding election.

It is difficult to achieve absolute public confidence in an internet voting system (article 20). Efficient observation measures could mitigate and perhaps overcome this challenge, although concerns over transparency in this area preclude an easy and foolproof solution. The Study twice mentions that, for security reasons, observers may not have access to the most important computer rooms –exception accepted by article 23 of the explanatory memorandum— and that scrutinisers must be trained in advance. Whilst supplementary monitoring measures could be used to address the first issue, the training required for scrutinisers could raise questions about the accessibility and rationale of an open-to-all, supposedly transparent, observation system.

However, a recount is always a good way to address any perceived problems with electronic voting methods although, in the case of internet/remote voting this recount would once again be wholly reliant on electronic tallying (article 26). This may prove acceptable only if, in accordance with Council of Europe standards, the electronic recount is carried out on a different system or by a different method i.e. the recount must not be technically identical to the first count (article 98).

The Belgian Authorities should also take the following issues into consideration:

1. There is no clear plan on how to deal with the registration of the voters (article 2, 40).
2. It is unclear how tabulation takes place (the report speaks of one token and later of tokens).
3. The voter has to download software in order to vote (article 61 states that software should be able to be used by all voters, and article 93 describes how to delete information which has been left on a computer).
4. The Study's table comparing the fourth scenario with the requirements of the Recommendation needs more attention.

Finally, although deemed inapplicable in the Study, article 43 could also be enforced for remote internet voting: Citizens should receive a paper list of the candidates before the elections, either by post or as part of an identification procedure that might be introduced in conjunction with internet voting.

7. THE FIFTH SCENARIO- Kiosk Voting

Having analysed the first four scenarios, the last one offers few novelties. Its architecture is a mixture of internet voting, cast through an open network, and stationary voting, cast within a supervised environment. This so-called "kiosk voting" attempts to solve the problems of internet-based remote voting, especially

regarding identification and the freedom of the vote, by supervising the environment in which it takes place. The following paragraphs focus on some specific features of this system, although a more complete picture of its advantages and drawbacks can and must be seen by stepping back and viewing it together with the other scenarios.

The identification procedure is a key difference between kiosk and internet voting. Whereas the latter merges the identification and voting process (with only secure computer settings standing in the way of any further and improper connection of this data); the former faces no such threat by relying on traditional identification procedure. The Consortium accepts this system although it is worth noting that the thin client method, which is very similar to the 5th scenario, uses an electronic identification card and therefore also poses the risk of connecting personal and voting data.

The compulsory use of a voting booth in order to guarantee the freedom of the vote is another central feature of this scenario. Although the inherent problem remains that the electronic ballot is immediately transmitted to a central server, the citizen's freedom of choice is nonetheless secured. Furthermore, unlike a remote internet voting system, the kiosk system would mean that computer settings could be properly checked and constantly monitored (for spy ware for example); though in the event of improper information being displayed to the voter (article 48) the consequences would be more dangerous than in the current voting system given that the device is not isolated.

Besides the technical mechanisms required to secure an open network, the kiosk system will have to ensure, as in the first scenario, that the voting computer complies with Council of Europe standards. Amongst other things, the computer must not be able to store information or display one citizen's vote to the next voter. Mixing two voting methods—open network with supervised environment—requires the use of mixed security arrangements. Furthermore, the network managers would have to collaborate to ensure that the ballot box remains open until the vote of the last citizen to arrive at the polling station before the official voting period closes, has been cast.

As ever, the list of candidates should be available by non-electronic means (Recommendation 43). Despite the Consortium's comments on this subject, the condition remains applicable to this scenario and would in fact pose no great challenge were for example, the list displayed in the polling station itself.

Finally, public confidence remains a major, if not the major challenge. As the Consortium points out, the absence of a paper trail and the transmission of the vote to a central server are changes, or rather losses in control over the electoral process that the voter could find difficult to accept. In this regard, the kiosk system is little different to internet voting, despite its considerable security advantages.

APPENDIX

Article-by-Article Assessment of the Belgian Study in comparison with Recommendation Rec(2004)11 of the Committee of Ministers of the Council of Europe to member states on legal, operational and technical standards for e-voting

The following provides a list of the Articles set out in the Appendix to the Recommendation. Under each Article, the corresponding part of the Belgian study is shown in italics followed by the comments resulting from this assessment. These comments do not necessarily mean that a contradiction exists between the proposed system and the requirements. They are intended to provide supplementary data and outline discrepancies where they do occur. The most relevant issues have already been addressed in the above overview.

Appendix I

Legal standards

A. Principles

I. Universal suffrage

1. The voter interface of an e-voting system shall be understandable and easily usable.

Similar to eVoting system currently in use.

Though similar, there are some important differences such as the use of a barcode reader instead of the laser pen and the introduction of the paper ballot printout which the voter must then physically cast. The overall operation is easily understandable and usable, but there are some key steps that should be analysed in depth (e.g. the selection of candidates with the barcode reader, folding the booklet).

2. Possible registration requirements for e-voting shall not pose an impediment to the voter participating in e-voting.

Identical to traditional paper ballot voting.

Identical to traditional paper ballot voting that is still used in many Belgian polling stations.

3. E-voting systems shall be designed, as far as it is practicable, to maximise the opportunities that such systems can provide for persons with disabilities.

Similar to eVoting system currently in use. The proposed system also includes support for blind and visually impaired persons.

The new system can strengthen these capabilities. However, given that the Belgian e-voting system will completely substitute paper ballots, prior training in the use of the new machines will be necessary to ensure that citizens will not refuse to vote on the grounds of difficulty. Extensive and continuous training campaigns should be foreseen, especially for specific groups (such as the blind).

4. Unless channels of remote e-voting are universally accessible, they shall be only an additional and optional means of voting.

N. A.

—

II. Equal suffrage

5. In relation to any election or referendum, a voter shall be prevented from inserting more than one ballot into the electronic ballot box. A voter shall be authorized to vote only if it has been established that his/her ballot has not yet been inserted into the ballot box.

The voting computer requires the presence of a voting token before it can be used by the voter to cast a vote. The presentation of one voting token results in the production of one ballot booklet. One voting token=one ballot.

Identical to traditional paper ballot voting: the booklet ballot is introduced into the urn by the voter after identification and authorization by the President.

The ballot booklets are digitally signed by the voting computers, which prevent the insert of ballot booklets that did not originate from a genuine voting computer.

Actually this requirement does not mention that the ballot should be a genuine one. It only focuses on the fact that the voter can cast only one vote, that is, they can only put one ballot into the ballot box. The procedural guarantees are the same as those for the traditional paper ballot system. Even if the voting computer prints out several booklets, the inspection by the Chief Returning officer ensures that only one ballot (one booklet) is introduced into the ballot box.

