

**Directorate General of Political Affairs
Project "Good Governance in the Information Society"**

**Direction Générale des Affaires Politiques
Projet « Bonne gouvernance dans la société de l'Information »**



FFD (2008) 11 E

Strasbourg, 7 October 2008

**Meeting to review developments in the field of e-voting since the adoption of
Recommendation Rec(2004)11 of the Committee of Ministers to member states
on legal, operational and technical standards for e-voting**

**Municipal Congress Centre of the City of Madrid
16 October 2008**

**Organised in the framework of the 2008 session of the Council of Europe's Forum
for the Future of Democracy on the theme of e-democracy (15-17 October 2008)**

Additional information on e-voting from the Netherlands

- 1. Voting with confidence**
- 2. Letter of the State Secretary for the Interior and Kingdom Relations to the
Speaker of the House of Representatives of the States General**
- 3. Tempest Report**

Voting with confidence

Election Process Advisory Commission

27 September 2007

Credits

Published by:

Election Process Advisory Commission (Adviescommissie inrichting verkiezingsproces), c/o
Ministry of the Interior and Kingdom Relations, PO Box 20011, 2500 EA The Hague,
info@minbzk.nl www.minbzk.nl www.verkiezingsproces.nl (until 1 September 2007)

Contents

Summary	5
1. Introduction	10
1.1 Background	10
1.2 Composition	10
1.3 Remit	11
1.4 Modus operandi	12
2. The principles of the election process	13
2.1 Introduction	13
2.2 The international and national legal framework	13
2.3 Striking a balance	16
3. Comparison of voting methods	19
3.1 Introduction	19
3.2 Voting using paper ballots at polling stations	19
3.3 Electronic voting at polling stations	20
3.4 Postal voting for Dutch citizens eligible to vote from abroad	21
3.5 Proxy voting	23
3.6 Internet and telephone voting	23
3.7 Discussion	25
4. Voting in the future	26
4.1.1 Voting at polling stations	26
4.1.2 Discussion	30
4.2.1 Electromagnetic radiation	33
4.2.2 Discussion	34
4.3.1 Voting at any polling station	36
4.3.2 Discussion	38
5. Voters with impairments	40
5.1 Introduction	40
5.2 Discussion	41
6. Proxy voting	43
6.1 Introduction	43
6.2 Discussion	44
7. Voters abroad	46
7.1 Introduction	46
7.2 Experience so far with remote voting	46
7.3 Discussion	48

8.	Voting for the European Parliament	52
	8.1 Introduction	52
	8.2 Discussion	53
9.	Duties and responsibilities in the election process	56
	9.1 Introduction	56
	9.2 Discussion	57
10.	Miscellaneous topics	60
	10.1 Introduction	60
	10.2 The answers to the questions in the Commission's remit	60
	10.3 Answers to other questions	61
	10.3.1 The Swedish messenger system	61
	10.3.2 Elections Act terminology	63
11.	Financial consequences	65
	11.1 Introduction	65
	11.2 Electronic voting and paper voting	66
	11.3 Voting at any polling station outside the voter's municipality	68
12.	Conclusions and Recommendations	70
	12.1 Conclusions	70
	12.2 Recommendations	71
	List of acronyms and abbreviations	74
	Appendices	75
	Glossary of polling card terms	77

Summary

The Commission considers that the election process in the Netherlands should safeguard the following principles:

- **Transparency**
The election process should be organized in such a way that the structure and organization is clear, so that everyone in principle can understand it. There must be no secrets in the election process: questions must be able to be answered, and the answers must be verifiable.
- **Verifiability**
The election process should be objectively verifiable. The verification tools may differ, depending on the method of voting that is decided upon.
- **Fairness**
The election process should operate in a proper manner, and the results must not be capable of being influenced other than by the casting of lawful votes.
- **Eligibility to vote**
Only persons eligible to vote must be allowed to take part in the election.
- **Free suffrage**
Every elector must be able to choose how to vote in complete freedom, free from influence.
- **Secret suffrage**
It must be impossible to connect the identity of a person casting a vote to the vote cast. The process should be organized in such a way that it is impossible to make a voter indicate how he or she voted.
- **Equal suffrage**
Each voter, given the Dutch election system, must be allowed to cast only one vote in each election, which must be counted precisely once.
- **Accessibility**
Voters should be enabled as far as possible to participate directly in the election process. If this is impossible, there must be a way of taking part indirectly, i.e. by proxy.

These principles are to some extent enshrined in the Dutch Constitution and laid down in international and European treaties and recommendations of e.g. the Organization for Security and Co-operation in Europe and the Council of Europe. Dutch law and regulations must provide these safeguards. The Commission has examined the methods of voting used at present in the light of them, namely:

- Voting using paper ballots at polling stations
- Electronic voting at polling stations
- Postal voting
- Internet voting
- Voting by telephone
- Voting by proxy

The report indicates how well the principles are safeguarded with these methods of voting, explicitly discussing the dilemma that there is no method of voting that provides 100% safeguards. In the end it is a question of striking a balance between the principles: feasibility and

cost are factors here, as is the point that the election process must be flexible enough to respond to new developments.

Having weighed up the various principles, the Commission concludes that voting at polling stations should be the main method of voting in the Netherlands. Other methods, such as Internet, telephone and postal voting, do not provide the same degree of safeguards as voting at polling stations, so the report does not generally recommend them. The Commission also takes the view that the method of voting at polling stations in the Netherlands should be standardized, i.e. the same in every municipality.

Voting using paper ballots at polling stations is the preferred option on the grounds of transparency and verifiability. Given the problems encountered in practice with the manual counting of these ballots, however, the Commission also investigated whether a method of electronic voting is conceivable that provides equal safeguards. The Commission takes the view that this is feasible, provided it produces a paper ballot that can be checked by the voter. The report describes two methods of voting by electronic means at polling stations and electronic counting of the votes cast:

- A *ballot printer* on which the voter makes his or her choice: this produces a paper ballot that is deposited in a ballot box and is counted electronically, when the ballot closes, by a *vote counter*.
- An electronic voting device with a memory and an additional paper trail for verification purposes.

The two methods differ substantially. The Commission only recommends introducing *ballot printers* with electronic *vote counters*, because of the conceptual clarity of the system and the unambiguous results it produces. Although counting can be carried out more quickly using voting devices with a paper trail, by using the device to do the counting, this advantage is outweighed by the disadvantages, as it still means relying on the software correctly storing the votes cast. In the case of a *ballot printer* choosing how to vote is completely separate from the casting of the vote, so there is no need to rely on the vote being stored correctly. A count by an electronic *vote counter* is estimated to take 15 to 30 minutes at each polling station.

The Commission also noted that there is a method using pre-printed paper ballots upon which voters mark their choice with a pen or pencil, and this is then read by a scanner and counted.

A system of this kind was tried in the United Kingdom just recently. The Electoral Commission produced a report on it in August 2007, which indicated that there were a number of problems. Voting using optical scanning systems takes place on a fairly large scale in the United States of America. Nine states use this method exclusively. Scanning systems where voters insert their ballot papers in a ballot box with a built-in scanner produce 0.7% invalid votes in those states. Nevertheless, as with all 100% electronic systems, optical scanning systems have also demonstrated vulnerabilities that might make it possible to manipulate the results. California has wholly or partly withdrawn approval from all the suppliers of these systems.

The ballot papers used and scanned in the United States and the United Kingdom are much smaller than those used in the Netherlands. Because of the large number and length of the lists

of candidates, Dutch ballot papers need to be of a size that does not fit in standard scanners. Splitting the papers up into separate pages, with voters only using the page on which they cast their votes, would create the risk of the other pages being used to cast fraudulent votes. Scanning ballot papers is therefore not really feasible in the Netherlands, and the Commission does not recommend this method.

In recent years there have been experiments with voting at any polling station within the voter's municipality under the Remote Electronic Voting (Experiments) Act.¹ The evaluations showed that both municipalities and voters were enthusiastic about the possibility of voting at other than a designated polling station. Given the need for the election process to be accessible, the Commission takes the view that voting at any polling station should be introduced in all municipalities. Although the results of the experiments were overwhelmingly positive, some new vulnerabilities came to light as regards protecting voting passes against forgery or counterfeiting and establishing that the person using a voting pass actually is the elector whose name is stated on the pass. Both these vulnerabilities need to be dealt with before it is decided to introduce voting at any polling station. Voting pass security can be improved by incorporating authenticity features. More reliable identification can be achieved by requiring users of voting passes to identify themselves when voting. Since the introduction of the Compulsory Identification Act everyone in the Netherlands over the age of 14 is required to hold a valid identity document and carry it with them at all times.² All electors will therefore have an identity document on their person when they go to vote and will be able to produce it.

The Ministry of the Interior and Kingdom Relations has long had the intention of making it possible not only to vote at any polling station in all municipalities but also to extend the principle so that in any election a voter can vote in the electoral district in which he is eligible to vote at any polling station in the Netherlands. Introducing this would have major consequences. First, every polling station would need to have the complete national register of cancelled voting passes (containing the serial numbers of voting passes that are invalid, for instance because a replacement card has been issued). The register would have to be compiled very quickly (in the space of two days) and distributed to all polling stations before the start of the election. In principle it could be in paper form, but to avoid errors and speed up the process during the election it would be advisable to use an electronic version. It does not need to be on-line, as the voting pass is collected by the polling station committee³ when the vote is cast, so the voter cannot go and vote again at another polling station. When the votes are counted the polling station committee would have to separate the votes cast into the various districts. This would be easy to do if the count is performed electronically, as recommended by the Commission. The counts would then have to be distributed to the principal polling stations where they 'belong'. To achieve this the Minister of the Interior and Kingdom Relations would need to create a central facility (distribution platform) to which the polling station committees would send the counts electronically. The central facility would also publish the counts of votes cast at each polling station on the Internet, thus enabling anyone who is interested to check the count. The distribution platform would pass on the results received directly (electronically) to the principal

¹ Act of 11 December 2003.

² This obligation has been in force since 1 January 2005.

³ For the terms 'polling station committee', 'principal electoral (district) committee' and 'Central Electoral Committee' see OSCE/ODIHR Election Assessment Mission Report, 12 March 2007, Chapter V A, pp. 10 and 11.

electoral committee³ concerned. If it is decided to introduce the option of voting at any polling station in the Netherlands in all elections it will not be possible to use pre-printed paper ballots.

The Commission recommends introducing voting at any polling station in all municipalities as the first step. The second step, the national introduction of voting at any polling station, should be taken later on, once all the authorities responsible for organizing elections and the public are accustomed to the new voting method at polling stations.

For certain groups of people, namely Dutch citizens living abroad or away from the Netherlands on account of their work or business or that of their spouse, registered partner, partner or parent, and people unable to vote at a polling station because of a physical impairment, other methods of voting than voting at a polling station need to be provided. This is necessary because they will otherwise be excluded from one of their most basic civil rights or completely reliant on proxy voting. In the case of these groups the Commission considers that access to elections outweighs the principles of transparency and free suffrage.

For Dutch citizens abroad postal voting is currently the regular method of voting. The Ministry of the Interior and Kingdom Relations experimented with Internet voting for this group in 2004 and 2006, and this was found to improve access. A large majority of these voters explicitly wish to vote using the Internet. The Commission therefore recommends making Internet voting the regular voting method for them. Postal voting should however be retained for the time being for those Dutch citizens who do not have Internet access or are unable or unwilling to use it.

Access for this group is substantially affected by the registration procedure, and the one used at present is cumbersome and arouses antagonism. The Commission therefore recommends that it be improved as soon as possible. In the longer term registration for each election could be dropped with the advent of the Register of Non-Residents, provided all non-resident Dutch citizens are registered in it.

As regards the physically impaired, the Commission concurs with the opinion of the Council for the Disabled and Chronically Ill, the Disability in the Community Task Force and Viziris, that greater efforts need to be made to allow this group of citizens to vote independently. This can be achieved at polling stations by improving physical access to them and equipping the electronic voting equipment with audio facilities. Anyone who is demonstrably unable to visit a polling station or to operate the voting equipment there should not be entirely dependent on proxy voting. The Commission agrees with the Council for the Disabled and Chronically Ill, the Disability in the Community Task Force and Viziris that telephone voting should be made available to this group.

The Netherlands has long had proxy voting. From time to time this attracts criticism internationally, e.g. from the observation missions of the Organization for Security and Co-operation in Europe. The criticism is directed in particular at the risks proxy voting entails to the principles of equal and secret suffrage. The Commission takes the view that proxy voting is well established in the Netherlands and should be retained. The risk of proxy votes being misused by intercepting voter registration cards or voting passes needs to be reduced. This can be done by means of regulations requiring anyone appointed to vote on behalf of another person to produce

a copy of a valid identity document of that person. This would enable the polling station committee to compare the two signatures if necessary.

The Commission looked in depth at the way in which duties and responsibilities for the election process are allocated. This is generally satisfactory, but there are two areas that have not been adequately provided for, if at all: the laying-down of requirements for equipment used in ballots, the enforcement of these requirements and the security and management of the equipment are not properly regulated. This responsibility should rest overall with central government, specifically the Minister of the Interior and Kingdom Relations, and should be enshrined in the law and regulations. This is also the case with the new duties arising from the Commission's recommendations on voting at any polling station and Internet and telephone voting. In view of the government's standpoint on the report of the Voting Machines Decision-Making Commission, the logical course is for these to be assigned to the Personal Records and Travel Documents Agency.

The transparency and verifiability of the election process also need to be improved. This can be achieved by subjecting the preparations for, and conduct of, every election to an audit, the aim being:

- to gain an objective idea of any incidents and errors relevant to the results when these are being determined by the Central Electoral Committee,³ and
- to learn lessons for future elections.

The election data (e.g. the official reports) should also be kept, and released for academic research after a specified period. The Commission takes the view, incidentally, that a new organization is not needed to carry out the audits: responsibility for auditing municipal council and provincial council elections should be assigned to the Minister of the Interior and Kingdom Relations, and for auditing general elections and European Parliamentary elections to the House of Representatives. The bodies carrying out the audits should be independent and the findings disclosed publicly: this must be enshrined in the law and regulations.

1. Introduction

1.1 Background

Before the general election on 22 November 2007 the question arose of whether there are adequate safeguards, when using voting machines or voting computers of the kind used in elections in the Netherlands for some years now, that the votes cast by voters using these devices are recorded and counted absolutely correctly and that the ballot is secret. The ensuing debate led the then Minister of Governmental Reform and Kingdom Relations, A. Nicolaï, to decide in December 2006 to set up two external commissions. The first of these was tasked with examining how decisions on the approval of voting machines had been made in the past (up to and including the 7 March 2007 elections) and what lessons the Ministry of the Interior and Kingdom Relations could learn from them. This body, the Voting Machines Decision-Making Commission, was set up on 19 December 2006 and published its report on 16 April 2007.

The second external commission, the Election Process Advisory Commission, was tasked with examining the current organization of the election process and making proposals for improvements and changes where necessary. The Commission was asked to address a number of questions, which were included in the establishing order.⁴ This expressly stipulated that it was not part of its remit to make recommendations on the Dutch electoral system.

1.2 Composition

The Commission started work on 18 January 2007, on the basis of a draft establishing decree, with the following composition:

- F. Korthals Altes, Honorary Minister, Chairman and member
- Prof. J.M. Barendrecht, Professor of Private Law at the University of Tilburg
- Mrs A.Th.B. Bijleveld-Schouten, Mayor of the Municipality of Hof van Twente
- Prof. B.P.F. Jacobs, Professor of Computer Security at Radboud University, Nijmegen and Eindhoven University of Technology
- J.C. de Jager, Director of Spectra Vision, Rotterdam
- M.J.C. van der Wel MBA, Business Development EMEA Manager (Fox-IT), Delft

The composition of the Commission was changed as a result of the formation of the fourth Balkenende government, in which Mrs Bijleveld-Schouten and Mr De Jager were appointed State Secretaries. To fill the resulting vacancies the State Secretary for the Interior and Kingdom Relations appointed C. Meesters, Director of Public Affairs, Municipality of Rotterdam and Chairman of the Nederlandse Vereniging van Burgerzaken (the association of organizations concerned with municipal documentary services to citizens), as a member of the Commission in February 2007. The establishing decree was dated 6 April 2007 (Appendix 1).

⁴ Appendix 1.

The Commission was assisted by Mrs M. Gonzalez, Programme Manager at the Ministry of the Interior and Kingdom Relations, as Secretary, and Mrs D.E.G.H. Laurent as Deputy Secretary. The Commission gained a good deal of valuable information from the knowledge and experience of its Secretary, and the Secretariat owes her a substantial debt of gratitude for her efficient and appropriate assistance.

1.3 Remit

The Commission's remit⁵ was to examine the election process and make proposals to improve or change it in line with the principles of secret, free, reliable, practical and transparent elections that are equally accessible to everyone. It was expressly stipulated that the remit did not include the electoral system or the position of the political parties.

The remit was set out in detail in the following questions, which the Commission was required to answer in any event:

- What role does IT play in the various stages of the election process (from the preparations for nominations to the appointment of new members to the representative body)?
- Which of these stages are in need of review in the light of new technologies and from the point of view of the electorate and the authorities?
- Is responsibility for organizing the election process correctly allocated (the relationship between central and local government, the relationship between polling station committees, principal electoral district committees and the Central Electoral Committee), and what should the relationship be between the private sector and government as regards the use of aids (voting machines and election results computation systems)?
- Is there adequate supervision of the proper conduct of the election process, who should supervise it and what enforcement powers should they have?
- What structural risks are associated with the current voting machines/electronic voting and pencil voting?
- Are there any alternatives conceivable to the current method of casting votes, e.g. non-place-dependent voting using the Internet?
- How do these alternatives compare as regards reliability, safeguarding the principle of secret suffrage and permitting recounts?
- Which is preferable: diversity (spreading the risk) or standardization (verification)?
- What is the relationship between the rapidity of technological development and the election process (could today's watertight solution be hacked into tomorrow)?
- To what extent do election aids remain usable when changes occur in practice, e.g. more parties standing in elections, combined elections?

⁵ Establishing Decree of 6 April 2007, Appendix 1.

1.4 Modus operandi

When starting work the Commission considered how best to address the questions put to it. It decided first of all to consider the question of what basic requirements the election process in the Netherlands should meet, putting a lot of work into identifying and defining these basic requirements, the 'principles' that need to be safeguarded. The results of this work guided it in the remainder of its work.

The Commission decided at an early stage only to review those parts of the election process where there was a demonstrable need, e.g. based on well-founded criticism. To identify these we spoke to various organizations on one or more occasions, either at the Commission's invitation or at the request of the organizations concerned.

The discussions served various purposes. First, they were used to gain a better idea of the problems that crop up in practice. They also covered ways of solving the existing problems and the pros and cons of the solutions put forward. Lastly, they were used to see whether there was any support for the kinds of solutions considered by the Commission. A list of the organizations consulted is appended (Appendix 13). The Commission is very grateful to these organizations and the people who provided information or responded to the web site (www.verkiezingsproces.nl).

The Commission met on 18 January, 5 March, 10 April, 7 May, 11 June, 3 and 12 July and 4 & 10 September 2007. Hearings were held on 29 January, 11 & 19 June and 21 & 24 August. On the evening of 7 March 2007 the Commission paid a working visit to the Municipality of Amsterdam to observe the count (of a ballot with paper ballots and manual counting). On 23 March it held a transfer meeting with the Voting Machines Decision-Making Commission. On 3 July it had a discussion with experts on compromising electromagnetic radiation. The State Secretary for the Interior and Kingdom Relations talked to the Commission on 31 May and to the Chairman on 22 August concerning progress. The Commission also had an extensive exchange by e-mail of ideas on documents, and from June 2007 on draft chapters of its report.

The organization of elections is a hot topic internationally, e.g. in the United States, Great Britain and Estonia. When forming its opinion, the Commission used relevant foreign documents, albeit not exhaustively.

2. Safeguards in the election process

2.1 Introduction

Confidence is a prerequisite in a democratic constitutional state. The government must enjoy the trust of the elected parliament. If parliament passes a vote of no confidence in a Minister or government, the Minister or government resigns. The courts must enjoy public trust. People must have confidence in the authorities that they will comply with and enforce the law. The electorate must have confidence that the parliament that it has elected is representative of the way the voters have voted – the totality of individual votes cast.

Trust has to be won and assured. Rulers must see to it that their policies and proposed measures and laws are supported by a parliamentary majority, otherwise they lose that confidence. Trust in judges is established by appointing them for life, so that they cannot be deposed by another state power. The courts try to win and retain trust by giving reasons for their decisions and making them open to public scrutiny. Lord Chief Justice Hewart formulated the requirement of trust in 1924 in his dictum *‘Justice should not only be done, it must be manifestly and undoubtedly seen to be done’*. As regards the election of parliament itself, again the electorate must have total confidence that elections are reliable and produce results in line with the totality of individual votes cast. People must be able to see and understand how the election process works (it must be transparent and verifiable), that the results are correct (fair) and that the secrecy of the ballot cannot be violated.

2.2 The international and national legal framework

Article 53 (2) of the Constitution requires elections in the Netherlands to be held by secret suffrage: i.e. every voter has the right to keep it entirely to himself how he or she intends to vote, is voting or has voted. First and foremost this means that the election process must be organized in such a way that it is possible to cast a vote without anyone else being able to find out how you have voted. Article 53 (2) of the Constitution also lays down that no-one may be obliged in any circumstances whatever to disclose for whom he or she has voted.⁶

In addition to secret suffrage, another basic principle is free elections, i.e. elections where voters are not subjected to any illegal influence, either from government or from any other quarter. This principle has never been formulated positively in specific provisions in the Elections Act, although when revising the Constitution in 1983 the government did state that it is an essential feature of democratic elections.⁷

The principles of secret and free suffrage are laid down not only in the Dutch Constitution but also in various international and European treaties to which the Netherlands is a party and some international and European documents.

⁶ Parliamentary papers II 1978/79, 14 223, No. 6, pp. 4 and 5.

⁷ Parliamentary papers II 1978/79, 14 223, No. 6, p. 5.

The treaties and documents are as follows:

- Article 21 (3) of the Universal Declaration of Human Rights:

The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures.

- Article 25, opening passage and (b), of the International Covenant on Civil and Political Rights

Every citizen shall have the right and the opportunity, without any of the distinctions mentioned in article 2 [such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status] and without unreasonable restrictions:(b) To vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret suffrage, guaranteeing the free expression of the will of the electors.

- Article 3 of the First Protocol to the European Convention for the Protection of Human Rights and Fundamental Freedoms:

The High Contracting Parties undertake to hold free elections at reasonable intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature.

- The Copenhagen Document 1990 of the Organization for Security and Co-operation in Europe (OSCE):

(5) The participating states solemnly declare that among those elements of justice which are essential to the full expression of the inherent dignity and of the equal and unalienable rights of all human beings are the following:

(5.1) free elections that will be held at reasonable intervals by secret ballot or by equivalent free voting procedure, under the conditions which ensure in practice the free expression of the opinion of the electors in the choice of their representatives. ...

(7) To ensure that the will of the people serves as the basis of the authority of government, the participating States will ...

(7.4) ensure that votes are cast by secret ballot or by equivalent free voting procedure, and that they are counted and reported honestly with the official results made public.

- Article 4 a. of the Code of Good Practice in Electoral Matters of the European Commission for Democracy through Law (Venice Commission) of the Council of Europe:
For the voter, secrecy of voting is not only a right but also a duty, non-compliance with which must be punishable by disqualification of any ballot paper whose content is disclosed.

- Council of Europe Recommendation Rec(2004)11, passed by the Committee of Ministers on 30 September 2004 on electronic voting (E-voting).⁸

The full text of this recommendation is reproduced in Appendix 11.

Although less explicit than the free and secret ballot, there is also an international consensus on a number of other principles that need to be safeguarded. It is generally accepted, for example, that only persons who are eligible to vote must be allowed to do so and that each vote cast must be counted only once. There is also agreement that the process associated with elections must be transparent, verifiable and fair.

⁸ Legal, Operational and Technical Standards for E-Voting, Recommendation Rec(2004)11 adopted by the committee of ministers of the Council of Europe on 30 September 2004, and Explanatory Memorandum.

The Commission adopts these principles in their entirety: the Dutch election process must safeguard them in any event. To ascertain whether this is the case, and if not, where the process is in need of improvement, we sought a more detailed definition of the principles, again trying to use international documents where possible. In particular we used Council of Europe Recommendation Rec(2004)11 of 30 September 2004. The Netherlands was closely involved in developing these recommendations, which explicitly relate to electronic voting.

The Commission defines the safeguards needed in the election process as follows:

Transparency

The election process should be organized in such a way that the structure and organization is clear, so that everyone in principle can understand it. There must be no secrets in the election process: questions must be able to be answered, and the answers must be verifiable.

Verifiability

The election process should be objectively verifiable. The verification tools may differ, depending on the method of voting that is decided upon.

Fairness

The election process should operate in a proper manner, and the results must not be capable of being influenced other than by the casting of lawful votes.

Eligibility to vote

Only persons eligible to vote must be allowed to take part in the election.

Free suffrage

Every elector must be able to choose how to vote in complete freedom, free from influence.

Secret suffrage

It must be impossible to connect the identity of a person casting a vote to the vote cast. The process should be organized in such a way that it is impossible to make a voter indicate how he or she voted.

Equal suffrage

Each voter, given the Dutch election system, must be allowed to cast only one vote in each election, which must be counted precisely once.

Accessibility

Voters should be enabled as far as possible to participate directly in the election process. If this is impossible, there must be a way of taking part indirectly, i.e. by proxy.

2.3 Striking a balance

Ideally the results of an election should precisely represent what the totality of the voters who turned out – all of whom will have received invitations to vote – freely intended to vote for. The process must be designed to provide error-free recording and counting of each individual voter's voting intention and actual vote and to publish the totals for each candidate and each list.

In practice it is not possible to provide 100% safeguards, as there are too many conflicting interests in the election process. A balance must therefore always be struck. It must be the case, for example, that each vote contributes only once to the final result of the election (under the principles of fairness and equal suffrage). The content of each vote must also remain confidential (the principle of secret suffrage). This places demands on the organization of the process and requires a careful balance to be struck. Verifiability and transparency could of course be increased by keeping a detailed log of each stage in the process (as is customary e.g. in the banking world with Internet banking), so that it can be reconstructed and rectified if there is even a semblance of impropriety. This approach, however, is incompatible with safeguarding the principle of secret suffrage.

Another area of conflict is between the principles of accessibility and free suffrage. Access could be improved by permitting the public to cast their votes in the simplest possible way at a whole host of locations (at home, at railway stations, supermarkets, etc.). The result, however, would be to jeopardize free and secret suffrage: if voting were to take place without supervision by a polling station committee it would not be possible to guarantee that people are voting without being influenced or that no-one can find out how they have voted.

If free and secret suffrage are to be guaranteed 100%, access for certain groups of people – such as Dutch citizens abroad and people with a physical impairment that prevents them from voting at a polling station – has to be substantially restricted, thus violating the principle of accessibility.

In certain cases, then, 100% safeguards cannot be provided. In these cases the Commission applies the rule 'either safeguard the principle or explain why a different balance has been struck'. Examples are voters abroad and voters with an impairment that prevents them from voting at a polling station. In these cases the principles of secret and free suffrage cannot be safeguarded to the same degree as in the case of voting at polling stations, but in the Commission's opinion the principle of accessibility outweighs those of secret suffrage and free suffrage here.

The election process must be conducted fairly, but it is an illusion that errors can be ruled out. They will be made, however much trouble is taken to avoid them. Those that *are* made, however, must be confined to incidents and must be able to be checked.

Organizing elections is a complex affair that requires the utmost care, given their importance. In the Netherlands, where the municipal authorities are responsible for organizing elections, tens of thousands of people are involved before, on and after election day: over 30,000 as polling station staff on election day alone, for instance.

As elections are relatively infrequent, occurring on average only once a year, organizing them is not a routine matter, so it is vital for the election process to be practicable. Here again a balance has to be struck, between 'making it as easy as possible' for those organizing the election on the one hand and safeguarding the principles on the other. Ease of conduct must not be allowed to become the overriding factor: the adverse effects this can have on confidence in the election process are described abundantly clearly in the report of the Voting Machines Decision-Making Commission. On the other hand, there is no point in designing an election process that on paper safeguards all the principles but is too complicated, because of the quantity of rules and procedures and/or the complexity of the aids used, and is therefore impracticable and/or impossible for voters to understand. It must also be organized in such a way that the results can be finalized as soon as possible after election day. On top of this, the cost of the election process must be acceptable.

The organization of the election process, given its complexity and importance, must be well delineated on the one hand but flexible on the other. The public are demanding better and better service from government, and this applies to elections too. People would like to be able to vote where and when it best suits them. The government has responded to this in recent years by extending polling station opening hours and (as an experiment under the Remote Electronic Voting Project) introducing voting at any polling station within the voter's municipality. Other options, such as voting at any polling station outside the voter's municipality, have not been tried as yet.

Because of their complexity, elections are not a suitable place to carry out experiments or test new technologies, but this is not to say that the election process has to be rigid and inflexible. The Commission takes the view that it should be able to respond wherever possible to new or changing ideas and/or preferences among the public – provided that the safeguards are re-examined again publicly and political decisions are made on the results, resulting in a fresh balance being struck where necessary. This entails taking a critical look at the election process each time (see Chapter 9), maintaining it and recalibrating it. Everyone who has a responsibility or duty in the process must contribute to this. The Minister of the Interior and Kingdom Relations (IKR) bears formal responsibility, and this must be explicitly enshrined in the law and regulations.

As regards the requirements that hardware and software for the election process need to meet, it must be possible to adapt them in the light of new developments, e.g. voting at any polling station outside the voter's municipality.

'Elections don't have to be on the cheap': this view has recently been expressed by a number of parliamentary parties in the House of Representatives. The Commission considers that it is indeed necessary to invest in the election process now. Precisely how large (in terms of money) the investment will have to be, the Commission cannot say, as it was unable to examine this in the time allotted to produce its report. The most that can be done here is to indicate the possible cost of the equipment (or part of it) needed for the new method of voting that the Commission recommends. This indication is given in Chapter 11.

In the ensuing chapters the Commission puts forward specific proposals for a way of organizing the election process that provides adequate safeguards in its opinion, mentioning any implications that the proposals have for the law and regulations where appropriate.

Aside from this, the Commission notes that the questions put to it apply to all the countries where free and democratic elections are held. It therefore proposes that in the Council of Europe, following on from Recommendation Rec(2004)11 of 30 September 2004, the government should work towards European technical standards for equipment used in elections so as to achieve a European certification system with regular re-examination of the certification criteria. One possibility is a certification system with gradations, under which a Member State could bring its procedures and technologies into line with new developments and thus gain a higher-category certificate. This kind of system would be particularly useful if protection against compromising radiation (see Chapter 4) is demanded at international or European level in order to protect against violations of the principle of secret suffrage.

In general terms the Commission also recommends that the law and regulations should be such that violations and breaches of the principles are precluded by preventive measures as far as possible and the rules do not have to be enforced after the event by criminal prosecution. Here the Commission would mention two examples: its proposal to require people using voting passes to identify themselves so as to prevent their unauthorized or fraudulent use as far as possible, and its proposal to require anyone voting on behalf of another person to produce a copy of an identity document of that person so as to reduce the incidence of forged proxies. In addition to this preventive measure, this practice should remain a criminal offence and the Public Prosecution Service should be urged to pursue an active prosecution policy.

3. Comparison of voting methods

3.1 Introduction

The law and regulations currently permit four methods of voting:

- Voting using paper ballots at polling stations
- Electronic voting at polling stations
- Postal voting for Dutch citizens eligible to vote from abroad
- Proxy voting

In addition, since 2003 it has been possible, under the Remote Electronic Voting (Experiments) Act, to experiment with telephone and Internet voting in the case of Dutch citizens eligible to vote from abroad.

The Commission was asked to indicate what risks are entailed in the way voting takes place in the Netherlands. The answer can be found in our threat analysis, the full text of which is given in Appendix 2. We did not carry out our own risk analysis of Internet and telephone voting as the Ministry of the Interior and Kingdom Relations (MolKR) carried out and published detailed risk analyses of these for the experiments in 2004 and 2006 (Appendices 3 and 4). In our view these provide an adequate account of the threats and risks involved in Internet and telephone voting.

Every method of voting has its risks, some or all of which may or may not be able to be countered with preventive or corrective measures. There is no such thing as a risk-free election process. In our view the risks should be offset against the principles discussed in the previous chapter, and not only may the outcome differ from one group of electors to another, it may also change over time.

3.2 Voting using paper ballots at polling stations

Voting using pre-printed paper ballots at polling stations is transparent, verifiable and fair. The process can be understood and observed by every voter. What votes have been cast and how they have been counted can be determined objectively. A recount can be carried out by counting the paper ballots again. As no technical devices are used, there is no risk of the election result being influenced by anything other than the votes cast. As, in practice, a small proportion of voters do not fill in their paper ballots correctly, the polling station committee has to decide whether these votes are valid, with the result that some votes are declared invalid. In municipalities where voting takes place with paper ballots 0.3-0.4% of votes on average are found to be invalid or blank.⁹

Eligibility to vote is guaranteed by the fact that the polling station committee checks the voter registration card or voting pass. Experience in recent years with the voting pass (in the

⁹ This average is based on Electoral Council statistics on general, provincial and municipal council and European Parliamentary elections during the 2002-2007 period (<http://www.verkiezingsuitslagen.nl>); it is an indicative average, not adjusted for population figures.

experiments under the Remote Electronic Voting (Experiments) Act) shows that it entails a greater risk of fraud and misuse. Voting passes (and voter registration cards for that matter) are not well protected against copying or forgery. The risk of misuse of voter registration cards is nevertheless relatively low, as they only permit the holder to vote at one particular polling station, where a member of the polling station committee checks the voter's name against the copy of the electoral register and then initials the card.¹⁰ The voter cannot therefore vote again. This is not the case with voting passes: unless countermeasures are taken, someone with a counterfeit voting pass could go on and vote at any number of other polling stations, as no check is made against the electoral register. The risk of apprehension is thus much smaller.

Free, secret and equal suffrage are guaranteed. The voter votes in a ballot booth to which only he or she has access. Each voter is given only one ballot paper (for each election) and makes his or her choice on a ballot paper that contains no information that could connect it with his or her identity. Voters place their ballot papers in the ballot box themselves.

Access is not optimal, and this is true of all methods of voting at polling stations. It may be difficult or impossible for people with a physical impairment and old people who have restricted mobility to attend a polling station. Not all polling stations have wheelchair access, and paper ballots cannot be used by the visually impaired.

There are a number of problems with this method of voting. Manual counting of paper ballots is error-prone and relatively time-consuming. The use of paper ballots is also an obstacle to the introduction of voting at any polling station outside the voter's municipality (see Chapter 4) and in that respect reduces the flexibility of the election process. The costs of voting using paper ballots are those of making and installing ballot booths and ballot boxes and printing ballot papers, all of which is relatively inexpensive. The staffing required, according to reports from a few municipalities, is much higher than when using voting machines.

3.3 Electronic voting at polling stations

Voting takes place using voting machines in 97.7% of Dutch municipalities.¹¹ The machine displays the lists for which the voter can vote and stores the votes cast. Counting is done by the machines once the election has closed.

In its report the Voting Machines Decision-Making Commission set out in detail why the voting machines used hitherto in the Netherlands are not sufficiently transparent and verifiable. We share this analysis entirely and therefore conclude that, because of the lack of transparency and verifiability, these voting machines do not guarantee the principle of fairness.

Eligibility to vote is guaranteed just as well by electronic voting at a polling station as by voting with paper ballots. With the voting machines used hitherto in the Netherlands, whether the principle of equal suffrage has been guaranteed can only be determined theoretically, by counting

¹⁰ Elections Act, Section J 25 (4).

¹¹ The percentage of municipalities that used voting machines in the municipal council elections on 7 March 2006.

the number of voter registration cards/voting passes and comparing this with the number of votes counted by the machine, since at present there is no technical way of checking the machine's operation so as to ascertain whether each vote cast has been stored in its memory correctly and only once.

Free suffrage is ensured by the requirement to place the voting machine in the polling station in such a way that other people cannot see how the voter is voting. It emerged in the run-up to the general election on 22 November 2006 that voting machines can emit compromising radiation, which could constitute a threat to secret suffrage. The Commission considers the problem of compromising radiation in detail in Chapter 4.