The procedures implemented to avoid overvotes are the same that currently exist for paper ballots i.e. a manual mark on the poll book. However, the Returning officer may also scan the same barcode several times. Computer settings should prevent this scenario.

Voting computers could also encode several votes within the same barcode, but proper computer settings can prevent this danger. It is also important to include in the official non-electronic documents the total sum of voters per polling station according to a manual recount of the poll books' marks.

6. The e-voting system shall prevent any voter from casting a vote by more than one voting channel.

Only one channel is available.

Only one channel is available.

7. Every vote deposited in an electronic ballot box shall be counted, and each vote cast in the election or referendum shall be counted only once.

Not applicable: the voting urn (ballot box) does not perform the counting. It is only a recipient in which the ballot booklets are collected.

Appropriate procedural measures and technical safeguards must be installed to prevent loss of voting urns or voting ballots.

Actually there are two different ballot boxes: one physical, where the booklets are stored, and one electronic, that is, the file that is generated after the scanning of the barcodes. Procedural measures should ensure that all the votes are scanned and that the first ballot box is properly managed. The decoding and counting software should be correctly set up so that no vote is deleted or changed and every single vote is counted only once.

8. Where electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the correct result.

Similar to eVoting system in use.

The current and the proposed systems are based on a complete substitution of the traditional voting channel, that is, there will be only one way to vote in each polling station. The votes from other channels will be merged only at a totalisation level where e-voting ballots will have been already decoded and counted.

III. Free suffrage

9. The organization of e-voting shall secure the free formation and expression of the voter's opinion and, where required, the personal exercise of the right to vote.

Identical to traditional paper ballot voting, Guaranteed by the use of a voting booth. The possibility of revealing the content of the ballot before inserting it into the urn is already forbidden by article 143 of Electoral law.

Identical to traditional paper ballot voting.

10. The way in which voters are guided through the e-voting process shall be such as to prevent their voting precipitately or without reflection.

The design of the voting process shall ensure that this requirement is met.

The report includes specific provisions preventing electronic procedures from being either too fast or even too slow (p. 41). The confirmation step and the option to change the selection at any time before the final confirmation are critical guarantees to achieve this goal (p. 43).

11. Voters shall be able to alter their choice at any point in the e-voting process before casting their vote, or to break off the procedure, without their previous choices being recorded or made available to any other person.

The design of the voting process shall ensure that this requirement is met.

A procedure is available to void a ballot booklet and have the possibility to restart the voting process if a voter claims that the printed ballot does not correspond with the content of his vote.

The proposed system includes the option to alter previous selections at any time (p. 43). However, breaking off the procedure is only possible when the booklet is already printed out. Otherwise, if the voter leaves the booth without selecting a given option and therefore without a booklet, the Returning officer would normally ask them to go back and complete the procedure. Thus, specific legal provisions should be set up for this situation, for those people who leave the booth before ending the session and also those who refuse to continue the formal procedure.

12. The e-voting system shall not permit any manipulative influence to be exercised over the voter during the voting.

Identical to traditional paper ballot voting. Secrecy is guaranteed by the voting booth.

A manipulative influence could potentially come from the voting computer itself if its settings allow the transmission of improper images or messages to the voter. Therefore the voting booth is not enough and this requirement must also be achieved by appropriate control over the computer devices.

13. The e-voting system shall provide the voter with a means of participating in an election or referendum without the voter exercising a preference for any of the voting options, for example, by casting a blank vote.

Identical to traditional paper ballot voting. The voter may be asked to confirm a blank vote.

Identical to traditional paper ballot voting.

14. The e-voting system shall indicate clearly to the voter when the vote has been cast successfully and when the whole voting procedure has been completed.

Satisfied with the printing of the ballot and its insertion into the urn.

Given that the proposed system maintains the traditional ballot box, the insertion of the booklet is a clear message for the voter that the procedure is completed.

15. The e-voting system shall prevent the changing of a vote once that vote has been cast.

The voting computers digitally sign the barcode of the voting ballots, which means that it is impossible to alter the votes once the ballot has been printed: the voter inspects the human readable part of the voting ballot, and inserts it into the voting urn after the president of the polling station has inspected the ballot for marks.

Procedural mechanisms must be installed to guarantee that it is impossible to replace voting ballots that have been inserted in the voting urn.

Once the booklet has been printed out and inserted into the ballot box, the only way to alter the vote is to manipulate the booklet and this could be prevented by adequate procedural and computer means.

IV. Secret suffrage

16. E-voting shall be organised in such a way as to exclude at any stage of the voting procedure and, in particular, at voter authentication, anything that would endanger the secrecy of the vote.

Identical to traditional paper ballot voting. The voter receives a voting token from the President of the polling station after he has been successfully identified as an eligible voter. The token is no way linked to the voter: any voting token that was issued to use in a polling station will trigger the voting computer to start the voting process.

Obviously the tokens cannot be numbered because, if the voting computer also stores some critical data, a chronological reconstitution of the votes' sequence would be then feasible. It is advisable to use a limited

amount of tokens in each polling station (e.g. around ten) so that the same voting token will be used by several citizens during the voting day.

17. The e-voting system shall guarantee that votes in the electronic ballot box and votes being counted are, and will remain, anonymous, and that it is not possible to reconstruct a link between the vote and the voter.

Identical to traditional paper ballot voting. There is no direct link between the voting ballot and the voter. In particular: there is no information about the voter in the barcode of the ballot.

At the end of the voting period on Election Day, a mixed list of electronically scanned barcode is processed further on. The mixing even prevents establishing indirect link between the chronological order in which the barcodes are scanned and the ballot booklets in the voting urns.

The only way to reconstruct a link between voter and vote would be to match a list of barcodes in a given polling station with a chronological list of voters, but the proposed systems prevents this risk with neutral barcodes and further mixing procedures. Both measures rely on proper computer settings that should be duly controlled and audited. See also the explanatory memorandum of article 17.

18. The e-voting system shall be so designed that the expected number of votes in any electronic ballot box will not allow the result to be linked to individual voters.

Identical to traditional paper ballot voting. Totals for individual booths or for individual polling stations are not publicly available.

OK

19. Measures shall be taken to ensure that the information needed during electronic processing cannot be used to breach the secrecy of the vote.

There is no direct link between the ballot booklet and the voter. The randomization of ballot booklets prevents establishing indirect links.

See above comments on Recommendation articles 17 and 18.

B. Procedural safeguards

I. Transparency

20. Member states shall take steps to ensure that voters understand and have confidence in the e-voting system in use.

The ballot booklets contain a human readable part and a barcode. Critics of the electronic voting system that is used currently demanded the introduction of a paper trail to strengthen the confidence in the electronic voting system.

The human readable part of the paper trail can be verified by the voter. Independent auditors can select a random set of ballot booklets to audit elections by confirming that the barcode of these randomly selected ballots corresponds with their human readable part.

The voting computers do not contain any secret information that could link the identity of a voter with a particular voting ballot; the voting computers digitally sign the barcode of the voting ballots to prevent insertion of alien ballots, this does not allow linking a particular voting ballot to a particular voter.

The ballot booklet, with its human readable part, is a key step to ensure citizen's confidence and the understanding of the system, but it should not be implemented as a single measure. The citizens' support will also depend on other actions like, for instance, previous training sessions or a good information campaign (see *infra* 22).

21. Information on the functioning of an e-voting system shall be made publicly available.

To be achieved by publishing the full specification of the electronic voting mechanism and the vote counting process.

The Belgian Study foresees the publication of the software immediately after the certification process. It is an important improvement since currently only IT experts from each democratic party and the College of Experts receive this information prior to the elections, subject to a confidentiality agreement.

There is other critical information whose publication could enhance transparency. Internal and procedural rules, for example, are very important as they provide information about the content and handling of the hardware and software. Alongside other audit measures, this would publicly ensure that the installation and distribution of software is correctly done. The first section of the Consortium's Study describes the lack of comprehensive written information about the current e-voting system; this is something that could be avoided in the new scenario.

22. Voters shall be provided with an opportunity to practice any new method of e-voting before, and separately from, the moment of casting an electronic vote.

Training facilities should be made available both on the Internet and in the municipalities.

OK

23. Any observers, to the extent permitted by law, shall be able to be present to observe and comment on the e-elections, including the establishing of the results.

No specific provisions needed. The College of Experts should be kept in charge of this process.

Although it performs a valuable service, the College of Experts should not be considered a normal observer; it is a body whose members are appointed by the Chamber and is therefore not representative of civil society. Furthermore, the Document of the Copenhagen Meeting of the Conference on the Human Dimension of the OSCE of 29 June 1990 holds that member States must permit international and private observers.

II. Verifiability and accountability

24. The components of the e-voting system shall be disclosed, at least to the competent electoral authorities, as required for verification and certification purposes.

See general requirements.

The e-voting software is certified and based on open source patterns. It seems that the operating system will follow the same guidelines if we take into account that all the software, including the OS, will be open source (p. 13).

25. Before any e-voting system is introduced, and at appropriate intervals thereafter, and in particular after any changes are made to the system, an independent body, appointed by the electoral authorities, shall verify that the e-voting system is working correctly and that all the necessary security measures have been taken.

Belgian law stipulates that this should be done by a College of Experts: no specific provisions needed.

The legal framework and organisation of the College of Experts could be improved. For instance, until now the electoral duty of the College of Experts has not constituted a role in itself, and has had to be fulfilled alongside other ordinary tasks. The Consortium's Study itself stresses in the first section that even the current work load is proving difficult for the College to manage.

6. There shall be the possibility for a recount. Other features of the e-voting system that may influence the correctness of the results shall be verifiable.

Two types of recounts are possible:

a) Automated recount with different scanning equipment and/or software

b) Manual recount of human readable part of the ballot booklets (unless electronic ballots are considered authentic ballots).

The possibilities suggested by the CoE are the following: instruct the eVoting system to recount; transfer the electronic ballot box (voting urn) to a similar but distinct eVoting system and perform the second counting on this system; let the recount be performed by a different system which is interoperable with the eVoting system.

This means that the CoE accepts that the recounting of the ballot booklets would involve rescanning the 2D-barcode.

A recount is always possible by rescanning the barcodes and decoding and tallying a second time. However, if the recount is carried out by the same means i.e. the same barcode readers and decoders; the reliability of the electronic devices might still be called into question. Using different but interoperable equipment or carrying out a paper ballot recount would overcome these obstacles.

27. The e-voting system shall not prevent the partial or complete re-run of an election or a referendum.

No specific provisions needed.

No specific provisions needed.

III. Reliability and security

28. The member state's authorities shall ensure the reliability and security of the e-voting system.

Can be achieved by adequate procedures during pre-voting, voting, and post-voting stages.

—

29. All possible steps shall be taken to avoid the possibility of fraud or unauthorized intervention affecting the system during the whole voting process.

Can be achieved by adequate procedures during pre-voting, voting, and post-voting stages, as well as through the general requirements.

Although the report mentions security measures such as secure environments and digital signatures, it would be worth enhancing transparency and multi-responsibility at each step. For example, a secure environment can prevent external attacks, but the threat of internal attacks can only be avoided by collective responsibility (i.e. no action is decided by one person alone) and additional audit and certification measures.

30. The e-voting system shall contain measures to preserve the availability of its services during the e-voting process. It shall resist, in particular, malfunction, breakdowns or denial of service attacks.

Can be achieved by adequate procedures during pre-voting, voting, and post-voting stages, as well as through the general requirements.

The initializer of the voting computers can specify more than one boot credential for the voting computers, such that voting computers of one polling station can also be activated by the president of a polling station of another polling station. This would guarantee that the voting computers can be exchanged from one polling station to another in case of necessity. The only requirement is that the voting computers that are exchanged from one polling station to the other use the same voting configuration file, i.e., the voting computers must contain identical lists of elections, parties and candidates.

Each polling station has several voting computers that can be easily replaced as long as boot credentials are previously stored on spare devices. The breakdown of scanning and decoding equipment will not stop the procedure as the booklets could be processed by similar devices already deployed in other electoral districts. Finally, the lists with scanned and decoded barcodes as well as the final lists with the results could be reconstructed with the ballot booklets that are stored in a traditional ballot box.

31. Before any e-election or e-referendum takes place, the competent electoral authority shall satisfy itself that the e-voting system is genuine and operates correctly.

Can be achieved by adequate procedures during pre-voting, voting, and post-voting stages, as well as through the general requirements.

Pre-voting organisational measures (e.g., secure environments, encoded seals, digital signatures) are the only means available to achieve this goal, though absolute security cannot be guaranteed. Procedural mistakes may still occur and computerised security tests are, likewise, never 100% reliable. Transparency and the involvement of different stakeholders are key measures.

32. Only persons appointed by the electoral authority shall have access to the central infrastructure, the servers and the election data. There shall be clear rules established for such appointments. Critical technical activities shall be carried out by teams of at least two people. The composition of the teams shall be regularly changed. As far as possible, such activities shall be carried out outside election periods.

Can be achieved by adequate procedures during pre-voting, voting, and post-voting stages, as well as through the general requirements.