Access is more restricted when using voting machines at a polling station than when using ballot papers. It may be difficult or even impossible for people with a physical impairment and old people to operate a voting machine without assistance. The machines can be equipped with audio facilities to improve access for the visually impaired, as has been done in recent years.¹²

Voting machines enable the count to be carried out quickly, which is why municipal authorities consider that they make a substantial contribution to the practicality of elections. The machines currently in use are not capable of carrying out recounts; all they can do is print out the result of the count again.

On top of the cost of procuring voting machines (the investment) there are recurring costs for each election (licences, supplier support, etc.).

3.4 Postal voting for Dutch citizens eligible to vote from abroad

The amendment of 26 October 1983 permits postal voting (Chapter M of the Elections Act). This is available to voters who are actually resident abroad on nomination day or away from the Netherlands on account of their work or business or that of their spouse, registered partner, partner or parent on the day of the election (Section M 1). Postal voting was introduced to improve access to general elections and European Parliamentary elections.

When postal voting was introduced in 1983 there was not much debate as to whether it safeguarded the principles of secret and free suffrage. In its recommendations on the original bill the Council of State pointed out that not enough attention had been paid to the principle of the secret ballot.¹³ This resulted in an amendment to the bill regarding the procedure at polling stations, but there was no public debate on the matter, as the government considered the risk of irregularities to be low among the category of voters who would be eligible to vote by post. In the parliamentary debate on the bill the then Minister of the Interior, Koos Rietkerk, conceded that postal voting did entail certain risks, noting that the voters would be voting outside a polling station, so it would not be possible to ensure that voting was taking place in secrecy and complete freedom. In the government's opinion these dangers, however, were within acceptable

¹² In March 2006 eleven municipalities used voting machines equipped with audio facilities (source: MolKR).

¹³ Parliamentary papers II 1982/83, 17 819, No. A-C, p. 3.

proportions, as postal voting would only be available to voters resident abroad or temporarily away from the Netherlands.¹⁴

There have been comments on postal voting vis-à-vis secret suffrage in a European context too. The Council of Europe's European Commission for Democracy through Law, in the notes to its Code of Good Practice in Electoral Matters of 2002,¹⁵ considered that postal voting should not be widely encouraged as *'problems with the postal service are added to other difficulties inherent in this kind of voting, including the heightened risk of family voting'*.¹⁶ The Code adds, however, that – provided certain precautions are taken – postal voting could be used to enable certain groups of voters, such as hospital patients, prison inmates, people with restricted mobility and voters abroad, to vote, as long as there is no risk of fraud or intimidation.

The postal voting process is transparent and capable of being understood by everyone, but verifiability is not guaranteed throughout the process. This is particularly true of the transport of postal votes, which eludes any form of monitoring. This is one reason why fairness cannot be completely guaranteed: it is not out of the question that a postal vote could be intercepted and changed en route. As in the case of voting using paper ballots at polling stations, this method of voting produces invalid votes, as a small proportion of voters do not fill in their ballot papers correctly.

Eligibility to vote can be determined by comparing the signature on the registration form with the one on the postal voting slip. If a copy of the person's travel document is included with the registration form (as proof of Dutch citizenship), this signature can also be compared. This is not completely watertight, as those who carry out the checks are not expert in judging the authenticity of signatures, and the signatures on travel documents are small.

Equal suffrage is safeguarded in the case of postal voting by the fact that each voter is sent only one ballot paper. The polling station committee opens the envelope containing the ballot paper with his vote on it and is then able to see whether the envelope contains only one ballot paper.

Postal voting entails a relatively large administrative burden. Registering voters for an election is a highly cumbersome process, involving a lot of red tape for both voters and the authorities. On top of this, it is error-prone: there are problems with sending out the voting documents to voters and receiving them back in quite a few cases, with documents not arriving on time if at all. The result is that the voter concerned cannot vote, or his vote is not counted.

The cost of postal voting cannot really be compared with that of voting using paper ballots and/or voting machines, as postal voting is only available to a limited group of electors.

¹⁴ Proceedings II 1983/84, p. 5418.

¹⁵ Appendix 10.

¹⁶ Code of Good Practice in Electoral Matters, p. 16.

3.5 Proxy voting

Proxy voting is a common phenomenon in the Netherlands, compared with other countries. The possibility of proxy voting was initially restricted, in that voters were only permitted to appoint close blood relatives, relatives by marriage and housemates to vote on their behalf.¹⁷ Since the 1960s the range of people who are allowed to serve as proxies has been extended on a number of occasions, though the number of proxy votes any one person is permitted to accept has remained limited to two. A person who has accepted one or two proxies must cast these votes at the same time as his or her own vote, thus providing an automatic check that the limit of two is not exceeded.

In principle a voter is free to choose anyone as his or her proxy. However, there is no way of ruling out the possibility that the proxy has been assigned under duress to a family member or housemate upon whom the voter is dependent. As with postal voting there is thus a risk of family voting, which is a breach of free suffrage.

Secret suffrage is not safeguarded in the case of proxy voting. The voter appointing the proxy 'voluntarily' waives this right by telling the proxy how he or she wants the latter to vote. There is no way of checking whether the proxy does actually vote that way, a risk that the voter implicitly accepts.

Given the possibility of breaches of the secrecy of the ballot, the verifiability and fairness of proxy voting cannot be guaranteed to the same extent as in the case of voting with paper ballots at a polling station.

The postal voting process is transparent and capable of being understood by everyone. Equal suffrage is guaranteed by the fact that voting takes place at a polling station, as is eligibility to vote. Proxy voting does not have much effect on practicality or cost.

3.6 Internet and telephone voting

The transparency of Internet and telephone voting depends to a large extent on the system that is used. They are only transparent if the systems are completely 'open', e.g. because they use open source software, and even then this is highly dependent on the reliability of the technology used and of the organization that manages that technology. On top of this, system security often requires this to take place in a room to which access is restricted or prohibited, which means that the ballot cannot be public. Moreover, only experts are able to understand how such systems work because of the complexity of the technology. As far as transparency and verifiability are concerned, then, Internet and telephone voting cannot be compared with voting at a polling station.

¹⁷ Under Section K 5 of the Elections Act of 13 July 1951 the only categories of person who could be designated as proxies were the spouse, relatives by blood or marriage up to the third degree, the spouse of a sister-in-law or brother-in-law, or one of the voter's housemates.

It has been argued, e.g. by the organization Burger@Overheid.nl, that the ballot process is no different in essence from many other processes where the public rely on technology (e.g. paying by PIN and over the Internet) – processes where they are also unable to check the fine detail. People who so wish should be given the opportunity to vote using the methods they wish and believe they can trust. Elections do however differ in essence from these other processes, in that voters must be able to have confidence in the way not only their own votes are processed but also those of all the other voters. The Commission would point out that comparison with Internet banking is not appropriate, since there detailed logs are kept and users are identified, which would be incompatible with the secrecy of the ballot in the case of Internet voting. Also, as with all other methods of remote voting (i.e. voting other than at a polling station), free and secret suffrage are not guaranteed, since the environment and the circumstances in which votes are cast escape the scrutiny of the authorities responsible for organizing the elections. This makes family voting more likely to occur, for example. In this sense Internet and telephone voting are no different from postal voting.

In the case of postal voting, eligibility to vote can be checked by comparing the physical signature on the registration form with the one on the postal voting slip. It is difficult to envisage how such a check could be carried out in the case of Internet and telephone voting. There are ways of determining whether the person casting the vote is identical to the elector, for example by using biometrics, e.g. fingerprints, as a method of authentication. The risk, however, is that a connection could be also made between the elector and the vote cast, which would be a breach of the principle of secret suffrage. The most common method of authentication in Internet and telephone voting is by means of one or more codes. These suffer from the risk of being stolen or guessed, making it possible for someone other than the elector to vote and thus excluding the elector. Verifiability and fairness are therefore very difficult to guarantee with such methods of voting. Also, if Internet and telephone voting were to be made available to everyone, it would be difficult to combat abuses such as vote buying.

While the accessibility of Internet and telephone voting is high (almost everyone has access to the Internet and/or a telephone), Internet voting is particularly vulnerable to attacks resulting in no-availability (known as 'denial of service' attacks). Risks of this kind can only be defended against at relatively high cost or by extending the ballot over a longer period.

Internet and telephone voting have hitherto taken place in the Netherlands only as an experiment. All that is known is the cost of these experiments, which runs into millions of euros.¹⁸ It is difficult to compare this with the cost of voting using paper ballots and/or voting machines, though the cost of Internet voting in particular is likely to be much higher than that of voting with paper ballots at polling stations.

¹⁸ Parliamentary papers II 2003/2004, 29 200 VII, No. 51; 2006/2007, 30 800 VII, No. 48.

3.7 Discussion

The Commission takes the view that free and secret suffrage can only be adequately safeguarded in the case of voting at polling stations, which should therefore remain the main method of voting in the Netherlands. We further consider that the procedure at polling stations should be standardized throughout the Netherlands, as the election process should in principle provide the same degree of safeguards to all voters. Every elector should be able to vote using a method that strikes the best balance between the principles.

The Commission's recommendations are confined to the organization of the election process; in other words, there is no intention to send out a signal that other electronic processes are not reliable. Internet voting is a subject that has been studied intensively by academic researchers in recent years. In the future we may see new, generally acceptable solutions emerging that do provide adequate safeguards.

Voting using paper ballots at polling stations is the preferred option on the grounds of transparency and verifiability. There are practical problems with the counting of paper ballots, however, to which the Commission is sensitive. We therefore examined whether there might be an alternative that enables counting to take place electronically while retaining the transparency and verifiability of voting using paper ballots. We believe we have found such an alternative, namely voting using electronic devices that produce paper records of the votes cast. We would point out, however, that voting using electronic devices does entail a substantial financial investment. The next chapter gives a detailed description of this method of voting.

Methods other than the main method of voting, at polling stations, should only be provided for special groups of voters, to enable them to take part in those elections in which they are eligible to vote (access). The voters concerned are those who are eligible to vote from abroad and a limited group with physical impairments (and the elderly) who can prove that they are unable to attend a polling station or vote there. The Commission proposes that voters who are eligible to vote from abroad should henceforth be permitted to use Internet and postal voting. As regards the physically impaired, the Commission concurs with the opinion of the Council for the Disabled and Chronically Ill, the Disability in the Community Task Force and Viziris, and proposes that they should be allowed to vote by telephone.

4. Voting in the future

For the vast majority of electors voting in the future, in the Commission's opinion, should be standardized and take place in polling stations, where a polling station committee supervises the conduct of the ballot and the ballot and the count are public. The organization of the polling station and the authority of the polling station committee should guarantee that voters can cast their secret votes in complete freedom.

Below we consider the various methods of voting at polling stations. The Commission is aware that other methods are conceivable and that technology will not stand still: the development of a voting method is therefore a matter requiring a good deal of care and consideration.

4.1.1 Voting at polling stations

Voting at polling stations is the preferred option on the grounds of transparency, verifiability and free and secret suffrage. The Commission notes that there are four methods of voting at polling stations:

- Voting with pre-printed paper ballots which are counted manually
- Voting with pre-printed paper ballots which are scanned and the votes counted electronically
- An electronic voting device with a memory and an additional *paper trail* for verification purposes
- Electronic counting (by a *vote counter*) of votes cast on paper which are printed by a *ballot printer* to enable them to be counted electronically. The voter makes his or her choice on the *ballot printer*: this produces a paper ballot (*ballot printout*), which the voter deposits in a ballot box. When the ballot closes the *ballot printouts* are counted electronically.

See the table later on in this chapter for an overview of the advantages and disadvantages of the four methods.

Method 1 is the traditional method of voting with pre-printed ballot papers. In the Commission's opinion this method safeguards the principles; indeed, it is the preferred option on the grounds of transparency and verifiability. There are major practical problems with the counting of paper ballots, however, as it is error-prone and takes a long time. According to the municipal authorities, the number of votes that can be cast at a polling station, taking the long polling station opening hours into account, needs to be smaller than when using voting machines. As a result, more polling stations and polling station committees are required, and in practice municipalities find it increasingly difficult to find suitable premises and staff. The need to restrict the number of votes cast at a polling station also makes voting at any polling station (even within the voter's municipality) impossible, since the number voting at any given polling station is unforeseeable, as it cannot be predicted where voters will vote.

In method 2 voters make their choice in the same way as in method 1, using a pen or pencil on a paper ballot. For the count the ballots are scanned and counted using a scanner. A system of this kind was tried in the United Kingdom just recently: the Electoral Commission published a report on it in August 2007, indicating that there had been major problems, which even resulted in the

paper ballots having to be counted manually.¹⁹ The problems were due, among other things, to the fact that voters did not indicate their choices uniformly (e.g. they did not make the required cross for the chosen candidate precisely in the box provided or they wrote a dot instead of a cross). The scanner had difficulty coping with these variations, causing processing to break down. Voting using optical scanning systems takes place on a fairly large scale in the United States of America.²⁰ Nine states use this method exclusively. Scanning systems where voters insert their ballot papers in a ballot box with a built-in scanner produce only 0.7% invalid votes in those states. Nevertheless, as with all 100% electronic systems, vulnerabilities have been found in optical scanning systems that might make it possible to manipulate the results.²¹ California, for example, has wholly or partly withdrawn approval from all the suppliers of these systems.

The ballot papers used and scanned in the United States and the United Kingdom are much smaller than those used in the Netherlands. Because of the large number and length of the lists of candidates, Dutch ballot papers need to be of a size that does not fit in standard scanners. Splitting the papers up into separate pages, with voters only using the page on which they cast their votes, would create the risk of the other pages being used to cast fraudulent votes. Scanning ballot papers is therefore not really feasible in the Netherlands, and the Commission does not recommend this method.

Method 3, *electronic voting with a paper audit trail*,²² entails voting on a 'voting device' in stages. First the device shows the voter a list of the election(s) in which he or she is eligible to vote. Then he or she decides which election to vote in (the elections can be taken in any order). Once he or she has selected a candidate, or a blank vote, the device asks for confirmation. If the voter confirms the choice, the *voting device* prints it out on paper. The paper record is shown to the voter, but in such a way (e.g. behind glass) that he or she cannot touch it and hence cannot tear it off or take it away.

The paper record contains the following data:

- The election in which the vote has been cast
- The electoral district
- The vote cast (name or list number and name of candidate or 'blank')

The voter is then asked to confirm his or her choice once more. Only once (a) the voter has satisfied himself or herself that the choice displayed by the device corresponds to that on the paper record and (b) the second confirmation has been received, is the vote cast, by that second confirmation. The vote (as displayed to the voter) is stored electronically by the *voting device*. The paper audit trail is collected in a sealed space in or adjacent to the *voting device*. As long as the voter has not confirmed his or her choice, he or she can return to the list of elections and start again. The voter moreover always has the option of not voting in one or more of the elections.

¹⁹ The Electoral Commission, May 2007 electoral pilot schemes, Electronic counting, August 2007; Electoral pilot scheme evaluation. Overall report, Ovum Consulting, May 2007 (available on-line at <http://www.electoralcommission.org.uk/elections/pilotsmay2007.cfm>).

²⁰ Election Data Services, *Almost 55 Million, or One-Third of the Nation's Voters, Will Face New Voting Equipment in 2006 Election*, 2 October 2006 (available on-line at http://www.edssurvey.com/images/File/ve2006_nrpt.pdf).

²¹ http://sos.ca.gov/elections/elections_vsr.htm; http://voter.engr.uconn.edu/voter/Report-OS_files/uconn-report-os.pdf; http://www.sos.ca.gov/elections/voting_systems/ttbr/red_sequoia.pdf.

²² Direct Recording Equipment + Voter Verified Paper Audit Trail.

If the voter considers that the name on the paper record does not correspond to the choice he or she made on the voting device, he or she reports this to the polling station committee. If the vote has not been confirmed, he or she is given one more opportunity to vote. The voting device therefore needs to have a facility for invalidating the paper record shown to the voter. The opportunity for the voter to vote again is provided in the same way as laid down currently in Section J 27 (1) of the Elections Act. The polling station committee restarts the procedure by reading in the election codes on the voting pass, following which the voter can vote in any elections in which he or she has not yet voted. If the voter, after a second attempt, again reports to the polling station committee that the choice on the paper record does not correspond to his or her choice, the committee must carry out an investigation to ascertain whether the device is working properly. Rules on this will need to be laid down in the law and regulations. In the worst case, i.e. if it is not certain that the device is working properly, the committee will have to order it to be replaced. In this situation the law and regulations will have to lay down how the votes stored in the device that is being replaced are to be counted.

The advantage of this method is that, once the ballot is closed, the count can be just as quick as it is at present with voting machines. There are some disadvantages, however. This method relies on the electronic device operating reliably. Although voters are shown their choices on paper, during the ballot there is no way of checking whether the device is electronically storing the votes correctly. In other words, in principle this type of device has the same vulnerabilities as the current voting machines, although there is the possibility of carrying out a random check on the paper audit trail after the ballot has closed.

Another risk is that a situation could occur where a voter considers that the paper record of his or her vote is incorrect. At this point he or she has made a choice on the device (albeit unconfirmed as yet). In this case we need to be able to depend on the device not storing the choice and including it in the count. An advantage is that the correctness of the count carried out by the device can be checked by counting the paper records. If any discrepancies are found between the count of the paper audit trail and that of the device, however, it needs to be clear beforehand which count is valid.

The Commission has examined whether this method using a paper trail has already been used elsewhere in the world, and has found this to be the case in Belgium, the United States of America, Brazil and Venezuela.²³ Reports indicate that experience has been mixed.²⁴ Various complications can occur with this method of voting that can substantially hamper the ballot at the polling station. Fault-free, reliable equipment needs to be developed – reliable in terms of both

²³ 2006, Cuyahoga County, Ohio, United States; 2006, Bibb County, Camden County & Cobb County, Georgia, United States; 2005 Venezuela; 2003, Waarschoot & Verlaine, Belgium; 2002 Brazil. In the Netherlands a survey of voters' experience of voting on a Nedap voting machine with paper trail in the provincial council elections on 7 March 2007 in The Hague, Utrecht and Zwolle was carried out for Nedap Elections Systems by the University of Twente. This was an initiative of the manufacturer, not part of the official election organization.

²⁴ Election Science Institute, 2006, DRE Analysis for May 2006 Primary Cuyahoga County; Office of the Secretary of State, 2007, Voter Verified Paper Audit Trail. Pilot Project Report; College van deskundigen belast met de controle van de geautomatiseerde stemmen en stemopneming (Panel of experts responsible for monitoring computerized ballots and counts), Verslag betreffende de verkiezingen van 18 mei 2003 (Report on the elections of 18 May 2003); Supremo Tribunal Eleitoral, through the Netherlands Embassy in Brasilia; European Union Election Observation Mission, Final Report, Parliamentary Elections Venezuela 2005.

the electronic memory and the paper trail – as an absolute precondition if this method is to be employed. The Commission would note here that the secrecy of the ballot is not adequately safeguarded in the case of a paper trail where the written records of votes are made on a roll (as in the United States of America), as the voting passes are usually kept in order of arrival – the same order as that of the written records of the votes.

A fundamental drawback with this method of voting arises from the fact that each voter's vote is recorded twice, electronically in the voting device and in written form in the paper audit trail. There could therefore be a discrepancy between the electronic and the paper result from one and the same device. Experience elsewhere shows that this is no mere theoretical possibility. The law and regulations will have to lay down what the polling station committee should do in such cases and which count is valid. It should be remembered here, as past experience shows, that errors can be made in the manual count where pre-printed ballot papers are used.

In the last method, *electronic voting using a paper ballot*, the voter makes his or her choice in stages on a '*ballot printer*'. First the device shows the voter a list of the election(s) in which he or she is eligible to vote. Then he or she decides which election to vote in (the elections can be taken in any order). Once he or she has selected a candidate, or a blank vote, the *ballot printer* displays that choice (as in the case of the voting machines used hitherto). The *ballot printer* then asks for confirmation. If the voter confirms the choice, the *ballot printer* prints it out on paper. If there is more than one election, a paper ballot is printed for each election. The printout (*ballot printout*) contains the following data:

- The election in which the vote has been cast
- The electoral district
- The vote cast (name or list number and name of candidate or 'blank')
- Possibly a bar code containing the above information

The voter always has the option of cancelling the vote in that particular election. As long as the voter has not confirmed his or her choice, he or she can return to the list of elections and start again. The voter still has the option of not voting in one or more of the elections, of course. The voter can check from the printout whether the vote is shown correctly. If so, he or she casts his or her vote by depositing the paper ballot(s) in a physical ballot box. The ballot box must have a sufficiently wide aperture but otherwise must be sealed and non-transparent.²⁵

If the voter considers that the printout of the vote (the *ballot printout*) does not correspond to his or her choice, he or she reports this to the polling station committee. The polling station committee collects the paper ballot(s) and invalidates it/them in the voter's presence in the manner to be laid down in the law and regulations. The voter is given another opportunity to vote. The opportunity for the voter to vote again is provided in the same way as laid down currently in Section J 27 (1) of the Elections Act. If the voter, after a second attempt, again reports to the polling station committee that the printout of the vote does not correspond to his or her choice, the committee must carry out an investigation to ascertain whether the *ballot printer* is working properly. Rules on this will need to be laid down in the law and regulations. In the worst case, i.e.

²⁵ The printout of the ballot should not in principle be folded, so as to facilitate electronic counting. The printouts of the ballots are not readable in a non-transparent ballot box.

if it is not certain that the *ballot printer* is working properly, the committee will have to order it to be replaced. As no votes are stored in the *ballot printer*, replacing it has no effect on the ballot, since the votes cast are deposited in the ballot box.

The main advantage of this method is that the operation of the *ballot printer* is completely transparent and verifiable. It merely presents the options available to voters and prints out their choices. Otherwise it does nothing, so there is no question of voters' choices being stored electronically. The printout is the only record of the vote cast. A *ballot printer* can therefore use commercial software, since whether the software is working properly can be checked from the *ballot printout*. If this does not correspond to the choice that the voter has made, the *ballot printer* can simply be replaced.

From the point of view of practicality, this method has the disadvantage that the votes still have to be counted once the ballot is closed. This can be done manually, but this is not the preferred option, in view of the likelihood of errors. The votes could be counted automatically using optical character recognition (OCR) technology. A scanner, or *vote counter*, reads the printed votes optically, counts them and produces a result. The technology required is on the market and already in use for many applications. The number of votes at any given polling station is relatively small, so it should not take more than 15-30 minutes to count them. Adding a bar code could have practical advantages, as it would make the votes easier to recognize, but this is not desirable as a matter of principle, as the *ballot printout* would then contain information that cannot be checked directly by the voter, thus reducing transparency. If it were to be decided nonetheless to use bar codes, the bar code system should be published for the sake of transparency and verifiability, e.g. by posting all the choices available and the corresponding bar codes at the polling station. Any voter so wishing could then check the code at the polling station.

4.1.2 Discussion

The four possible methods of voting at polling stations all have their advantages and disadvantages, as shown in tabular form below.

The Commission recommends solely the introduction of *ballot printers*, because of the conceptual clarity of the system and the unambiguous results it produces. Although counting can be carried out quickly using a voting device with a paper trail, by using the device to do the counting, this advantage is outweighed by the disadvantages, as it still means relying entirely on the software correctly storing the votes cast. In the case of a *ballot printer* the voter's choice is completely separate from the casting of the vote, so there is no need to rely on the vote being stored correctly.

Because of the practical problems likely to occur in manual counting, the Commission recommends electronic counting (using a *vote counter*). The paper records or paper ballots should only be counted manually if there is doubt as to whether the electronic counting software is working properly or a technical fault. A *vote counter* can be replaced without losing any stored votes, as the *ballot printouts* are still there and can be counted by the replacement *vote counter*. The law and regulations will have to lay down what the polling station committee should do if the

electronic count is unsatisfactory. The *vote counter* must be able to distinguish automatically between votes cast in different elections.

It is worth considering following up the electronic count with a manual count at a number of polling stations as a spot check, since this could be a way of creating and maintaining confidence in the voting system.

The result – as long as voting is not allowed to take place at any polling station nationwide (see 4.3.1, **Voting at any polling station**) – should then be determined in the same way as in the current election process, where the count from each polling station is sent to the principal electoral district committee, which tots up the results and sends them to the Central Electoral Committee. This is done in the official report, to which the result of the count is appended. The counts could also be transmitted electronically.

	Voting with paper ballots and manual counting	Voting with paper ballots which are scanned and the votes counted electronically	Voting device with paper records (paper trail)	Ballot printer with separate vote counter (paper ballots)
Making the choice	Manually	Manually	Electronically	Electronically
Casting the vote	Manually	Manually	Electronically	Manually
Storing the vote cast	On paper	On paper	Electronically and on paper	On paper
Method of counting	Manually	Electronically (optional manual count)	Electronically (optional manual count)	Electronically (optional manual count)
Main advantages	Safeguards the principles.	Safeguards the principles. Can be faster than manual counting.	Count is just as fast as with current voting machines. Not affected by completion errors made by voters. Manipulation of electronically stored votes detectable by counting paper trail. Enables VAPS(N) to be introduced. Audio facilities could be provided for the visually impaired.	Safeguards the principles. Commercial hardware could be used. Not affected by completion errors made by voters. Not affected by any errors or manipulation of ballot printer or vote counter. Enables VAPS(N) to be introduced. Audio facilities could be provided for the visually impaired. Ballot not affected by replacement of ballot printer.
Main disadvantages	Counting is error-prone and takes a long time. More polling stations needed. Presents an obstacle to the introduction of voting at any polling station. Limited access for the visually impaired.	Scanning of ballot papers is error-prone. Presents an obstacle to the introduction of voting at any polling station. Limited access for the visually impaired. Unfolding ballot papers is time-consuming.	Risk of discrepancy between number of votes stored electronically and paper records, resulting in doubts as to reliability of voting device. Possible failure of hardware. Compromising radiation (TEMPEST).	Possible failure of hardware. Compromising radiation (TEMPEST) from ballot printer (not from vote counter).

Table: Main characteristics of the four ballot systems

VAPS(M): Voting at any polling station inside the voter's municipality

** VAPS(N): voting at any polling station outside the voter's municipality (nationwide)

4.2.1 Electromagnetic radiation

Where electronic devices are used for voting, the question is whether they emit compromising radiation, and if so, whether this could be misused. The problem of compromising radiation in the ballot process came to light in autumn 2006, as shown in a report²⁶ and video clip²⁷ by a citizens' group, 'We do not trust voting computers'. An investigation by the Minister for Governmental Reform and Kingdom Relations led to measures including the suspension of approval for one type of voting machine.²⁸ Given that the Commission is proposing that *ballot printers* be used for voting at polling stations, the question is whether standards should be set for these devices, and if so, what these standards should be.

Every electronic circuit, device and wire emits electromagnetic radiation, which can interfere with the operation of other electronic equipment (electromagnetic interference or EMI). For this and other reasons, electronic equipment must comply with statutory standards before it can be brought onto the market. The best-known standards are those of the American Federal Communications Commission (FCC) and the European Union (the CE marking system).

If an electronic device complies with the standard, this means that the radiation emitted is so low that it does not interfere with the operation of other electronic equipment. It does not mean that it emits no electronic radiation at all: there is always some residual radiation.

When an electronic device is on, the electronic radiation it emits can be deliberately intercepted remotely and processed. Information may be able to be obtained or computed from the residual radiation picked up in this way. Radiation that contains information and is emitted unintentionally is referred to as 'compromising radiation'. Signals from electronic equipment can thus be intercepted. A Dutch author, Wim van Eck, published an article back in 1985 demonstrating that it is possible to reconstruct information displayed on the screen of an electronic device from residual radiation.²⁹

Compromising residual radiation can be picked up in the immediate vicinity of the device in question using simple technology; sophisticated equipment enables it to be picked up from dozens of metres away in some cases. In this way a VDU can be spied upon from a distance of dozens or even hundreds of metres without the person operating it noticing anything. While this is not a problem with everyday consumer electronics and their uses, it can be a serious problem if the electronic equipment in question is being used to handle confidential or classified information. Electromagnetic radiation is relevant to sophisticated security systems as regards both defence (protecting oneself) and offence (eavesdropping on someone else).

²⁶ 'Nedap/Groenendaal ES3B voting computer, a security analysis', last revision 6 October 2006, Chapter 6, **Compromising emanations** (available on-line at <http://www.wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf>).

²⁷ This can be viewed on-line at <http://www.youtube.com/watch?v=B05wPomCjEY>.

²⁸ 'Voomemen tot intrekking goedkeuring stemmachines' (Proposed withdrawal of approval of voting machines), communication from the Minister for Governmental Reform and Kingdom Relations, 30 October 2006/No. 2006-0000352288 CZW.

²⁹ W. van Eck, 1985, Electromagnetic radiation from video display units: an eavesdropping risk, PTT Dr. Neher Laboratories.

Electronic voting equipment also emits electromagnetic radiation, and the secrecy of the ballot can be violated by intercepting compromising radiation thus emitted. Here the Commission uses 'compromising' in the sense of 'revealing how a voter has voted'.

The existence of electromagnetic radiation and the possibility of picking it up have been known about for a long time. It is possible, however, to modify equipment in such a way that radiation (hence compromising radiation) is minimized. NATO has drawn up regulations on the matter, known under the name of TEMPEST. The abbreviation stands for various phrases, the most common of which is *Telecommunications Electronics Materials Protected From Emanating Spurious Transmissions*. Another term used is EMSEC, short for *Emission Security*, which also covers other areas of electronic security.

The TEMPEST standards lay down the best way of protecting equipment to avoid compromising radiation. NATO applies three standards, known as SDIP-27. The most stringent standard assumes that an attacker has virtually direct access to the device emitting the electromagnetic radiation; the other two standards assume that the attacker is at an increasing distance from the device. They take into consideration not only radiation that can be picked up in the vicinity of the device but also compromising signals accidentally 'hitching a ride' on other signals, for example secret information unintentionally leaving the room via the mains network.

Intercepting compromising signals is one of the techniques an intelligence service might use in the course of its work, so the extent to which a government protects itself against other intelligence services is secret information. NATO's TEMPEST standards are consequently classified and not published. Generally speaking there is hardly any information or expertise publicly available on TEMPEST. At the time of writing, as far as the Commission is aware, little if any public research is being done into TEMPEST. Expertise is thin on the ground in the Western world. The European Union is currently drawing up its own TEMPEST standards for the purpose of harmonization. Some of the new Member States are not members of NATO, so do not have access to secret NATO information. The future EU standards are designed to cover the same area as the NATO standards and will therefore also not be published.

4.2.2 Discussion

To gain some understanding of this complex subject the Commission invited representatives of a number of Dutch and foreign companies professionally concerned with TEMPEST to discuss the matter. It was clear from these conversations that compiling a new published standard for compromising radiation would probably be no easy task (and a costly one into the bargain).

Ballot printers or voting devices can be protected against emitting compromising radiation over excessive distances. The measures a supplier of *ballot printers* or voting devices needs to take are known only to a select few commercial TEMPEST suppliers and NATO-accredited testing laboratories, however. There are special off-the-shelf computers, VDUs and printers that already

have built-in protection, and information on these is available publicly.³⁰ These are supplied by the specialist TEMPEST suppliers.

Protecting equipment against compromising radiation is no easy task, according to the experts. The TEMPEST requirements need to be taken into account at the design stage. It would not be advisable, therefore, to phase in TEMPEST requirements gradually, only requiring equipment to comply with the standards in, say, a few years' time.

The experts we consulted said that the most stringent NATO standard requires each device to be tested individually. In the case of elections this would mean testing some 10,000 devices in this way (before each election). Also, this standard sets requirements for the environment in which the device is installed which cannot be met in polling stations. The least stringent NATO standard does not provide adequate protection, hence the secrecy of the ballot could be jeopardized. In view of this the intermediate-level standard, NATO SDIP-27 Level B, would be most suitable for devices on which voters make their choices. It should be stressed that compliance with NATO SDIP-27 Level B does not provide absolute protection against the emission of compromising radiation: the protection provided extends only to a particular zone around the device on which voters make their choices.

Equipment which has been fitted with protection still has to be tested before it is officially 'TEMPEST APPROVED'. If it passes the test, the testing authority seals the equipment: nothing in the hardware may be altered, otherwise the approval is invalidated. If a component is replaced, the equipment has to be retested before it can be approved again. This is a major problem in the case of voting devices, as it needs to be possible to replace a component, e.g. the printer, on polling day. The NATO SDIP-27 Level B standard is known to certificated testing authorities in NATO countries, so a supplier of voting devices can choose where to have the equipment tested, albeit these authorities are few in number.

It might be wondered how great the need is to protect voting equipment against compromising TEMPEST radiation. There are both matters of principle and pragmatic aspects here. The rules and regulations require the secrecy of the ballot to be protected. The question, however, is: how great is the risk of the compromising radiation emitted by the voting equipment being misused? Sophisticated TEMPEST expertise is currently well protected, but a motivated, technically knowledgeable amateur can go a long way. Ignoring the phenomenon is not an option, especially now that the subject is commanding wide attention. It is not desirable, for example, for the political leanings of Dutch celebrities to be published on the web. Theoretically it is even conceivable that real-time election results could be obtained on election day and published on the Internet. This, however, would involve eavesdropping on the ballots in at least enough polling stations for the results to be representative of the totality, and it is highly doubtful whether anyone would be willing to go to that much expense and trouble. To some extent, developments of this kind could be tackled by other reactive means (e.g. making such practice a criminal offence and prosecuting offenders), but the Commission's preferred option is prevention, where this is feasible and financially viable. An additional criminal or administrative law sanction could also be

³⁰ <http://nato-cat.softbox.co.uk/Pages/ProductsByCategory.aspx?CategoryID=18>.

considered, namely temporarily or permanently withdrawing the offender's right to vote and to stand for election.

The Commission sees a dilemma in the secrecy surrounding the existing NATO standards. Not only do potential manufacturers of voting devices need to know what is required, in principle the public also need to be able to understand what standards voting equipment is required to meet. From the discussions conducted by the Commission it was clear that there is probably no solution to this dilemma in the short term. The secrecy surrounding the standards is unfortunate from the point of view of transparency, but in practical terms there is no other option when it comes to prevention policy. On the other hand, if *ballot printers* are introduced with separate *vote counters*, the transparency of the *ballot printers* is much less important than in the case of voting devices with an electronic memory.

It is likely, moreover, that the subject of TEMPEST will be taken up in the civil sphere in the coming years: its relevance to voting equipment can be seen as a harbinger of this. Another problem is cost. The Commission is unable to estimate what this would be, but presumes that it would be relatively high, especially considering that the equipment in need of protection is used once a year on average.

The Commission recommends that reactive measures be taken, by making such practice a criminal offence and reaching clearly defined agreements with the Public Prosecution Service on investigation and prosecution. If the additional cost of protection against compromising radiation is not prohibitive, the current NATO SDIP-27 Level B standard should also be applied.

4.3.1 Voting at any polling station

In recent years the MolKR has experimented with voting at any polling station (VAPS) within the voter's municipality under the Remote Electronic Voting (Experiments) Act, and the experiments have been evaluated.³¹ The evaluations showed that both municipalities and voters were enthusiastic about the possibility of voting at other than their designated polling station. Although the results of the experiments were overwhelmingly positive, some new vulnerabilities came to light, in particular as regards protecting voting passes against forgery or counterfeiting and establishing that the person using a voting pass actually is the elector whose name is stated on the pass (see also 3.2). The Commission considers that both these vulnerabilities need to be tackled before it is decided to introduce VAPS within the voter's municipality in all municipalities.

Voting pass security could be improved by incorporating authenticity features. The Commission realizes that these will have to be different from, say, the authenticity features in travel documents, as regards both complexity and cost, since the members of polling station committees who will need to check them are not experts on this subject. Also, voting passes are designed to be used once only, so the cost should not be too high. It will be the responsibility of the Minister of the Interior and Kingdom Relations to lay down the requirements for the standardized model voting pass.

³¹ Parliamentary papers II 29200 VII, No. 5.1.

More reliable identification can be achieved by requiring users of voting passes to identify themselves when voting. The Electoral Council recently advised the State Secretary for the Interior and Kingdom Relations to introduce compulsory identification.³² Since the introduction of the Compulsory Identification Act everyone in the Netherlands over the age of 14 is required to hold a valid identity document and carry it with them at all times. All electors will therefore have an identity document on their person when they go to vote and will be able to produce it. Compulsory identification when voting must be enshrined in the law and regulations.