The report often mentions the critical role of the system administrator(s), but it does not include as a general rule that there be a minimum of two system administrators or a larger team with a frequent changeover of its members.

33. While an electronic ballot box is open, any authorized intervention affecting the system shall be carried out by teams of at least two people, be the subject of a report, be monitored by representatives of the competent electoral authority and any election observers.

Not applicable: the electronic urns (ballot boxes) do not contain any electronic components.

If a ballot box is the place where votes are stored, the proposed Belgian system will have two different urns: one with the ballot booklets and another, electronic box, in which the files containing the scanned barcodes that will later be decoded and counted. Within this framework, the decoding of such files is an action similar to opening a traditional ballot box and it should therefore have the guarantees mentioned in this Recommendation: teams of two people, specific report and monitoring carried out by the electoral authorities and any observer.

34. The e-voting system shall maintain the availability and integrity of the votes. It shall also maintain the confidentiality of the votes and keep them sealed until the counting process. If stored or communicated outside controlled environments, the votes shall be encrypted.

Three options exist to protect the information encoded in the barcode of the ballot booklet: (i) no encryption (i.e., no confidentiality protection of the vote), (ii) the application of a cryptographic padding scheme to hide the information of the barcode, (iii) encrypt the information of the barcode.

The voter must fold the paper ballot to hide the human readable part of the ballot booklet from third parties, in particular from the president of the polling station, as this official must inspect the ballot booklets to confirm that the folded ballot does not contain any marks. It is also possible to fold the human readable part of the booklet, and to glue it together, e.g., using the same mechanisms as used to seal an envelope.

If the ballot box is closed and sealed by traditional means, the folding of the booklet in conjunction with the encryption of the barcode ensures the integrity and confidentiality of the paper ballots. Proper computer settings should ensure the same goals with the list of scanned barcodes.

35. Votes and voter information shall remain sealed as long as the data is held in a manner where they can be associated. Authentication information shall be separated from the voter's decision at a pre-defined stage in the e-election or e-referendum.

See general requirements. There is no direct link between a ballot booklet and the voter. The ballot booklets are mixed before they are electronically scanned which prevents establishing indirect links.

If voting computers do not store any data about the vote's content and the barcodes are completely neutral and not somehow ordered, there will be no link between vote and voter.

Appendix II

Operational standards

I. Notification

36. Domestic legal provisions governing an e-election or e-referendum shall provide for clear timetables concerning all stages of the election or referendum, both before and after the election or referendum.

Clear procedures should be defined by the law as regards the use of ballot booklets.

The timeframes of the proposed system are similar to those already in use in traditional and e-voting procedures.

37. The period in which an electronic vote can be cast shall not begin before the notification of an election or a referendum. Particularly with regard to remote e-voting, the period shall be defined and made known to the public well in advance of the start of voting.

No specific provisions needed.

No specific provisions needed. The proposed scenario does not include advance voting.

38. The voters shall be informed, well in advance of the start of voting, in clear and simple language, of the way in which the e-voting will be organised, and any steps a voter may have to take in order to participate and vote.

Information about the procedure to be followed should be provided to the voter.

Detailed information could be sent to each voter and training sessions arranged in order to achieve this goal.

II. Voters

39. There shall be a voters' register which is regularly updated. The voter shall be able to check, as a minimum, the information which is held about him/her on the register, and request corrections.

No specific provisions needed.

No specific provisions needed.

40. The possibility of creating an electronic register and introducing a mechanism allowing online application for voter registration and, if applicable, for application to use e-voting, shall be considered. If participation in e-voting requires a separate application by the voter and/or additional steps, an electronic, and, where possible, interactive procedure shall be considered.

N. A.

—

41. In cases where there is an overlap between the period for voter registration and the voting period, provision for appropriate voter authentication shall be made.

N. A.

—

III. Candidates

42. The possibility of introducing online candidate nomination may be considered.

N. A.

—

43. A list of candidates that is generated and made available electronically shall also be publicly available by other means.

The Electoral Authorities publish the list of candidates and the layout of the voting screens and voting ballots prior to the elections.

Currently this data is sent to each voter so there is no reason to change the procedure for the new system.

IV. Voting

44. It is particularly important, where remote e-voting takes place while polling stations are open, that the system shall be so designed that it prevents any voter from voting more than once.

N. A.

—

45. Remote e-voting may start and/or end at an earlier time than the opening of any polling station. Remote e-voting shall not continue after the end of the voting period at polling stations.

N. A.

—

46. For every e-voting channel, support and guidance arrangements on voting procedures shall be set up for, and be available to, the voter. In the case of remote e-voting, such arrangements shall also be available through a different, widely available communication channel.

Can be achieved by means of adequate procedures during pre-voting stages, by supplying adequate information about the voting process.

It is feasible to arrange these information channels. The report includes specific mentions regarding, for instance, the instructions provided by the voting computer itself (pp. 39 and 47).

47. There shall be equality in the manner of presentation of all voting options on the device used for casting an electronic vote.

Similar to eVoting system currently in use.

The study foresees an equitable presentation of all candidates, and suggests that the layout should be similar to that used in paper ballot systems. However, due to technical limitations, all the individual candidates cannot be displayed together. Therefore, the list of candidates for a given party appears only after the voter has selected their preferred party on the first screen. The current e-voting system uses a similar layout. The Recommendation accepts this kind of solution.

Official members of the Administration and auditors have access to the configuration and installation steps (p. 13) in order to guarantee, among other issues, that no content is missing.

48. The electronic ballot by which an electronic vote is cast shall be free from any information about voting options, other than that strictly required for casting the vote. The e-voting system shall avoid the display of other messages that may influence the voters' choice.

Similar to eVoting system currently in use.

Secure computing settings should be set up to achieve this goal and prevent the voting computers from displaying inappropriate information to the voter. Control of these settings requires audit and certification mechanisms.

49. If it is decided that information about voting options will be accessible from the e-voting site, this information shall be presented with equality.

N. A.

This is not planned for because Belgian electoral law does not recognise this option, though it could be implemented if necessary.

50. Before casting a vote using a remote e-voting system, voters' attention shall be explicitly drawn to the fact that the e-election or e-referendum in which they are submitting their decision by electronic means is a real election or referendum. In case of tests, participants shall have their attention drawn explicitly to the fact that they are not participating in a real election or referendum and shall – when tests are continued at election times – at the same time be invited to cast their ballot by the voting channel(s) available for that purpose.

N. A.

The polling station layout must clearly indicate a binding and official election is underway.

51. A remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast.

N. A.

—

52. In a supervised environment, the information on the vote shall disappear from the visual, audio or tactile display used by the voter to cast the vote as soon as it has been cast. Where a paper proof of the electronic vote is provided to the voter at a polling station, the voter shall not be able to show it to any other person, or take this proof outside of the polling station.