To identify himself or herself to the polling station committee a voter will have to produce a valid identity document, by which the Commission means:

In the case of Dutch citizens:

1. A valid travel document as referred to in the Passports Act, Section 2 (1) a, b, c, d, e and g or (2)
2. A valid driving licence issued under the Road Traffic Act or as referred to in the Road Traffic Act 1994, Section 107

In the case of foreigners eligible to vote in municipal council elections and/or European Parliamentary elections:

1. The documents that a foreign national is required to hold under the Aliens Act 2000 in order to establish his identity, nationality and residence status
2. A valid national, diplomatic or service passport issued by the competent authority of another Member State of the European Communities or another state party to the Agreement on the European Economic Area, if the holder is a national of that other Member State
3. A driving licence issued by the competent authority of another Member State of the European Communities or another state party to the Agreement on the European Economic Area, if the holder is resident in the Netherlands, provided the validity period in the Netherlands laid down in the Road Traffic Act 1994 has not expired, no administrative order as referred to in the Road Traffic Act, Chapter VI (9) and no additional penalty as referred to in Section 179 of that Act has been imposed on the holder, and the licence bears a passport photograph of the holder

An elector might lose his or her identity documents (passport, driving licence, etc.) so soon before election day that it would be impossible to obtain a new document by election day even by making an urgent application. In this case he or she can report the loss to the police (this has to be done anyway before applying for a new travel document or driving licence). A copy of the police report, along with a photocopy of the lost or stolen identity document – or, if the elector does not have this either, some other identity card or document such as a company pass, membership card or bank or giro card – should then be produced to the polling station committee as identification, preferably one bearing a photograph. The law and regulations will need to provide for this.

The government has long had the intention not only of making VAPS possible in all municipalities but also to extend the principle so that in any election a voter can vote for the electoral district in which he is eligible to vote at any polling station in the Netherlands. Introducing this would have consequences, especially if it were to apply to all elections, i.e. including municipal council

³² Electoral Council, 2007, Report 'Legitimatieplicht in het stembloot' (Compulsory authentication at polling stations; available on-line at <http://www.kiesraad.nl/contents/pages/88488/advieslegitimatieplicht.pdf>).

elections.³³ The consequences are not only of an organizational nature but also financial, as additional technical facilities would be needed.

Each voting pass would have to bear a unique number created when it is produced. This means that voting passes would have to be produced centrally. In every election every polling station would need to have the national register of cancelled voting passes (containing the numbers of voting passes that are invalid, e.g. because a replacement has been issued). The register would have to be compiled very quickly (in the space of two days) and distributed to all polling stations before the start of the election. In order to produce the national register each municipal authority would have to send a list of the voting passes cancelled in that municipality to a central point: here the numbers of all the cancelled passes would be collected into a single database and distributed to the municipalities. Although the national register could conceivably be in paper form, it would be more logical to envisage it as an electronic file available on a free-standing computer which every polling station should have. It would be advisable to check voting pass numbers electronically, so as not to delay the ballot at the polling station; this would also avoid errors in typing the numbers or reading them in the register of cancelled voting passes.

Voting at any polling station outside the voter's municipality would also mean that votes could be cast for any district at a polling station. When counting the votes at the polling station the results would therefore need to be able to be grouped by district. The Commission envisages that the polling stations would transmit the count to a central facility in electronic form. This distribution platform would count the votes cast by district electronically and then distribute the results to the principal electoral committees electronically. Each of these would determine the results of the election in its district from the official reports from the polling station committees and the count and send it, just as at present, to the Central Electoral Committee. The polling station committees would continue to send their official reports with counts to the principal electoral committee, so the municipalities would have provisional results that they could announce, just as in the present election process.

To enhance transparency and verifiability, the central facility should publish on the Internet the counts of votes cast at each polling station. It is important to stress that the polling station committee's count is a provisional result, not the actual election result, which will be announced by the Central Electoral Committee. For the sake of verifiability, however, the Central Electoral Committee would need to announce any discrepancies from previously announced counts.

4.3.2 Discussion

The Commission considered whether it would be possible to introduce VAPS outside the voter's municipality quickly, and came to the conclusion that there are obstacles to this if it is combined with a new method of electronic voting at polling stations. If the recommendation on the new method of voting at polling stations is adopted, VAPS outside the voter's municipality should

³³ There are 443 different candidate lists for municipal council elections, which would all have to be available at all the polling stations.

preferably not be introduced until the authorities responsible for organizing elections and the public are accustomed to the new system of voting at polling stations.

Implementing so many changes all at once would be too risky, in the Commission's opinion. Our proposal would also provide an opportunity to spread the financial investment required for the changes over a period of time. Experience of voting at any polling station in more than one election could be gained on a limited scale in municipalities where municipal district council elections are held simultaneously with municipal council elections.

The Commission would stress, as regards the introduction of VAPS outside the voter's municipality, that – as already noted – this is only feasible if *ballot printers* and *vote counters* are used, or voting devices with a *paper trail*. To use pre-printed ballot papers would make it impossible to introduce VAPS outside the voter's municipality, and it would be problematic even in municipalities where district council elections or referendums in municipal districts are also held.

5. Voters with impairments

5.1 Introduction

In response to letters received from the Netherlands Council for the Disabled and Chronically Ill, the Disability in the Community Task Force and Viziris (network organization for the visually impaired), and discussions with their representatives, the Commission also drew up recommendations to improve access for people with physical impairments and hence participation by these voters.³⁴

As responsibility for choosing polling station premises and setting up polling stations is highly decentralized, responsibility for making polling stations accessible to voters with physical impairments rests with the municipal authorities. Each municipality has a different policy on the matter, with the result that some municipalities provide more facilities to encourage the physically impaired to participate in elections than others. Also, some polling station committees are more accommodating than others. In this connection the Elections Act only lays down that the committee must permit a voter found to be in need of assistance on account of his physical condition to be assisted (Section J 28).

The Council for the Disabled and Chronically Ill has made a large number of recommendations, some of which are addressed to political parties and other organizations whose work lies outside the Commission's remit. One area that does fall within its remit, in the Commission's opinion, is the obligation that the access requirement places on municipalities to ensure that voters with physical impairments are able to cast their votes within a reasonable distance of their homes. In the case of elections where voters can choose which polling station to use this means that not all polling stations need be adapted to the needs of this group. Given that adapting all polling stations to these needs would presumably not be possible within the foreseeable future, the access requirement is another argument in favour of non-place-dependent voting as recommended by the Commission, with voters themselves choosing the polling stations that suit them best.

So far this has been possible under Section K 1 of the Elections Act, under which a voter is required to apply to take part in the ballot at the polling station of his or her choice. If the application is granted, he or she is issued with a voter's pass. If voting at the polling station of the voter's choice becomes the rule and every voter receives a voting pass instead of a voter registration card, this will make it easier for voters with impairments to vote at polling stations which provide them with easy access.

It is central government's responsibility to draw the municipalities' attention to their responsibility to make enough polling stations accessible to voters with physical impairments and to encourage the municipalities to listen to the organizations that represent them.

³⁴ The letters and approved reports of meetings are included as Appendices 14 and 15 respectively.

The Council for the Disabled and Chronically Ill, the Disability in the Community Task Force and Viziris asked the Commission whether people with impairments that prevent them from going to or being taken to a polling station, or from casting their votes there, could be allowed to vote by telephone. The Commission asked the spokesmen for these three organizations how the group of people who would be eligible for this could be defined.

5.2 Discussion

The municipalities are responsible for providing enough polling stations that are accessible to voters with physical impairments. In the Commission's opinion this responsibility means that every voter with an impairment who is able to attend a polling station, with or without assistance, must be able to actually cast his or her vote there. This is not just a question of the accessibility of the building and the specific location of the polling station but also of providing adjustable voting desks for voters who need to cast their votes seated in their wheelchairs and voting equipment for visually impaired voters that gives instructions through headphones. When sending out voter registration cards or voting passes, municipalities should indicate which polling stations have special access for voters with physical impairments.

The Commission would however ask everyone involved in the election process to consider the recommendations that the Council for the Disabled and Chronically Ill has made on the matter and will no doubt continue to make. It is not just a question of rules and regulations but above all of the attitudes of all concerned and their willingness to encourage active participation in the election process by voters with impairments. In many cases it is a question not so much of regulations but of whether those involved in the process are attentive to these voters during the preparations and on election day.

The possibility of applying for a voter's pass that enables them to vote at the polling station of their choice to some extent meets the need of voters with impairments to vote at polling stations that take account of their limitations. This does mean, however, that municipalities must inform these voters which polling stations are adapted to their needs when sending out polling cards or before.

If voting passes become the rule and all voters can vote at the polling station of their choice, this will also improve access for voters with impairments. The municipalities will still be responsible for providing voters who have impairments with information (in suitable form in the case of a visual impairment) on adapted polling stations/polling stations that could be problematic for those with particular impairments. Eventually, adaptation to voters with impairments should be the rule and polling stations with obstacles to them the exception, and these should be mentioned when sending out voter registration cards or voting passes.

Based on the proposal by the spokesmen for the Council for the Disabled and Chronically Ill, the Disability in the Community Task Force and Viziris, the Commission recommends that telephone voting should be made available to voters unable to vote at a polling station because of their impairments. In the case of this group the need to provide access to elections outweighs the principles of secret and free suffrage and transparency. The Council for the Disabled and Chronically Ill, the Disability in the Community Task Force and Viziris recommend that this group

be defined using the International Classification of Functioning, Disability and Health (ICF) of the World Health Organization (WHO; see Appendix 15.12), and the Commission adopts this recommendation. The ICF classification is a statutory element in eligibility for health care and individual facilities under the Exceptional Medical Expenses and Social Support schemes. We recommend that people classified as totally dependent under 'walking and moving' and 'moving around using transportation' be regarded as eligible for telephone voting. The spokesmen of the Council for the Disabled and Chronically Ill, the Disability in the Community Task Force and Viziris take the view that precisely who meets the criteria can be ascertained through the Centrum Indicatiestelling Zorg (CIZ, the body that assesses people's care needs), care administration offices and municipalities' Social Support scheme information desks. The Commission would note, however, that the ICF criteria must be applied strictly and as uniformly as possible throughout the country, so that the facilities associated with the classification – in this case the right to vote by telephone – can only be used by those for whom they have been created.

Lastly, the Disability in the Community Task Force asked the Commission to consider an incident where a chairman of a polling station committee refused to allow a voter with a mental impairment to vote. The Commission would stress that anyone holding a voter registration card, voter's pass or voting pass is thereby authenticated as eligible to vote and should therefore be allowed to take part in the election. It must be established, however, whether the person producing the voter registration card, voter's pass or voting pass to the polling station committee is actually the person whose name is stated thereon – this is the purpose of compulsory identification. If the person whose name is stated on the voter registration card, voter's pass or voting pass is identical to the person producing that document, that person is authenticated as having the right to vote. The polling station committee has no power to cast doubt upon this, unless the identity document produced indicates that the person is under the minimum voting age, in which case the committee will have discovered an error by the municipal administration in issuing the voter registration card, voter's pass or voting pass.

The above incident led the Commission to question whether it is still right to confine the right of a voter to be assisted to cast his or her vote to voters in need of assistance on account of their physical condition under Section J 28 of the Elections Act. If a voter with a mental impairment needs help to operate the *ballot printer* because of that condition, he or she should also be permitted assistance, in the Commission's opinion. The assistance must be given to cast the vote, however, not to choose how to vote. There also need to be facilities for practising using the voting equipment, possibly in the form of an electronic simulation on the Internet.

6. Proxy voting

6.1 Introduction

Proxy voting is a common phenomenon in the Netherlands, compared with other countries. Based on the data available from municipalities, proxy votes account for about 15% of the votes cast.³⁵ The magnitude of this phenomenon and the simplicity of appointing a proxy and having the proxy document recognized have led to criticism from the OSCE/ODIHR observers, among others. In their report of 12 March 2007 on the general election of 22 November 2006 they noted that the Netherlands has a long tradition of proxy voting and that this practice generally commands public support. It is based more on trust than regulation. The OSCE/ODIHR considers it would be worthwhile to consider revising the regulations on, and practice of, proxy voting to bring it more into line with the principles of equal suffrage and the secret ballot, in accordance with §7.4 of the OCSE Copenhagen Document of 1990.³⁶

The possibility of proxy voting was initially restricted, in that voters were only permitted to appoint close blood relatives, relatives by marriage and housemates to vote on their behalf.³⁷ Since the 1960s the range of people who are allowed to serve as proxies has been extended on a number of occasions, though the number of proxy votes any one person is permitted to accept has remained limited to two. A person who has accepted one or two proxies must cast these votes at the same time as his or her own vote, thus providing an automatic check that the limit of two is not exceeded.

Section L 1 of the Elections Act defines the right to appoint a proxy very broadly: any voter who expects not to be able to take part in the ballot is permitted to vote by proxy. There is no requirement, in other words, to state any reasons for this or to substantiate them. Reasons can range from not being available because of having to work elsewhere or because of holidays or illness, through physical impairments that make it impossible to vote at a polling station, to imprisonment or mere laziness. Serious illness, admission to hospital, severe physical impairments and imprisonment are cases of compulsion, in the sense that the voter is unable to vote himself or herself and thus obliged to appoint a proxy in order to take part in the ballot. In principle a voter is free to choose anyone as his or her proxy, however, so there is no way of ruling out the possibility that the proxy has been assigned under duress to a family member or housemate upon whom the voter is dependent. This phenomenon is referred to as 'family voting'.

While the option of proxy voting makes for greater access, in the case of family voting there is the risk of the principles of free and secret suffrage being breached.

³⁵ Based on data on the general election in 2002 (38 municipalities) and municipal council elections in 2006 (67 municipalities), Remote Electronic Voting Project, MolKR.

³⁶ The relevant passage in the Document of the Copenhagen Meeting of the Conference on the Human Dimension of the Conference on Security and Cooperation in Europe, 5-29 June 1990 (Appendix 9), reads as follows:

(7) To ensure that the will of the people serves as the basis of the authority of government, the participating States will ... (7.4) ensure that votes are cast by secret ballot or by equivalent free voting procedure, and that they are counted and reported honestly with the official results made public;

³⁷ Under Section K 5 of the Elections Act of 13 July 1951 the only categories of person who could be designated as proxies were the spouse, relatives by blood or marriage up to the third degree, the spouse of a sister-in-law or brother-in-law, or one of the voter's housemates.

6.2 Discussion

The OSCE/ODIHR observers rightly note that proxy voting has the support and trust of the public. The Commission considers that this trust is based on the idea that, in principle, everyone is free to appoint someone else as a proxy or not. If a voter does so, this is based on trust that the other person will use the proxy in accordance with the voter's wishes. This confidence was able to grow as the range of people who could be appointed as proxies was enlarged, hence voters had more freedom of choice, as has been the case since the 1970s. The Commission regards this trust on the part of voters appointing proxies in those proxies as being typical of Dutch society. There is a risk of the principle of secret suffrage being violated, albeit as a result of the choice made by the person appointing the proxy. The risk is more serious the more the choice is dictated by circumstances – serious illness or physical impairment, imprisonment, being away from the Netherlands, etc. – or the smaller the range of people who can be appointed as proxies.

The Commission acknowledges that for people who are seriously ill, physically impaired or imprisoned the fact that they are obliged to vote by proxy (or not to take part in the election) is a restriction, even if they have some freedom of choice in designating a proxy. With this group in mind the Commission examines the advantages and disadvantages of the Swedish option of having a postal vote delivered to the polling station by a messenger in Chapter 10.

From the point of view of the safeguards that need to surround the election process, the phenomenon of family voting – appointing a proxy because the voter is under duress from that person – is the one that causes the most concern. Where it occurs it jeopardizes accessibility and free suffrage. There is no information on the extent of this phenomenon, but the supposition that it exists, given the importance of the principles at stake, is sufficient cause to consider it.

The Commission first discusses whether the existing proxy voting system provides opportunities for misuse and whether this could be tackled preventively. Under Section L 14 of the Elections Act one way of appointing a voter registered in the same electoral district as a proxy is for the person appointing the proxy and the proxy himself or herself to sign a proxy declaration on the voter registration card. This turns the voter registration card into the proxy document. If the option of non-place-dependent voting using voting passes were to be introduced, the voting pass could be converted into a proxy document, raising the issue of identification. It is not inconceivable that the declaration on the voter registration card or voting pass may not have been signed by the voter appointing the proxy. Some guarantee of authenticity could be gained by laying down that any such proxy document – i.e. any voter registration card or voting pass converted into a proxy – is only valid and can only be accepted as a proxy document by the polling station committee if the proxy produces a photocopy of an identity document of the voter. The polling station committee would keep this photocopy along with the proxy document and the proxy's voter registration card or voting pass. While the Commission realizes that producing a photocopy of an identity document of the voter does not provide absolute certainty as to the authenticity of the signature, it would help to prevent simple misuses of voting passes that have been left lying around. The Commission is aware that this requirement would raise the barrier to proxy voting slightly, but

considers this to be justified in order to reduce the incidence of fraud using proxy documents not signed by the voters themselves.

As regards prison inmates, it could be examined in consultation with the Ministry of Justice and the municipal authorities whether, given the need for order and security in penal institutions, it would be possible to open special mobile polling stations there for part of a day. The mobile station would need to have a ballot printer and a ballot box which could be used by both inmates and staff. Mobile stations of this kind opened for part of a day could also be set up in hospitals, nursing homes, etc. These stations would have a three-member polling station committee but would differ from other mobile polling stations in that they would only be open for part of a day and not to the public. The ballot box would then have to be taken to a fixed polling station, where the count would take place once the ballot closed. Separate statutory provisions would have to be introduced on the non-public nature of these stations, the non-standard opening hours, the transport of the ballot box and the count at a normal polling station. If this option is rejected, all that remains for prison inmates and some patients is proxy voting, as currently laid down for the former in Section B 6 of the Elections Act.

To combat family voting the authorities need to stress the strictly personal nature of the individual right to vote in the information provided at election time and e.g. assimilation courses. The great benefit of everyone in our society being able to have a political vote in freedom and in secret, as set out in §7.4 of the OSCE Copenhagen Document of 1990, should be pointed out. The need to produce a photocopy of an identity document of the person appointing the proxy could raise something of a barrier to voting under compulsion and reduce the incidence of fraud with voters' signatures.

The Commission realizes that, in spite of these proposals, the availability of proxy voting remains broad in the Netherlands, and it considers this to be desirable from the point of view of access. It takes the view, however, that the admonition by the OSCE/ODIHR observers to bring the regulations and practice more into line with §7.4 of the OCSE Copenhagen Document of 1990 can be heeded by facilitating voting by electors with impairments, making telephone voting available to those who are unable to vote at a polling station, and setting up special mobile polling stations in hospitals, nursing homes and penal institutions. The Commission also anticipates that introducing the option of voting at any polling station, including outside the voter's municipality, will reduce the need to appoint proxies. We do not propose abolishing the possibility of converting a voter registration card or voting pass into a proxy document: while this would reduce the number of proxies it would also restrict access to elections for people prevented from voting themselves at a polling station at the last minute (on account of illness, foreign travel, etc.).

7. Voters abroad

7.1 Introduction

Since 1 November 1989 voters who are actually resident abroad on nomination day for a general election (Category 1) or away from the Netherlands on polling day on account of their work or business or that of their spouse, registered partner, partner or parent on the day of the election (Category 2) have been permitted to vote by post provided they have applied to do so within the time limit (Elections Act, Section M 1). This provision also applies to European Parliamentary elections, since under Section Y 2 of the Elections Act the provisions of Part II concerning the election of members of the House of Representatives of the States General apply *mutatis mutandis*, except as stipulated in Chapter Y of the Act or pursuant to the Act of 20 September 1976 concerning the election of the members of the European Parliament by direct universal suffrage.³⁸ Dutch voters participating in European Parliamentary elections in the Member State where they are resident are excluded from postal voting. The Commission discusses the particular problems this causes in the next chapter.

Dutch citizens who are actually resident outside the Netherlands (Category 1) are not residents of a Dutch province or municipality and therefore not eligible to vote in provincial or municipal council elections. The right to vote by post in the case of Category 2 electors, who *are* eligible to vote in provincial and municipal council elections, is restricted to general elections and European Parliamentary elections; if they wish to exercise their vote in provincial or municipal council elections they must appoint another voter in their province/municipality to vote on their behalf under the existing law and regulations.

Under the MolKR's Remote Electronic Voting Project, electors eligible to vote by post were also permitted, as an experiment, to vote by Internet or telephone in the European Parliamentary election on 9 June 2004. The experiment was repeated, as regards Internet voting, in the general election on 22 November 2006 (telephone voting was not permitted). The statutory basis for these experiments was the Remote Electronic Voting (Experiments) Act of 11 December 2003, which ceases to apply on 1 January 2008. The State Secretary for the Interior and Kingdom Relations has announced, however, that the Act is to be renewed for a possible experiment in the European Parliamentary election on 11 June 2009.

7.2 Experience so far with remote voting

The 2004 and 2006 experiments have been evaluated and detailed risk analyses carried out.³⁹ The option of voting by telephone or using the Internet was assessed favourably, much more favourably than postal voting. Of a total of over 15,000 registered voters abroad, however, fewer than 500 availed themselves of the opportunity to vote by telephone, which is why this option was not included in the 2006 experiment.

³⁸ Council Directive 93/109/EC of 6 December 1993 was implemented in the Elections Act.

³⁹ Parliamentary papers II 29200 VII No. 51; 30 800 VII, No. 48, Appendices 3 and 4.

The Commission has looked in particular at the experience of voters abroad as reported in the evaluations of the experiments carried out by the MolKR. Criticisms of postal voting are that as a result of delivery times, and in some cases incorrect delivery, electors do not receive the postal voting slip in time (if at all), or the return letter containing the ballot paper and postal voting slip does not reach the Municipality of The Hague in time (if at all). A factor here is that the voting documents sent out to registered electors are not available until relatively late, because of the period of 43 days that elapses between nomination day and election day, during which the lists of candidates have to be checked and approved before the ballot papers can be printed and sent out. From the number of applications for registration submitted it is clear that the vast majority⁴⁰ of electors in both categories do not register, thus failing to carry out the first step required in order to vote from abroad.⁴¹ The number of electors abroad who successfully registered for the European Parliamentary election was 15,991, of whom 8,795 stated they wished to vote by post. The number of electors who actually voted was 12,030: 6,695 by post and 5,335 by Internet or telephone. 34,205 electors registered for the general election in 2006: 28,150 actually took part in the election, 19,815 by Internet and 8,335 by post.⁴²

Registration is required for each election (and here we are only talking about general elections and European Parliamentary elections).⁴³ The Municipality of The Hague keeps a 'semi-permanent' register of electors who registered in previous elections.⁴⁴ Electors on that register are sent unsolicited a voting eligibility registration form (D3 registration form) before each general election or European Parliamentary election. The register is 'semi-permanent' in the sense that an elector who has not submitted a registration application for the previous election is removed from the register and therefore does not automatically receive a D3 form for subsequent general or European Parliamentary elections. As part of the Remote Electronic Voting experiments D3 forms were sent to electors on the semi-permanent register by e-mail in many cases, and registration applications could also be submitted by e-mail. Experience showed that this method of delivery overcame the problems of using the postal service.

The vast majority of the estimated 700,000 non-resident Dutch citizens failed to meet the requirement to register before nomination day – i.e. 43 days before polling day. Registration is necessary because the authorities have to ascertain electors' names and addresses and citizenship (a document proving Dutch nationality has to be submitted). There is no national register of non-resident Dutch citizens. Not every non-resident Dutch citizen has a tax and social security number, hence in due course a Citizen Service Number.

The size of Category 2 – electors who will be away from the Netherlands on polling day on account of their work or business or that of their spouse, registered partner, partner or parent – is not known. The number varies from day to day. They have to submit their postal voting

⁴⁰ The precise number of non-resident Dutch citizens eligible to vote (Category 1) is not known. Estimates range from over 700,000 to a maximum of 1 million.

⁴¹ Again, only a small proportion of voters who are temporarily away from the Netherlands (Category 2) take advantage of the right to vote.

⁴² Sources: MolKR, Municipality of The Hague.

⁴³ Elections Act, Section 3.

⁴⁴ Elections Act, Section D 3a.

applications by the 28th day before the election to the mayor of the municipality where they are registered as electors. If the application is approved, the mayor of that municipality sends it as soon as possible to the Mayor of The Hague. The remainder of the procedure is the same as for non-resident electors registered with the Municipality of The Hague. Strangely, the option of voting from abroad by post is not available to the – presumably large – group of voters who are away from the Netherlands on polling day for reasons other than those stated in Section M 1 of the Elections Act (on holiday, visiting family, etc.). In their case, however, many of them will not know their address abroad more than a month in advance, so cannot register for that reason.

As regards the postal voting procedure, §2 of Chapter M of the Elections Act provides for the possibility of setting up postal voting electoral committees at Dutch diplomatic or consular missions and requires such committees to be set up in the Netherlands Antilles and Aruba. The registration procedure at the Municipality of The Hague remains the same, but in this case the voting documents are sent out by diplomatic mail to the head of the diplomatic or consular mission in question or the Dutch representative in the Netherlands Antilles or Aruba.

7.3 Discussion

The Commission notes that only a small proportion of electors in Categories 1 and 2 actually take part in the elections. Whether electors who do not submit registration applications fail to do so because they find the red tape too daunting, because they take a conscious decision not to avail themselves of the right to vote granted to them as non-residents, or because they are unaware of their right to vote in general or European Parliamentary elections, is impossible to say. As regards European Parliamentary elections there is a further group of electors who vote in the Member State where they are resident, in which case they do not have the right to vote in the country of which they are nationals.

Category 1

The experience of electors abroad who did submit registration applications indicates that they found the information provided on the web sites www.kiezenuithetbuitenland.nl and www.kiesraad.nl adequate. The site of the Municipality of The Hague also provides information. While there was criticism of the semi-permanent (temporary) nature of the register, contamination of the address database as a result of unnotified changes of address needs to be avoided. The correspondence via the Internet was found to be satisfactory. This form of message traffic overcomes the problems of using the postal service to a large extent.

Message traffic with this category of electors as such is unavoidable, certainly as long as there is no central register of non-resident Dutch citizens,⁴⁵ since it needs to be ascertained for each general or European Parliamentary election whether the person concerned still has the Dutch nationality and is eligible to vote.

⁴⁵ The Commission is aware that there are plans to create a Register of Non-Residents (RNI, Register Niet-ingezetenen). Whether this will be introduced, and if so when it will become operational, is not known. Many non-resident Dutch citizens do not have a tax and social security number (Citizen Service Number in future).

Although there are problems with Internet voting, as regards safeguarding the principles of transparency and free and secret suffrage, that lead the Commission not to wish to make this option available for the time being to electors who are able to cast their votes in the Netherlands, for electors abroad the requirement of accessibility – ability to take part in elections as simply as possible – must prevail. The same is true of the option of voting by post, which the Commission does not recommend for voting in the Netherlands from the point of view of safeguarding the principles of free and secret suffrage. As regards the choice between Internet and postal voting, the Commission's preference is for Internet voting, as it overcomes the problems of incorrect delivery or delays in the postal service. The option of postal voting should be retained for those who are unable or unwilling to vote using the Internet.

The Commission proposes that the register that the Municipality of The Hague keeps of electors who have registered for general or European Parliamentary elections should take on a permanent nature, in the sense that registered non-resident Dutch citizens should only be removed:

- a. on their own request,
- b. when moving back to the Netherlands or
- c. if they are found to have lost their Dutch nationality.

An unnotified change of address should be regarded as a request for removal.

To improve awareness of the right to vote in general and European Parliamentary elections among non-resident Dutch citizens, when receiving an application for renewal of a Dutch travel document, and in other communications, the consulates and consular departments of foreign missions should issue a leaflet providing brief information on this right, including the web sites mentioned above and the e-mail and postal address of the Municipality of The Hague (verkiezingen@dbz.denhaag.nl; Bureau Verkiezingen, Dienst Burgerzaken, Gemeente Den Haag, PO Box 12620, 2500 DL The Hague). As soon as polling day for a general or European Parliamentary election is known it should be included in the leaflet.

Also, anyone applying for a Dutch travel document should be explicitly asked whether or not they would like to state their postal address and e-mail address for the Municipality of The Hague's register of non-resident electors. The consulate or mission should then ensure that the name and address data, including any e-mail address, are passed on to the Elections Office (Bureau Verkiezingen).

Six months before polling day the Municipality of The Hague should send out a D3 registration form to all the persons on the register by e-mail, or in the absence of an e-mail address or if the e-mail is undeliverable by post (in the manner laid down in Section M 1 of the Elections Decree, as amended). This provision is the same as the present one, except that delivery by e-mail is made the general rule and the form is only sent by post if the person's e-mail address is not known or the e-mail address given is not working. Also, an elector who does not re-register for an election will remain on the register, so will again be sent a D3 form for the next election. The amendment to Section M 1 of the Elections Decree entails replacing airmail delivery with priority rate delivery, also in the case of Belgium.

If a register of non-residents were to be introduced in due course and all non-resident Dutch citizens registered in it, re-registration for each election (general and European Parliamentary) in which they are eligible to vote would no longer be necessary. The required voting documents would then be sent out under the same criteria for the sending of voting documents (voting passes) to electors resident in the Netherlands.

As regards voting by non-residents, the Commission proposes that Internet voting, as provided in 2004 and 2005, be made the general rule and that only non-resident electors who are unable or unwilling to vote using the Internet should continue to vote by post as provided in Chapter M of the Elections Act.

If Internet voting becomes the general rule for voters abroad, the question is whether responsibility for this should remain with the Municipality of The Hague – as is currently the case with postal voting – or be transferred to the MolKR. The Commission's preference is for the latter. This responsibility of the Minister of the Interior and Kingdom Relations would need to be enshrined in the Elections Act, with the details laid down in implementing regulations.

In the case of Internet voting, the role of postal voting electoral committees at Dutch diplomatic and consular missions and of the Dutch representation in the Netherlands Antilles and Aruba is no longer necessary.

By regularly organizing Internet voting for the small group of electors permitted to vote from abroad, the Netherlands will be in a position to keep an eye on current and future developments in this area and thus to maintain and develop its level of expertise.

Category 2

Category 2 applies only to electors who will be away from the Netherlands on polling day on account of their work or business or that of their spouse, registered partner, partner or parent. This includes military personnel on foreign missions. Otherwise few people make use of this option. There has not been any research into why this category of voters do not avail themselves of the postal voting facility. The Commission presumes that the red tape is an obstacle. It also needs to be remembered that the person concerned has to submit an application 28 days before polling day, giving the address to which the voting documents are to be sent. Electors who are temporarily away from the Netherlands for other reasons (on holiday, visiting family, etc.) are not eligible. The facility is only available for general and European Parliamentary elections. The postal voting procedure is not available in provincial and municipal council elections, although these electors are eligible to vote in them. In every case where the postal voting procedure is not available to an elector who is temporarily away from the Netherlands, the only option that remains is to vote by proxy.

The Commission recommends that consideration be given to extending the option of Internet or postal voting for Category 2 electors to provincial, municipal and district council elections. Unlike Dutch citizens who are permanently resident abroad and therefore not eligible to vote in provincial or municipal elections, Category 2 electors are eligible. The Commission also asked itself why the provision under Section M 1 of the Elections Act is restricted to electors who are away from the Netherlands on account of their work or business or that of their spouse, registered partner, or

parent. If it were to be extended to include those who are away for other reasons – on holiday, visiting family, etc. – the problem of not knowing where to send the voting documents is more likely to arise. Lastly, it would seem logical to make Internet voting available, in addition to postal voting, to the category of electors temporarily away from the Netherlands, and this should be the general rule.

8. Voting for the European Parliament

8.1 Introduction

In this chapter the Commission considers two questions:

- How, in European Parliamentary elections, a voter can be prevented from voting in both the Member State of which he is a national and the Member State of residence. This concerns the right to vote of (a) Dutch electors living in another European Union Member State and (b) electors who are nationals of another European Union Member State and actually resident in the Netherlands.
- How to prevent electors living in a Member State other than that of which they are nationals, where they are not registered as electors as a result of the regulations there, not being able to exercise their right to vote.

Dutch electors living outside the European Union or temporarily away from the European Union on account of their work or business or that of their spouse, registered partner, partner or parent are eligible to vote in European Parliamentary elections. The Commission's proposals in Chapter 7 apply to them.

Section Y 3 of the Elections Act lays down that, in addition to those who are eligible to vote in general elections, also eligible to vote are nationals of European Union Member States other than the Netherlands, provided they are actually resident in the Netherlands on nomination day, have attained the age of eighteen years on polling day and are not excluded from voting either in the Netherlands or in the Member State of which they are a national.

Section Y 6 of the Elections Act lays down that Dutch citizens who are actually resident in another European Union Member State shall only be registered as electors for a European Parliamentary election if they have undertaken not to vote in the election in another Member State as well. An application for registration will be rejected if the Municipal Executive of The Hague receives notification from the Member State in question that the applicant is registered as an elector in that Member State.

Section Y 31 of the Elections Act lays down that a national of a European Union Member State other than the Netherlands who is actually resident in the Netherlands shall vote either in the Netherlands or in the Member State of which he is a national. Section Y 32 of the Act is the provision under which the municipal executive of the municipality of residence registers these non-Dutch electors on application by them. Such registration is a precondition for taking part in the election. If the person is registered, the municipal executive informs the authority designated by the Member State in question that he is registered as an elector in the Netherlands.

Thus the system, which is in accordance with Council Directive 93/109/EC of 6 December 1993, provides (a) that the applicant for registration must undertake not to vote in the other Member State and (b) that the competent authorities must inform each other of the registration.

In practice this system has been found to contain loopholes, and the European Union has revision proposals in preparation.⁴⁶ The European Commission has ascertained that the exchange of information on registration between the authorities of the Member States is resulting in voters not being registered in time to exercise their right to vote.

In the current system equal suffrage is supposed to be guaranteed by means of (a) undertakings by voters and (b) exchange of information between the competent authorities. There are problems with this exchange of information: for example, there are three different alphabets in use in the expanded European Union, which creates particular difficulties with the transliteration of names; the procedures for establishing electoral registers are not the same, the deadlines are different and different media are used (paper, diskette, CD-ROM, etc.), with the result that data processing cannot be computerized. When exchanging information it is essential for names to be reproduced error-free in both directions, as it must be clear that both Member States are referring to the same elector. As a consequence of these defects in the exchange of information, some voters have voted in more than one Member State and others have not been able to exercise their right to vote, both of which are incompatible with the principles put forward by the present Commission. The European Commission has found that abuses involving a voter voting more than once in spite of his undertaking are uncommon. More common are cases where electors are unable to exercise their right to vote as a result of defects in the exchange of information, which was the reason for revising the Directive.

The European Commission proposes that the exchange of information be dropped, both in the case of candidates wishing to stand for election in a Member State other than that of which they are a national and in the case of electors resident in a Member State other than that of which they are a national. In its place the European Commission proposes requiring the Member States to apply effective, proportionate penalties to act as a deterrent against double voting (and double candidacy). In addition, the European Commission intends to produce a report on double voting and double candidacy based on information from the Member States after the first election following the introduction of the revised Directive.

The aim was for the revision proposals to be implemented in the national laws of the Member States by 30 June 2008, but the EU discussions have been subject to delay and the likelihood is that the Directive will not be implemented by the Member States in time for the 2009 election. The European Parliamentary election in June 2009 is therefore likely to take place on the basis of the unrevised rules.

8.2 Discussion

At the end of Chapter 2 the Commission pointed to the need for measures to prevent abuses. The Commission recognizes that exchange of information between the Member States will remain incomplete because of the short time in which it has to take place and the problems of transliteration. As a consequence the exchange of information does not work and thus has no

⁴⁶ Proposal for a Directive amending Council Directive 93/109/EC of 6 December 1993 (COM(2006) 791 of 12 December 2006).

preventive effect; on the contrary, the European Commission notes that electors are deprived of their right to vote as a result of the registration procedure. Making the penalty more severe is not a remedy if the risk of apprehension is low. Whether this will be increased by the reporting system envisaged by the European Commission we shall have to wait and see. The European Commission notes that abuses – voting more than once – are uncommon. The present Commission wonders whether this will still be the case if the registration requirement is dropped and the only formality is the undertaking by voters. A more severe penalty will only be effective if the risk of apprehension and the chances of actual and effective criminal prosecution are substantial. The first precondition is that the Member States must report as fully as possible on the electors who have registered with them, either as resident nationals of another Member State or as residents of a Member State other than that of which they are nationals. If these data are subsequently exchanged, it can be established whether voters have registered in more than one Member State in spite of their undertakings.