Similar to the eVoting system currently in use. No paper proof remains with the voter. The voting computer produces a paper ballot of which the voter hides the human readable part before leaving the voting booth. The folded ballot booklet is inspected by the president of the polling station, and then inserted by the voter into the voting urn.

The voter will handle the ballot booklet like a traditional paper ballot. Secure computing settings should prevent the voting computers from displaying inappropriate information to the next voter.

V. Results

53. The e-voting system shall not allow the disclosure of the number of votes cast for any voting option until after the closure of the electronic ballot box. This information shall not be disclosed to the public until after the end of the voting period.

This can be achieved by means of adequate procedures during pre-voting, voting and post-voting stages, as well as through the general requirements.

The ballot box containing the booklets will be sealed according to traditional procedure. The electronic component however, introduces a new risk if developed in such a way as to be able to publish partial results. A voting computer, for example, could provide information about the votes already cast in its booth. Moreover, the file containing the scanned barcodes could provide the same information for the whole polling station. This situation can be avoided by adequate computer security measures that should be regularly verified and audited.

54. The e-voting system shall prevent processing information on votes cast within deliberately chosen sub-units that could reveal individual voters' choices.

See general requirements.

The proposed system includes the general electoral Belgian guidelines about aggregated tallies embracing several polling stations.

55. Any decoding required for the counting of the votes shall be carried out as soon as practicable after the closure of the voting period.

This can be achieved by means of adequate procedures during post-voting stages. The voting urns are collected at the end of the voting period on Election Day, and are assembled at the Scanning Centers. After assembling the urns of different polling stations, the urns are opened and emptied, and their content is mixed to destroy any chronological order that may have been the result of entering voting ballots one after the other in the individual voting urns.

The shuffled voting ballots are then electronically scanned. List enumerating the electronically scanned barcodes of each ballot booklet is then digitally signed by the voting official active at the Scanning Center, and sent to the Counting Center, where the decoding of the barcodes will take place.

—

56. When counting the votes, representatives of the competent electoral authority shall be able to participate in, and any observers able to observe, the count.

Belgian law stipulates that this should be done by a College of Experts and by party witnesses: no specific provisions needed.

Please see comments to Rec. article 23.

57. A record of the counting process of the electronic votes shall be kept, including information about the start and end of, and the persons involved in, the count.

Can be achieved by means of adequate procedures during post-voting stages.

—

58. In the event of any irregularity affecting the integrity of votes, the affected votes shall be recorded as such.

See also Recommendations n° 107 and 108: What is considered as authentic vote should be defined: the barcode; the human readable part, the whole ballot or it depends on the counting phase (electronic counting, manual counting).

A problem could occur if a ballot booklet is deemed invalid. However, the solution will consist in defining which of the two parts of the ballot booklets is given legal validity.

—

VI. Audit

59. The e-voting system shall be auditable.

The complete electronic voting system is auditable: (i) the voting computers run an open source operating system; (ii) the voting software is published once it has been certified by an external auditor; (iii) the voting configuration can be published after it has carefully been verified; (iv) the voting procedure and the procedure to initialize and manage the voting computers publicly available; (v) the mechanisms and procedures to count ballot booklets can be observed by independent observers; (vi) the voter can confirm that the human readable part of the ballot booklet corresponds with the votes cast by means of the voting computer in the voting booth; (vii) independent auditors may select a random number of randomly chosen ballot booklets to verify that the human readable part of the ballot booklets corresponds with the barcode. Also see general requirements.

—

60. The conclusions drawn from the audit process shall be applied in future elections and referendums.

The Recommendations by the College of Experts should be implemented in future elections.

College of Experts Recommendations may be taken on board by the electoral authorities, though their decisions are not automatically binding.

Appendix III Technical requirements

The design of an e-voting system shall be underpinned by a comprehensive assessment of the risks involved in the successful completion of the particular election or referendum. The e-voting system shall include the appropriate safeguards, based on this risk assessment, to manage the specific risks identified. Service failure or service degradation shall be kept within pre-defined limits.

A. Accessibility

61. Measures shall be taken to ensure that the relevant software and services can be used by all voters and, if necessary, provide access to alternative ways of voting.

Section 5.6.2.3 includes specific accessibility guidelines for voting systems with respect to Recommendation.

Though section 5.6.2.3 summarizes some of the key issues related to the accessibility of the e-voting system, it would be advisable to develop a more detailed overview of accessibility requirements.

62. Users shall be involved in the design of e-voting systems, particularly to identify constraints and test ease of use at each main stage of the development process.

Section 5.6.2.3 includes specific accessibility guidelines for voting systems which include the involvement of real end-users in the design process of the layout of the voting screens and the voting process.

Section 5.6.2.3 includes general requirements that would need further development and detail. Sections 5.6.1.5.1 and 11.5 also foresee field-testing of the voting system.

63. Users shall be supplied, whenever required and possible, with additional facilities, such as special interfaces or other equivalent resources, such as personal assistance. User facilities shall comply as much as possible with the guidelines set out in the Web Accessibility Initiative (WAI).

Section 5.6.2.3 includes specific accessibility guidelines for voting systems with respect to Recommendation.

There is no mention of the Web Accessibility Initiative (WAI) in section 5.6.2.3 which otherwise includes references to several similar projects. However, the Study does foresee personal assistance for disabled voters by trained staff and the provision of (ix), special facilities like adapted outputs –synthetic voice, large characters— (v) or full physical access to the polling station and to the voting booth (viii).

64. Consideration shall be given, when developing new products, to their compatibility with existing ones, including those using technologies designed to help people with disabilities.

The proposed improved paper-based voting system is a close relative to the currently used electronic voting system.

—

65. The presentation of the voting options shall be optimized for the voter.

Sections 5.6.1.5 and 5.6.2.3 include specific layout guidelines for voting systems.

—

B. Interoperability

66. Open standards shall be used to ensure that the various technical components or services of an e-voting system, possibly derived from a variety of sources, inter operate.

The operating system, voting software and configuration files depend on open standards. The hardware (voting computer display, pointing device, and printer) also uses open standards to provide its services, which protects against vendor-lock in.

All the components have a standardized profile. The source code and the configuration files will be published. It is not clear that the operating system will also be published, although the reports states that the software installed in the voting computers is open source (p. 13). It would also be worth clarifying if the term "voting computers" actually includes in these cases any electronic device involved in the process or only those installed in the voting booths.

67. At present, the Election Markup Language (EML) standard is such an open standard and in order to guarantee interoperability, EML shall be used whenever possible for e-election and e-referendum applications. The decision of when to adopt EML is a matter for member states. The EML standard valid at the time of adoption of this Recommendation, and supporting documentation are available on the Council of Europe website.

The configuration files of the voting software may be encoded using EML.

—

68. In cases which imply specific election or referendum data requirements, a localization procedure shall be used to accommodate these needs. This would allow for extending or restricting the information to be provided, whilst still remaining compatible with the generic version of EML. The recommended procedure is to use structured schema languages and pattern languages.

The configuration files of the voting software are localized to accommodate the needs of specific polling stations.

—

C. Systems operation

(for the central infrastructure and clients in controlled environments)

69. The competent electoral authorities shall publish an official list of the software used in an e-election or e-referendum. Member states may exclude from this list data protection software for security reasons. At the very least it shall indicate the software used, the versions, its date of installation and a brief description. A procedure shall be established for regularly installing updated versions and corrections of the relevant protection software. It shall be possible to check the state of protection of the voting equipment at any time.

The software used with the voting computers can be made public prior to the elections. Only the configuration files that contain the signing keys of the polling stations shall be kept secret. All other configuration files can be made public without restriction.

The description of the life-cycle of the voting computer system includes the patching and updating of the voting computer and its operating system prior to the installation of the voting software. At the end of the election period, the voting computer is deactivated.

The software is open source and should include detailed specifications (p. 129). The system administrator is responsible for patching and updating.

It is worth noting that the Recommendation's explanatory memorandum states that the results of the certification should be made available to political parties. This is not the case under the current Belgian system and the point is not referred to in the study.

Although there are computerised self-tests and audit checks that can verify the equipment at any time, a 100% guarantee that the voting computers are actually running the certified software correctly seems almost impossible. This is a challenge for any e-voting system given the inherent problems of relying on the computer testing itself, external seals which could be tampered with and on digital signatures which require the proper custody of keys. A thorough risk assessment should be undertaken.

70. Those responsible for operating the equipment shall draw up a contingency procedure. Any backup system shall conform to the same standards and requirements as the original system.

The administration is responsible for the management of the voting computers.

—

71. Sufficient backup arrangements shall be in place and be permanently available to ensure that voting proceeds smoothly. The staff concerned shall be ready to intervene rapidly according to a procedure drawn up by the competent electoral authorities.

All voting computers of a polling station are interchangeable. The voting computers of a polling station use the configuration file(s) which is (are) specific to the boot credential of the president of the polling station. This means that voting computers of another polling station, or spare voting computers, can be used and quickly activated whenever necessary.

The other computer devices (e.g., scanners, decodes, barcode readers) are also interchangeable.

72. Those responsible for the equipment shall use special procedures to ensure that during the polling period the voting equipment and its use satisfy requirements. The backup services shall be regularly supplied with monitoring protocols.

Strict access control mechanisms are put in place so that only authorized people can use the voting computers' services.

See comments to Recommendation article 69.

73. Before each election or referendum, the equipment shall be checked and approved in accordance with a protocol drawn up by the competent electoral authorities. The equipment shall be checked to ensure that it complies with technical specifications. The findings shall be submitted to the competent electoral authorities.

The life-cycle description of the voting computers includes the initialization of the voting computers prior to the Election Day, and the deactivation after the voting period on Election Day.

Disabling unnecessary services or hardware of the voting computers is part of the responsibilities of the system administrator of the voting computers.

Following the explanatory memorandum, a normal check is carried out when there is no modification of components but, in the second case, the task should be assigned to an external entity. The system administrator cannot be considered as an external body.

74. All technical operations shall be subject to a formal control procedure. Any substantial changes to key equipment shall be notified.

The life-cycle description of the voting computer includes the certification of the software. Proceeding from one stage to another in the life cycle is subject to successful completion of the previous.

A step-by-step procedure has no relationship with the content of this Recommendation that actually requires a formal control procedure within each step. The Study includes some provisions, mainly in the last section – general requirements— that should be detailed in a formal and detailed operational protocol.

75. Key e-election or e-referendum equipment shall be located in a secure area and that area shall, throughout the election or referendum period, be guarded against interference of any sort and from any person. During the election or referendum period a physical disaster recovery plan shall be in place. Furthermore, any data retained after the election or referendum period shall be stored securely.

In between election periods, the voting computers are stored in a secure environment, or returned to their supplier. At the end of the election period, all voting computers are deactivated, i.e., their storage medium is reset in its original state by securely wiping out all information.

Currently the equipment is stored by the municipalities themselves without any nationwide guidelines on procedure; the report only mentions the necessity of secure environments. A detailed protocol could help each stakeholder to properly perform this task.

76. Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment shall immediately inform the competent electoral authorities, who will take the necessary steps to mitigate the effects of the incident. The level of incident which shall be reported shall be specified in advance by the electoral authorities.

This can be achieved by means of adequate procedures during pre-voting, voting, and post-voting stages, as well as through the general requirements.

The proposed system can easily adopt these contingency measures.

D. Security

I. General requirements

(referring to pre-voting, voting, and post-voting stages)

77. Technical and organisational measures shall be taken to ensure that no data will be permanently lost in the event of a breakdown or a fault affecting the e-voting system.

None of the voting computers contains critical information that could endanger the whole electronic voting system. Permanent loss of a voting computer has no impact on the operation of other voting computers.

Note, however, that a fraudster who obtains a voting computer could extract the private signing key(s) of the polling station(s) that are stored in the respective configuration files.

It should be noted that a fraudster could be an insider. A more detailed evaluation of what could happen if somebody obtains the signing keys would be advisable.

78. The e-voting system shall maintain the privacy of individuals. Confidentiality of voters' registers stored in or communicated by the e-voting system shall be maintained.

There is no link between the identity of a voter and the paper trail which represents the voter's choice. If one would wish to counter all suspicion with respect to possibly hidden information in the barcode, the Administration should choose to not encrypt nor encode the barcode of the voter's paper ballot.

If the voting computer does not store any information about the content of the vote and if the barcodes are neutral and not numbered, there can be no link between the vote and the citizen.

79. The e-voting system shall perform regular checks to ensure that its components operate in accordance with its technical specifications and that its services are available.

The lifecycle of the voting computer includes self-tests of a voting computer whenever the computer is activated.

Self-tests are good and necessary measures, but it should be noted that a machine that had been tampered with could probably generate correct self-tests.

80. The e-voting system shall restrict access to its services, depending on the user identity or the user role, to those services explicitly assigned to this user or role. User authentication shall be effective before any action can be carried out.

Strict access control mechanisms are put in place to avoid unauthorized access to the voting computer and to its functionalities. The system administrator of the voting computers is responsible to install, update and patch the operating system of the voting computers to avoid circumvention of the user authentication mechanisms.