The only really foolproof system is to allow electors always to vote solely (a) in the other Member State or (b) in the Member State of which they are nationals. This solution is not only less European than the current arrangement, on further examination it is unworkable.

If electors living outside the country of which they are nationals were to be allowed to vote solely in the Member State of which they are nationals, there would be a problem with electors who have more than one nationality. If these nationalities were of European Union Member States, they would be able to vote in all the Member States of which they were nationals. Requiring them to give an undertaking would not help, as in many cases the authorities are unaware that a national of their country also has another nationality.

If, on the other hand, the right to vote were to be exercised solely in the Member State of residence, it would only be possible to vote for a candidate on a list filed in that Member State. Until such times as European lists of European parties are filed, many voters will prefer to vote for a candidate on a list filed in the Member State of which they are nationals. Furthermore, these electors will not normally be registered as eligible to vote in that Member State and would need to apply to be registered first.

The European Commission therefore wishes to retain the right to choose between the Member State of which the voter is a national and the Member State of residence.

In the European Commission's proposal, the subsequent reporting is vital in the present Commission's opinion (the subsequent reporting of voters registered in the Member States who are (a) resident in another Member State or (b) resident in that Member State but nationals of another Member State). If the reports are not reliable and full it will not be possible to track down electors who have registered in more than one Member State and prosecute them. In the absence of reliable and full reports a severe penalty will not have much preventive effect.

The importance of European electors living in another Member State than the one whether they are registered as eligible to vote actually being able to exercise their right to vote justifies dropping the prior registration required under the present system.

The present Commission therefore recommends that the government urge that the reports by the Member States be as full and reliable as possible when the proposal to amend Council Directive 93/109/EC of 6 June 1993 is debated. There must also be certainty that the prosecuting authorities in all the Member States will actually prosecute offenders. It must be clear in advance where the competence lies, i.e. in which Member State proceedings are to be taken. As this offence involves the perpetrator enabling himself to cast an extra vote by registering more than once (without it having been established whether he has actually voted in both Member States), an additional administrative or criminal law penalty of deprivation of the right to vote in one or more elections could be an appropriate sanction.

Once the Directive has been passed and implemented it will need to be strictly enforced.

9. Duties and responsibilities in the election process

9.1 Introduction

The Commission was asked whether responsibility for organizing the election process has been correctly allocated. To answer this question we talked to the Nederlandse Vereniging van Burgerzaken and the Electoral Council. We also asked Prof. M.J.W. van Twist to examine the various duties entrusted to the Electoral Council under the current legislation and identify the tensions that can occur between the duties of making recommendations, providing information, organization, conduct and supervision.

Deciding what principles the election process must safeguard, organizing elections and conducting them are the responsibility of government. There is only a secondary role for the private sector here, as a supplier of the aids the government wishes to use in elections. It would be wrong for the private sector to gain a decisive role in organizing the election process, e.g. as a result of special knowledge. The authorities need to ensure that they have sufficient expertise to weigh up the pros and cons (also in technical matters) and make choices, in full awareness of possible threats and risks. In a word, the government should be in charge and must guarantee to citizens that elections are in line with international, European and national standards and principles. This means that, if the Commission's recommendation to vote using *ballot printers* and *vote counters* at polling stations in future is adopted, the Minister of IKR must lay down the requirements (product specifications) and decide whether the devices available on the market meet them. This is part of the responsibility that the Minister of IKR has for the election process in the chain of responsibility. This also applies, for that matter, to Internet and postal voting for voters permitted to vote from abroad and to telephone voting for voters with impairments.

The Commission notes that there has been little if any criticism of the basic structure of the election process. In other words, the Minister of IKR is responsible for the law and regulations and their correct application, and the municipalities are responsible for organizing the elections. The Commission does however note that the responsibilities for the election process are not defined sufficiently clearly in the law and regulations. One example is the Minister's responsibility in the chain: the current law and regulations do not give the Minister adequate tools to fulfil it. The Voting Machines Decision-Making Commission has already come to the same conclusion and recommended that the Minister be given the powers needed to take charge. The Commission agrees with this conclusion and adopts it.

If the election process is to be verifiable the Minister should also preferably be responsible for the management, maintenance and security of electronic aids used in elections. This, however, will require close coordination with the municipalities, as they are responsible for the local organization of elections.

The new duties arising from the Commission's recommendations on voting at any polling station and Internet and telephone voting should be assigned to central government, i.e. the Minister of IKR. In view of the Government's standpoint on the report of the Voting Machines Decision-

Making Commission the logical course is for these to be assigned to the Ministry's Personal Records and Travel Documents Agency.

At present, supervision of the conduct of elections is only regulated as regards election day itself, when the polling station committees are responsible for ensuring their orderly conduct. It is the polling station committee that records in the official report whether any incidents have occurred and of what nature. There are regulations on the official report in the form of a model laid down by the Minister of IKR.

The heads of the polling station committees and the Central Electoral Committee decide what is to happen with the content of the official reports, after considering whether incidents at a polling station could have affected the result of the election. The Commission takes the view that this structure is adequate in principle but that there is room for improvement, especially as regards transparency and verifiability. In particular we are thinking of a framework to provide polling station committees with a clearer guide to drawing up official reports and make them more standardized. We also recommend that the official reports of the polling station committees should be published and kept (for a period to be specified in the Elections Act) for the purpose of academic research. Only then can lessons be learned for the future and steps taken to previous repetition.

9.2 Discussion

Supervision of the preparations for elections is not regulated at present. For the elections of 22 November 2006 and 7 March 2007 the Minister for Governmental Reform and Kingdom Relations therefore had to take ad hoc measures, such as sending inspectors to municipalities to ascertain what steps had been taken as regards voting machine security. The Commission considers that ad hoc measures should be replaced with a system of supervision for this preparatory phase of elections.

In this connection it is also important to ascertain whether there are potential tensions between the various responsibilities for the election process. Whether such tensions exist and whether they could give rise to problems has not been investigated as yet, and this needs to be done. This investigation should be carried out before the responsibilities for the election process as set out above are incorporated in the law and regulations.

The Commission identifies five responsibilities: providing information, making recommendations, organization, conduct and supervision. Tensions could arise within and between these five duties. The greatest risk lies in that of 'supervision'.

As the chart below shows, it is very difficult to combine a supervisory role with the advisory, organizational and administrative roles in the election process, as a supervisory body needs to check whether the elections have been conducted in accordance with the law and regulations. Where roles are combined, a situation can occur where the supervisory body has to judge its own functioning, and it is impossible to be certain that its judgment will be independent and impartial.

The risk is much greater where ‘conduct’ and ‘supervision’ are combined: the transparency and verifiability of the election process could be jeopardized if these roles become entangled.

	Providing information	Making recommendations	Organization	Conduct	Supervision
Providing information	I Not applicable				
Making recommendations	1 Not applicable	II Not applicable			
Organization	2 Not applicable	3 Not applicable	III Not applicable		
Conduct	4 Not applicable	5 Applicable	6 Not applicable	IV Applicable	
Supervision	7 Not applicable	8 Applicable	9 Applicable	10 Applicable	V Not applicable

Chart: Potential tensions between responsibilities⁴⁷
Roman numerals I-V: potential tensions within responsibilities
Arabic numerals 1-10: potential tensions between responsibilities

The Commission does not consider it prudent to create a new supervisory authority, but this responsibility cannot simply be assigned to one of the other authorities – including the Electoral Council – already involved in elections. This conclusion takes into account the fact that the Voting Machines Decision-Making Commission has established that these authorities do not at present have sufficient expertise (if any) to carry out this role.

The Electoral Council advises the government and the States General, on request or on its own initiative, on technical matters concerning the franchise or the conduct of elections.⁴⁸ While it is not responsible for the conduct of policy, it can guide policy with its recommendations. In this case the supervisory body would need to consider not only the conduct of policy but also the quality of the advice given. The Electoral Council also acts as the Central Electoral Committee for general elections, elections to the Senate and European Parliamentary elections, in which capacity it has an administrative role. Among other things the Central Electoral Committee determines the results of the elections and decides whether a recount is necessary. It would be wrong for the Electoral Council, acting as supervisory body, to then go on and check whether the Central Electoral Committee has acted in accordance with the law and regulations.

⁴⁷ From the report received from Prof. M.J.W. van Twist, ‘Potentiele spanningen tussen taakvelden in het verkiezingsproces: advies over de toekomstige invulling van taken van de Kiesraad’ (Potential tensions between roles in the election process: recommendations on the future allocation of Electoral Council responsibilities), report to the Election Process Advisory Commission, 2007 (Appendix 8).

⁴⁸ See Elections Act, Section A 2 (1) and <http://www.kiesraad.nl>.

Having regard to these points, the Commission recommends that an external audit of every election be carried out by independent experts.⁴⁹ An objective, independent and systematic assessment of the conduct of elections would provide additional certainty as regards results and contribute to the transparency and verifiability of the election process. Lessons for the future could moreover be learned from the audit. This should be seen as part of the ongoing scrutiny and review of the election process recommended by the Commission in Chapter 2.

To guarantee the independence of election audits the auditors for provincial and municipal council elections should be appointed by the Minister of IKR and those for general elections and European Parliamentary elections by the House of Representatives. The Commission does not consider it necessary to audit elections to the Senate, as these are limited in scale and transparent. The auditors should check the entire election process, i.e. both the preparations for and conduct of the elections. Immediately after each election, before the results are determined, the auditors should send an 'incident report' to the Central Electoral Committee, reporting any irregularities that occurred during the election process, the question being whether the elections have been conducted in accordance with the law and regulations. After the election, once the results have determined, the auditors should send a 'deliberative report' to the client, noting any areas where there is room for improvement and possibly including recommendations for the future. The Commission considers that the reports should be published so as to guarantee transparency and verifiability.

Election audits should include checks on the electronic aids used during elections, for example an EDP (electronic data processing) audit, also known as an IT audit. An EDP audit checks the IT systems for confidentiality, integrity (is the information accurate, reliable and timely) and availability.

⁴⁹ In line with the OSCE recommendation; The Netherlands Parliamentary Elections 22 November 2006, OSCE/ODIHR Election Assessment Mission Report (Appendix 12).

10. Miscellaneous topics

10.1 Introduction

The Commission begins this chapter by indicating where it has answered the questions put to it when it was set up. It then considers a question posed by the House of Representatives and a proposal from a correspondent.

10.2 The answers to the questions in the Commission's remit

Questions	Where to find answers
What role does IT play in the various stages of the election process (from the preparations for nominations to the appointment of new members to the representative body)?	Appendix 6
Which of these stages are in need of review in the light of new technologies and from the point of view of the electorate and the authorities?	Chapters 4, 5, 6, 7 and 9
Is responsibility for organizing the election process correctly allocated (the relationship between central and local government, the relationship between polling station committees, principal electoral district committees and the Central Electoral Committee), and what should the relationship be between the private sector and government as regards the use of aids (voting machines and election results computation systems)?	Chapters 5, 7 and 9
Is there adequate supervision of the proper conduct of the election process, who should supervise it and what enforcement powers should they have?	Chapter 9
What structural risks are associated with the current voting machines/electronic voting/pencil voting?	Chapter 3 and Appendix 2
Are there any alternatives conceivable to the current method of casting votes, e.g. non-place-dependent voting using the Internet?	Chapters 3 and 4
How do these alternatives compare as regards reliability, safeguarding the principle of secret suffrage and permitting recounts?	Chapters 3 and 4
Which is preferable: diversity (spreading the risk) or standardization (verification)?	Chapter 3
What is the relationship between the rapidity of technological development and the election process (could today's watertight solution be hacked into tomorrow)?	Chapters 3 and 4
To what extent do election aids remain usable when changes occur in practice, e.g. more parties standing in elections, combined elections?	Chapter 4

10.3 Answers to other questions

The House of Representatives also asked the Commission whether the Swedish election system could offer a solution to the problems with the use of voting passes for voting at any polling station. The Commission considers that its proposals to equip voting passes with authenticity features and the introduction of compulsory identification at polling stations could offer a solution to these problems.

10.3.1 The Swedish messenger system

When answering the question put by the House the Commission also formed an opinion on the Swedish practice of voting by means of a letter delivered to the polling station by a messenger. The Commission regards this method of voting as an alternative to proxy voting, especially for people who are prevented from attending a polling station themselves by special circumstances: serious illness, severe physical impairment, temporary absence from the Netherlands, imprisonment, etc.

Sweden has a system under which electors prevented from voting at a polling station by illness, physical impairment or age and imprisoned electors can have their vote delivered by a messenger. We discuss the system briefly below.

In addition to those mentioned above, the following categories are also allowed to have their vote delivered by a messenger:

1. Electors served by 'rural' postmen (*Posten AB*'s)
2. Electors who have been remanded in custody
3. Electors who are inmates of a penal institution and are not permitted to vote at the same mobile polling station as other prisoners for security reasons

The following categories of person are permitted to act as messengers:

1. The spouse or partner, children, grandchildren, parents, brothers and sisters of the elector or his/her spouse/partner
2. Carers
3. Messengers designated by the municipal authority
4. Postmen
5. Staff of remand centres and penal institutions

Three types of ballot paper are used in the elections: a ballot paper with the party name and names of candidates, a ballot paper with the party name, and a blank ballot paper. Electors wishing to vote by messenger can order a set of ballot papers and envelopes from the Central Election Authority (by telephone or Internet) or from the political party of their choice. The ballot papers and envelopes are also freely available from the various mobile polling stations.

The elector fills in the ballot paper himself or herself, places it in an envelope and seals it. The envelope is then placed in a special 'voting by messenger' envelope in the presence of the

messenger and a witness. On this envelope the voter writes his or her name and identity number, confirms that he or she has cast the vote in accordance with the requirements, and that he or she meets the requirements for voting by messenger. The messenger and the witness write their names, identity numbers and addresses and confirm that the voter has cast his or her vote in accordance with the requirements. If the elector is not known personally to the messenger he or she must produce identification.

Voting by messenger must not take place more than 24 days before election day.

The voter gives his or her polling card to the messenger, unless the envelope is handed in to the voter's polling station. At the polling station the election official checks whether the envelope is in order. After verifying the messenger's identity the official opens the envelope and checks whether it contains a ballot envelope. Before accepting the ballot envelope the official inspects the electoral register to check that the voter is eligible to vote and has not already voted. The official places the ballot envelope in the ballot box and marks the electoral register to show that the voter has cast a vote.

A voter who has voted in advance at a mobile polling station or by post is permitted to change his or her vote by voting at the polling station himself or herself on election day. This vote is then accepted and the advance vote declared invalid. Every voter (at a fixed or mobile polling station) casting a ballot places it in an envelope before depositing it in the ballot box. The votes cast in advance at the mobile polling station are placed in a window envelope along with the polling card (bearing the voter's identity) and sent to the polling station, where the voter is marked with a 'P' in the electoral register. The envelope containing the ballot is not opened until the ballot is closed. When a voter personally casts a fresh vote his or her name is marked with a '/' in the electoral register; the vote cast in advance can then be identified and destroyed. Only when the ballot has closed and all the voters who have cast votes in advance have been marked in the register are the advance votes deposited in the ballot box.⁵⁰

We do not have a category of 'voters served by rural postmen' in the Netherlands; this evidently relates to the isolated, thinly populated areas of Sweden.

The system of voting by messenger-delivered letter would not seem to be particularly useful, considering that it does not offer a solution for the relatively large group of voters who are temporarily away from the Netherlands and those with severe impairments, who are not likely to see this as their first option, their preference being for telephone voting. In Chapter 5, **Voters with impairments**, the Commission develops a proposal for telephone voting for voters with impairments severe enough to prevent them casting their votes at a polling station, even if it has been adapted. In Chapter 6 the Commission proposes that the feasibility and practicality of setting up special mobile polling stations in penal institutions (also hospitals and nursing homes) be examined. The mobile station would need to have a *ballot printer* and a ballot box which could

⁵⁰ Election Authority, Elections in Sweden. The way it's done! (available on-line at <http://www.val.se/pdf/electionsinsweden.pdf>); Elections Act 2005 (available on-line at http://www.val.se/pdf/2005_elections_act.pdf).

be used by both inmates and staff. The ballot box would then have to be taken to a fixed polling station, where the count would take place once the ballot closed.

As we have seen in Chapter 7, not much use is made of the facility offered under Section M 1 of the Elections Act to voters temporarily away from the Netherlands on account of their work or business. There has not been any research into why this category of voters do not avail themselves of the postal voting facility. The Commission presumes that the red tape is an obstacle. It also needs to be remembered that the person concerned has to submit an application 28 days before polling day, giving the address to which the voting documents are to be sent. Voting by messenger-delivered letter is not a solution for this group of voters or for those away from the Netherlands on polling day for reasons other than those stated in Section M 1 of the Elections Act (on holiday, visiting family, etc.). This group of voters thus remains dependent on proxy voting.

The postal voting option is not compatible with the ballot process envisaged by the Commission. The votes cast at polling stations are to be counted electronically. It would be going against this country's tradition to permit postal voting for groups other than Dutch voters abroad who are unable or unwilling to vote using the Internet.

10.3.2 Elections Act terminology

In a letter to the Chairman of the Commission of 20 March 2007, F.J.J.M. Andriessen of Zoetermeer points out that the terminology in the Elections Act is confusing.⁵¹ The Commission also takes the view that more consistency is required in the terminology used. Not every 'elector' (*kiesgerechtigde*, literally 'person eligible to vote') is a 'voter' (*kiezer*); he or she only becomes one by exercising the right to vote. Electors do not by definition have the right to take part in every ballot: in general elections this right obtains only in their own electoral district, and in provincial and municipal council elections only in their provincial electoral district or municipality. If voting at any polling station throughout the country is introduced, voters will only have the right to vote for someone on the list of their own electoral district or municipality. As the letter points out, a distinction also needs to be made between (a) citizens who are permitted to be present at the count under the principle of public access and (b) voters. Once a vote has been cast, a voter can be identified as such, as long as voting is still taking place at a polling station stated on the voter registration card, by checking the copy of data from the municipal records.⁵² If the voting pass is introduced, a voter will no longer be able to be identified as such, as the pass will have been handed in and kept by the polling station committee, and instead of a copy of data from the municipal records there will be a register of cancelled voting passes.

The Commission would therefore recommend that careful distinctions be made between the terms used in the Elections Act. In this connection the Commission notes that the Electoral Council considers in its recommendations of 22 June 2007 that the terms *identificatieplicht* (compulsory identification) and *legitimatieplicht* (compulsory authentication) are used

⁵¹ Appendix 15.1.