The system includes several access limitations, primarily during critical tasks.

81. The e-voting system shall protect authentication data so that unauthorized entities cannot misuse, intercept, modify, or otherwise gain knowledge of all or some of this data. In uncontrolled environments, authentication based on cryptographic mechanisms is advisable.

The privileged information in a voting computer's configuration file is encrypted using a cryptographic key that depends on the boot credential of the president of the polling station, which guarantees that unauthorized access is prevented as long as the boot credentials are kept secret.

Procedural arrangements that guarantee the chain of custody become critical.

82. Identification of voters and candidates in a way that they can unmistakably be distinguished from other persons (unique identification) shall be ensured.

The president of the polling station has an authentic list of eligible voters. Given a person's identification token (e.g., identity card), the president of the polling station can confirm the identity of that person, and that he is an eligible voter (or not).

Voters are identified in a traditional way checking a paper poll book.

83. E-voting systems shall generate reliable and sufficiently detailed observation data so that election observation can be carried out. The time at which an event generated observation data shall be reliably determinable. The authenticity, availability and integrity of the data shall be maintained.

Not applicable: the voting computers do not log any information.

The proposed system generates enough data to be duly observed, e.g., the human readable part of the booklets, the lists of scanned and decoded barcodes. Its authenticity, availability and integrity could be maintained by a normal safekeeping of the ballot box and the publication of the barcodes' list and the partial results.

84. The e-voting system shall maintain reliable synchronized time sources. The accuracy of the time source shall be sufficient to maintain time marks for audit trails and observations data, as well as for maintaining the time limits for registration, nomination, voting, or counting.

Not applicable: the voting computers operate in a standalone environment without any means to synchronize their system clocks.

—

85. Electoral authorities have overall responsibility for compliance with these security requirements, which shall be assessed by independent bodies.

Independent auditors need to verify that the correct procedures are correctly executed.

The current College of Experts or the private certification companies may easily be considered as independent bodies to carry out this task.

II. Requirements in pre-voting stages (and for data communicated to the voting stage)

86. The authenticity, availability and integrity of the voters' registers and lists of candidates shall be maintained. The source of the data shall be authenticated. Provisions on data protection shall be respected.

The administration takes care of the compilation of these lists.

The compilation of both lists is carried out by traditional means. Voter identification in each polling station remains computerless. The integrity of the list of candidates once uploaded to the voting computer relies on proper procedural guarantees and computer settings.

87. The fact that candidate nomination and, if required, the decision of the candidate and/or the competent electoral authority to accept a nomination has happened within the prescribed time limits shall be ascertainable.

The administration is responsible for this Recommendation.

Candidates' nominations and their acceptance are carried out without electronic means.

88. The fact that voter registration has happened within the prescribed time limits shall be ascertainable.

The administration is responsible for this Recommendation

—

**III. Requirements in the voting stage
(and for data communicated during post-election stages)**

89. The integrity of data communicated from the pre-voting stage (e.g. Voters' registers and lists of candidates) shall be maintained. Data-origin authentication shall be carried out.

Strict user access control mechanisms are enforced when accessing the voting computers. The integrity of the configuration files is verified whenever the voting computer performs its self-test.

Polling station staff should also carry out random verifications before opening the polling station that the configuration files are correct by checking the content of the candidates' list and other key data. Other procedural guarantees would also be useful because the computer's self-tests might not be enough. Voters' registers are manual.

90. It shall be ensured that the e-voting system presents an authentic ballot to the voter. In the case of remote e-voting, the voter shall be informed about the means to verify that a connection to the official server has been established and that the authentic ballot has been presented.

The configuration files loaded into the voting computers are prepared by authorized personnel in a secure environment. The voting software is initialized in such a way that the voting computer truly displays the lists of candidates taking part in the election corresponding to the polling station in which the voter has been authenticated.

See comments to Recommendation articles 69 and 89.

91. The fact that a vote has been cast within the prescribed time limits shall be ascertainable.

This may be specified in the configuration file of the voting computer.

—

92. Sufficient means shall be provided to ensure that the systems that are used by the voters to cast the vote can be protected against influence that could modify the vote.

There is no occasion for exerting influence during the voting process. A voter is alone in the voting booth (except for specific cases of voters with disabilities). Once he leaves the voting booth, his ballot must be folded and closed so that the votes are not visible (if he fails to do so, he will be asked to vote again by the president).

This Recommendation is particularly relevant for remote voting, but it can also apply here because a voter could leave inappropriate information in the booth for the next voter to see. This risk also exists in traditional paper ballot voting.

93. Residual information holding the voter's decision or the display of the voter's choice shall be destroyed after the vote has been cast. In the case of remote e-voting, the voter shall be provided with information on how to delete, where that is possible, traces of the vote from the device used to cast the vote.

The voting computer's software does not keep any state information, i.e., it does not memorise the voter's choice.

"Software shall produce time-stamped audit records of all operations executed during all phases before, during, and after an election" (p. 130) / "Audit records shall not contain information about the contents of a voter nor about the identity of a voter" (p. 131) / It seems therefore that the software somehow stores a track record. To prevent any connection being made between vote and voter, a special configuration should be set up to avoid the use of back buttons by the following voter.

94. The e-voting system shall at first ensure that a user who tries to vote is eligible to vote. The e-voting system shall authenticate the voter and shall ensure that only the appropriate number of votes per voter is cast and stored in the electronic ballot box.

The president of the polling station verifies the identity of the voter. Only if he is an eligible voter, the voter receives a voting token with which the voting computer can be activated. Not valid voting token = no possibility to cast a vote.

The Returning officer of the polling station will check that the citizen is entitled to vote and that they are only casting one vote, that is, one booklet. Secure computer settings should prevent multiple votes from being encoded in the same barcode.

95. The e-voting system shall ensure that the voter's choice is accurately represented in the vote and that the sealed vote enters the electronic ballot box.

The voting computer produces a paper trail consisting of a paper ballot with two parts: a human readable part and a barcode. The voter has to verify and confirm that the choice he cast with the voting computer corresponds with the human readable part.

Independent auditors have to verify that the barcode of randomly selected paper trails correspond with their human readable part.

The voter is also given the possibility to scan the barcode of his voting ballot while he is in the voting booth.

—

96. After the end of the e-voting period, no voter shall be allowed to gain access to the e-voting system. However, the acceptance of electronic votes into the electronic ballot box shall remain open for a sufficient period of time to allow for any delays in the passing of messages over the e-voting channel.

At the end of the voting period on Election Day, all voting computers are deactivated. During the deactivation of a voting computer, the voting computer's persistent storage medium is reset to its initial state.

The staff of each polling station will decide when the machines should be switched off, allowing first for those who arrived towards the end of the voting period to cast their votes. Voting computers should not provide booklets without the voting token that is given by the staff.

IV. Requirements in post-voting stages

97. The integrity of data communicated during the voting stage (e.g. Votes, voters' registers, lists of candidates) shall be maintained. Data-origin authentication shall be carried out.

The information sent from the Scanning Center(s) to their corresponding Decoding and Counting Center, and from the Counting Center(s) to their respective First Totalisation Center, and up to the Final Totalisation Center is digitally signed using an electronic identity card of the person in charge of the respective Centre.

—

98. The counting process shall accurately count the votes. The counting of votes shall be reproducible.

Official statements (PVs) are issued to report on the different stages of the voting process: from an empty voting urn to the Final Totalisation Center.

The counting can be reproduced by other technological means such as another barcode reader.

99. The e-voting system shall maintain the availability and integrity of the electronic ballot box and the output of the counting process as long as required.

This can easily be enforced using correct procedures with respect to the storage and processing of voting ballots.

It is easy to enforce with proper operational measures but the guarantee should include the voting ballots as well as other strategic components, like the files containing partial and final results.

E. Audit

I. General

100. The audit system shall be designed and implemented as part of the e-voting system. Audit facilities shall be present on different levels of the system: logical, technical and application.

The procedures of the proposed electronic voting system clearly specify the roles and activities of the different auditors that are active before, during and after the Election Day. The election software shall be designed according to specifications which will include provisions for auditing facilities.

The proposed system is auditable and the report includes independent auditors as key players (pp. 21-22) in its development. However, a further examination is required to determine who appoints the auditors and the precise consequences their decisions might have.

101. End-to-end auditing of an e-voting system shall include recording, providing monitoring facilities and providing verification facilities. Audit systems with the features set out in sections II – V below shall therefore be used to meet these requirements.

Since the proposed system is not an end-to-end automated system, this requirement is not fully applicable. Official statements (PVs) report on the monitoring activities of the independent auditors.

—

II. Recording

102. The audit system shall be open and comprehensive, and actively report on potential issues and threats.

The audit procedures are open by design.

The Recommendation also emphasises that the audit system should be comprehensive and active in its reports and not simply 'open'. To these ends, a further investigation of methods and organisation would be beneficial.

103. The audit system shall record times, events and actions, including:

- a. all voting-related information, including the number of eligible voters, the number of votes cast, the number of invalid votes, the counts and recounts, etc.;**
- b. any attacks on the operation of the e-voting system and its communications infrastructure;**
- c. system failures, malfunctions and other threats to the system.**

The auditors have to include this information in their official statements (PVs).

—

III. Monitoring

104. The audit system shall provide the ability to oversee the election or referendum and to verify that the results and procedures are in accordance with the applicable legal provisions.

The audit mechanisms described in the proposed system permit the verification of the elections results, and permit the audit of the whole Election by randomly selecting voting ballots and verifying their barcode and human readable text match.

This audit is implemented to verify both results and procedures. The first ones could be audited by the proposed random selection, matching results and human readable texts (see above "key issues"), though this mechanism does not include procedures and other components. For instance, the proposed audit could reveal a mistake during the tally due to a misscanned ballot booklet, but it would not detect the poor implementation of previous stages (e. g., a weak custody chain of the boot credentials).

105. Disclosure of the audit information to unauthorized persons shall be prevented.

The disclosure of audit information shall proceed according to legal provisions.

This can be easily organised through a list of those people entitled to receive audit information and a detailed agreement of confidentiality with all the stakeholders. The main problem here is not avoiding undue disclosure, but rather how to decide who should be authorised and whether this list is sufficiently representative from a democratic point of view.

106. The audit system shall maintain voter anonymity at all times.

There is no link between a voter and a voting ballot. This guarantees that even the auditors will not be able to restore this link.

If there is no direct or indirect link between voter and voting ballot (see above), the auditors will be unable to infringe anonymity.

IV. Verifiability

107. The audit system shall provide the ability to cross-check and verify the correct operation of the e-voting system and the accuracy of the result, to detect voter fraud and to prove that all counted votes are authentic and that all votes have been counted.

The audit procedures include that the auditors have to cross-check the partial election results with the number of voting urns and the respective ballots.

The proposed cross-check does not itself prove that all counted votes are authentic or that all votes have been counted. It is only a means of checking the total sum of votes and it should be complemented by other audit mechanisms which check that there have been no votes added or removed after the end of the voting period.

Moreover, the Recommendation mentions other issues not directly related to the results like the correct operation of the e-voting system.

108. The audit system shall provide the ability to verify that an e-election or e-referendum has complied with the applicable legal provisions, the aim being to verify that the results are an accurate representation of the authentic votes.

Independent certification of the operating system, the voting software, and the configuration files has to take place prior to the elections to confirm that they meet the relevant legal requirements.

A certification is not an audit and consequently, they are covered in two different sections of the Council of Europe's Recommendation: audit (5.7.2.4.5) and certification (5.7.2.4.6). The main difference is that audit mechanisms are deployed before, during and after the voting period. Certification on the other hand is not a dynamic procedure: It only analyses devices prior to the election and then issues a report. Therefore, it seems prudent that this matter be looked into further.

V. Other

109. The audit system shall be protected against attacks which may corrupt, alter or lose records in the audit system.

The official statements (PVs) should be digitally signed to prevent undetected modifications of their content.

Official statements by the auditors themselves are only a part of the audit system. The audit system also includes the internal structure of the machines in which, besides the voting operations, a specific software gathers information that will be use to assess these operations.

110. Member states shall take adequate steps to ensure that the confidentiality of any information obtained by any person while carrying out auditing functions is guaranteed.

This requirement must be enforced using organisational means.

The proposed e-voting system accepts organisational means required to achieve this confidentiality goal.

F. Certification

111. Member states shall introduce certification processes that allow for any ICT (Information and Communication Technology) component to be tested and certified as being in conformity with the technical requirements described in this Recommendation.

The specified procedures include the necessary certifications of the voting hardware, software, procedures and configuration.

This is logical for any technical product. Though the study briefly mentions certification the subject requires further analysis (see above).

112. In order to enhance international co-operation and avoid duplication of work, member states shall consider whether their respective agencies shall join, if they have not done so already, relevant international mutual recognition arrangements such as the European Co-operation for Accreditation (EA), the International Laboratory Accreditation Co-operation (ILAC), the International Accreditation Forum (IAF) and other bodies of a similar nature.

The proposed system can be exported to foreign countries which want to boost their citizen's confidence in electronic voting systems.

The layout of the Belgian certification procedures could take into account the outcomes of other countries like, for instance, France, the Netherlands and the United States of America.