⁵² Elections Act, Section J 17 (1).

interchangeably, as synonyms. It may be true that the two terms are used interchangeably, but the Commission takes the view that an elector authenticates (*legitimeert*) himself or herself as such by lawfully producing a voter registration card or voting pass bearing his or her name. Production of an identity document enables it to be established whether the person producing the card/pass is identical to the person whose name is stated on that card/pass.

11. Financial consequences

11.1 Introduction

This chapter gives an overview of the possible cost of voting at polling stations in the way recommended by the Commission in Chapter 4. It does not include any indication of the cost of Internet voting for voters permitted to vote from abroad and telephone voting for voters with severe impairments. The MolKR has experimented with these methods of voting and therefore has information on the potential cost.

On average, elections take place once a year in the Netherlands, so the hardware and software needed for voting at polling stations, Internet voting and telephone voting will see very little use. The question, then, is what is the most economical way of procuring the hardware and software. The MolKR could carry out a market consultation to ascertain this.

The Commission presumes that the MolKR will set up a project organization to implement its recommendations. This will need to be operational for at least the next three years (until the end of 2010) and it will need to have technical as well as legal and administrative expertise. An organization comprising at least six staff (FTEs) will certainly be needed, and it will have to be able to grow on an ad hoc basis (e.g. in order to conduct tests).

The Commission is unable to say anything about the structural overheads: these will be highly dependent on the choices made as regards the procurement and management of the hardware and software for the new method of voting. If the Commission's recommendation on the method of voting at polling stations is adopted, the investment cost will be substantial, but it should be remembered that by no means all of this will be additional expense, as municipalities (those using voting machines) are already incurring expenses (both investments and annually recurring expenses for maintaining, storing and transporting the machines and preparing them for each election).

Below is an indication of the current cost (to a municipality) of using a voting machine.⁵³

Indication of current cost of Nedap voting machine		Price indication
Voting machine	Unit price	€5,000
Maintenance per voting machine per annum	Per unit per annum	€75
Results computation and election software	Per voting machine per annum	€10
Audio module	Unit price	€800
Programming/reading unit	Unit price	€900
Ballot sheet per voting machine per election	Per unit per election	€17
Voting pass	Per unit per election	€0.15

⁵³ Based on the purchase cost of a Nedap machine with Integrated Voting System software; source: Municipality of Rotterdam.

11.2 Electronic voting and paper voting

The Commission estimates the cost of voting at polling stations on the following basis:

- The prices stated are purely indicative. They are based on commercial prices (including VAT) for commercial off-the-shelf hardware. No tenders were obtained. The prices stated in the table are taken from up-to-date published price lists of suppliers or based on information available at the MolKR.
- There are some 9,000 polling stations in the Netherlands at present, and this figure is not likely to change in the near future. In order to deal with any faults on election day a reserve supply of 10% of the hardware is assumed.
- With a contract for approx. 10,000 *ballot printers* and vote counters the price of the hardware and software is likely to be at least 20% less than the supplier's normal unit price.
- It is assumed that the software for the *ballot printer* and vote counter does not yet exist and will therefore have to be developed (custom-built). The cost of this can only be determined once a functional and technical design has been drawn up, on the basis of which the cost of development can be computed.
- Measures to combat compromising radiation (TEMPEST) are only required for the *ballot printer*. The Commission consulted various Dutch and foreign experts on the matter, and from the information they provided TEMPEST-proof equipment can be assumed to be at least twice as expensive as commercially available equipment.
- The authenticity features in voting passes are assumed to be based on the technology used for rail tickets (holographic foil), which is relatively inexpensive. There are other, safer technologies (as used e.g. in travel documents), but they are expensive and not necessary for this purpose in the Commission's opinion. For each election a different detail of the authenticity feature will have to be changed, e.g. a different image in the foil hologram. The cost of printing the new voting passes cannot be estimated, as the price will depend on the required quality of paper, machine-readable strip and authenticity features.
- The cost of maintaining and storing equipment, and of configuring it for each election, has not been estimated, as it will be highly dependent on the choices made by the government.

Integrated ballot printer ⁵⁴		Type	Price indication
Prices are based on commercially available separate components			
Computer		Standard	€1,000
Touch screen		Standard	€2,000
Printer		Standard	€450
Storage device for reading candidate lists and election data		Standard	€10
Election software		Custom	Unknown
Cables etc.		Standard	€50
Transport aids		Standard	€200
Additional cost of TEMPEST version of ballot printer		Custom	Unknown
Subtotal for one ballot printer (excl. TEMPEST measures)		approx.	€4,200

⁵⁴ The price is an indication based on standard computer and laser printer hardware without additional EMSEC/TEMPEST measures and with no special feed/output trays and guides.

Integrated ballot printer ⁵⁴	Type	Price indication
Prices are based on commercially available separate components		
Integration into single ballot printer in single casing (with fold-out side panels)	Custom	Unknown

Ballot box for paper ballots	Type	Price indication
Ballot box	Standard	€100

Integrated vote counter with optical or bar code scanner ⁵⁵	Type	Price indication
Prices are based on commercially available separate components		
• Computer	Standard	€775
• Optical or bar code scanner inc. OCR software	Standard	€700
• Printer for printing results of count	Standard	€50
• Storage device for storing results of count	Standard	€10
• Counting software	Custom	Unknown
Subtotal for separate optical vote counter	approx.	€1,550
Integration into single vote counter in single casing with feed and output trays	Custom	Unknown

There are integrated *vote counters* on the market, used particularly in the United States of America. An electronic vote counter is often combined with a sealed ballot box which receives the scanned ballots. The unit prices of systems of this kind are around €4,000, based on publicly available information on tender procedures in the United States, in particular the states of California, Michigan and New York for e.g. ES&S (Model 100), Diebold (AccuVote OS) and Sequoia (Optech Insight). *Vote counters* used in the United States could probably only be used in the Netherlands with modifications, which could affect the price.

Total for electronic voting and paper voting

Electronic voting and paper voting	Unit price	Quantity	Price indication
Ballot printer (excl. TEMPEST measures) ⁵⁶	€4,200	9000	€37,800,000
Ballot box	€100	9000	€900,000
Vote counter with optical scanner ⁵⁷	€1,550	9000	€13,950,000
Authenticity features reader (optional)	€240	9000	€2,160,000
Reserve system			
Ballot printer	€4,200	1000	€4,200,000
Ballot box	€100	1000	€100,000
Vote counter with optical scanner	€1,550	1000	€1,550,000
Authenticity features reader (optional)	€240	1000	€240,000
Total hardware		approx.	€60,900,000

⁵⁵ The price is an indication based on standard desktop or laptop computer and inkjet printer hardware with no special feed/output trays and guides.

⁵⁶ Excluding the cost of custom-built software, integration into a single ballot printer and maintenance or configuration.

⁵⁷ Excluding the cost of custom-built software, integration into a single vote counter and maintenance or configuration.

Consumables per election ⁵⁸	Unit price	Quantity	Price indication
Voting pass with authenticity features (additional cost)	€0.10	12,265,000	€1,226,500
Ballot printout	€0.04	9,855,000	€394,200
Toner for ballot printer(s)	€100	10,000	€1,000,000
Total per election		approx.	€2,620,700

11.3 Voting at any polling station outside the voter's municipality

The Commission bases its discussion of voting at any polling station on the following assumptions:

- Each polling station would need to have a polling station computer with a voting pass scanner in order to check the electronic copy of the national register of cancelled voting passes.
- Once the ballot has closed and the votes have been counted, the polling station computer would be used to send the results to the distribution platform over a secure Internet connection.
- It is assumed that the software for the register of cancelled voting passes and for sending the results of the count to the distribution platform does not yet exist and will therefore have to be developed (custom-built). It is also likely that the custom software for the *ballot printer* and vote counter will have to be developed further. The cost of this can only be determined once a functional and technical design has been drawn up, on the basis of which the cost of development can be computed.
- The estimate for an Internet connection for each polling station based on HSDPA/UMTS/GPRS is based on standard subscriptions with telecom providers, assuming irregular use and low data transport requirements for the transmission of results of counts. The price is likely to be lower with a contract for some 9,000 polling stations.
- The cost of the distribution platform comprises hardware (web and application servers), maintenance and Internet facilities. It is also assumed that software for the distribution platform does not yet exist and will therefore have to be developed (custom-built). The cost of this can only be determined once a functional and technical design has been drawn up, on the basis of which the cost of development can be computed.
- Given the required availability of the distribution platform a redundant configuration will be needed, requiring more than one server.

Polling station computer	Type	Price indication
Polling station computer	Standard	€775
Voting pass scanner (price of commercial MRZ scanner for travel documents)	Standard	€350
Internet connection (HSDPA/UMTS/GPRS): modem	Standard	€100
HSDPA/UMTS/GPRS subscription (annual) ⁵⁹	Standard	€100

⁵⁸ For example, the 2006 general election, with 12,264,503 electors and a turnout of 9,854,998 (80.35%); source: <http://www.verkiezingsuitslagen.nl/>.

⁵⁹ The price can be estimated for one polling station: regular monthly subscription of €7.50 plus €1.50 per 1MB of data with a

Polling station computer	Type	Price indication
Software for register of cancelled voting passes	Custom	<i>Unknown</i>
Cables etc.	Standard	€50
Transport aids	Standard	€150

Subtotal for polling station computer **€1525**

Distribution platform	Type	Price indication
Counting and distribution software	Custom	<i>Unknown</i>
Secure and redundant Internet facilities	Standard	<i>Unknown</i>
Redundant servers (price per server)	Standard	€5,000
Web site	Standard	<i>Unknown</i>
Maintenance	Custom	<i>Unknown</i>

total of 6MB data transfer (annual cost).

12. Conclusions and Recommendations

12.1 Conclusions

1. The election process should safeguard the following principles: transparency, verifiability, fairness, eligibility to vote, free, secret and equal suffrage, and accessibility. These principles are the criteria by which existing and future methods of voting should be judged.
2. In practice the election process cannot provide 100% safeguards, so it is necessary to strike a balance between them. Feasibility and cost are also factors here, as is the point that the election process must be flexible enough to respond to new developments.
3. The principles can only be safeguarded sufficiently when voting takes place at polling stations.
4. Voting using paper ballots at polling stations is the preferred option on the grounds of transparency and verifiability. In practice, however, there have been problems with the counting of paper ballots.
5. A method of electronic voting at polling stations that provides equal safeguards is feasible, provided it produces paper ballots that can only be checked by the voters themselves.
6. The device on which voters make their choice should be protected against compromising radiation where this is feasible and financially justified.
7. The introduction of voting at any polling station outside the voter's municipality has major consequences for the organization of the election process (the register of cancelled voting passes and the distribution of votes to the various districts).
8. For voters living abroad or away from the Netherlands on account of their work or business or that of their spouse, registered partner, partner or parent, and people unable to vote at a polling station because of a physical impairment, the principle of accessibility can only be safeguarded if other methods of voting than voting at a polling station are provided for these groups.
9. The current election process does not provide sufficient access for voters with impairments. Greater efforts therefore need to be made to allow them to vote independently, so as to make them less dependent on proxy voting.
10. Internet voting for voters living abroad or away from the Netherlands on account of their work or business or that of their spouse, registered partner, partner or parent, and telephone voting for people with impairments that prevent them from voting at a polling station, would improve access to elections for these particular groups of voters.
11. The current registration procedure for voters living abroad needs to be improved as soon as

possible, as it is cumbersome and arouses antagonism among those concerned.

12. Proxy voting is well established in the Netherlands and should be retained in the future election process. The risk of proxies being misused by intercepting voter registration cards or voting passes needs to be reduced.
13. If a register of non-residents were to be introduced in due course and all non-resident Dutch citizens registered in it, re-registration for each election in which they are eligible to vote would no longer be necessary.
14. Deciding what principles the election process should safeguard, organizing and administering elections are a government responsibility. There is only a secondary function for the private sector, as a supplier of aids used in elections.
15. The current election process does not provide adequate checks on compliance with the law and regulations. If the election process is to be transparent and verifiable, the organization and conduct of elections must be audited.

12.2 Recommendations

1. The Commission recommends that voting at polling stations should remain the main method of voting in the Netherlands.
2. Voting at polling stations should be standardized throughout the Netherlands.
3. The Commission recommends introducing *ballot printers* and *electronic vote counters* at polling stations, because of the conceptual clarity of the system and the unambiguous results it produces. The paper ballots should be counted electronically. Manual counting should only take place if there are technical faults or there is reason to doubt that the equipment is working properly.
4. Violation of the secrecy of the ballot by picking up compromising radiation should be combated reactively by making this a criminal offence and reaching clearly defined agreements with the Public Prosecution Service on investigation and prosecution; in addition, if the cost is not prohibitive, the preferred option is to take preventive measures in line with the current NATO standard SDIP-27 Level B.
5. Voting passes for voting at any polling station should be provided with authenticity features.
6. Voters voting at a polling station should be required to identify themselves.
7. The introduction of voting at any polling station outside the voter's municipality should be deferred until voters are accustomed to the new method of voting recommended by the Commission.

8. Municipal authorities should actively inform voters about which polling stations provide access for voters with impairments.
9. Telephone voting should be provided for voters who are unable to vote at a polling station because of an impairment. This group should be defined with the aid of the ICF classification.
10. Assistance to voters as provided for in Section J28 of the Elections Act should be extended to voters in need of help on account of their mental condition.
11. A person appointed to vote on behalf of another person should be required to produce a photocopy of that person's identity document as well as his own identity document. The polling station committee should collect the photocopy along with the person's voting pass.
12. The principle of special mobile polling stations should be introduced in the law and regulations so that voting can take place in penal institutions, hospitals, nursing homes etc.
13. To combat family voting, publicity should be given, in the run-up to elections and in assimilation courses, to the importance of every voter casting his or her own vote in freedom and in secret as far as possible.
16. Internet voting should be the regular method of voting for voters living abroad or away from the Netherlands on account of their work or business or that of their spouse, registered partner, partner or parent. The option of postal voting should be retained for the time being for those who are unable or unwilling to vote using the Internet.
17. The semi-permanent register of non-resident electors kept by the Municipality of The Hague should be made permanent. Anyone registered should only be removed from the register:
 - on their own request,
 - when moving back to the Netherlands or
 - if they are found to have lost their Dutch nationality.An unnotified change of address should be regarded as a request for removal.
18. Anyone applying for a new travel document abroad should be asked whether or not they would like to state their postal address and e-mail address for the register of non-resident electors.
19. The Municipality of The Hague should send out the D3 registration form for voters abroad by e-mail. It should only be sent by post if the person's e-mail address is not known or the e-mail address given is not working.
20. The following text should be deleted from Section M1 of the Elections Act: 'or will be away from the Netherlands on polling day because of their work or business or that of their spouse, registered partner or parent'.
21. The text in Section M1 of the Elections Decree 'by airmail unless the address to which they are to be sent is in Belgium' should be amended to read 'franked at the priority rate'.

22. Responsibility for administering Internet and postal voting should rest with the Minister of the Interior and Kingdom Relations.
23. Responsibility for laying down requirements for and approving aids used in elections, and for the management, maintenance and security of these aids, should rest with the Minister of the Interior and Kingdom Relations.
24. The Minister of the Interior and Kingdom Relations should be given the powers necessary to exercise control over elections.
25. A framework should be devised to provide polling station committees with a clearer guide to drawing up official reports and make them more standardized.
26. Official reports should be kept for a period to be specified in the Elections Act for the purpose of academic research.
27. Every election should be audited by independent experts. Responsibility for auditing municipal council and provincial council elections should rest with the Minister of the Interior and Kingdom Relations, and for auditing general elections and European Parliamentary elections with the House of Representatives.
28. In the Council of Europe the government should work towards European technical standards for electronic aids used in elections and a European certification and testing system.
29. The law and regulations should be such that violations and breaches of the principles are precluded by preventive measures as far as possible and do not have to be enforced after the event by criminal prosecution.

List of acronyms and abbreviations

AWBZ	Algemene Wet Bijzondere Ziektekosten (Exceptional Medical Expenses Act)
CE (mark)	Conformité Européenne (European mark)
CG-Raad	Council for the Disabled and Chronically Ill (Chronisch zieken en Gehandicapten Raad Nederland)
CIZ	Centrum Indicatiestelling Zorg (the body that assesses people's care needs)
DRE	Direct Recording Electronic
EDP	Electronic Data Processing
EMI	electromagnetic interference
EMSEC	Emission Security
EU	European Union
FCC	Federal Communications Commission
GPRS	General Packet Radio Service
HSDPA	High-Speed Downlink Packet Access
ICF	International Classification of Functioning, Disability and Health
ISS	Integraal Stemsysteem (integrated voting system)
KOA	Kiezen op Afstand (remote electronic voting)
MoIKR, IKR	(Ministry/Minister of the) Interior and Kingdom Relations
MPRD	Municipal Personal Records Database
MRZ	Machine Readable Zone
NATO	North Atlantic Treaty Organization
NVVB	Nederlandse Vereniging voor Burgerzaken (the association of organizations concerned with municipal documentary services to citizens)
OCR	Optical Character Recognition
ODIHR	Office for Democratic Institutions and Human Rights
OSCE	Organisation for Security and Co-operation in Europe
OSCE	Organization for Security and Co-operation in Europe
RIS	Register Ingetrokken Stempassen (register of cancelled voting passes)
RNR	Register of Non-Residents
SDIP	SECAN Doctrine and Information Publication
SECAN	Security and Evaluation Agency NATO
TEMPEST	Telecommunications Electronics Materials Protected From Emanating Spurious Transmissions
UMTS	Universal Mobile Telecommunications System
VAPS	Voting at any polling station
VAPS(M)	Voting at any polling station within the voter's municipality
VAPS(N)	Voting at any polling station outside the voter's municipality (nationwide)
VNG	Vereniging van Nederlandse Gemeenten (Association of Netherlands Municipalities)
VVPAT	Voter Verifiable Paper Audit Trail
WHO	World Health Organization
WMO	Wet maatschappelijke ondersteuning (Social Support Act)

Appendices

1. Decree Establishing the Election Process Advisory Commission
2. Threat analysis of the current election process
3. Risk analysis of Remote Voting. Voters abroad 2004
4. Risk analysis of Remote Voting. Voters abroad 2007
5. The 112 recommendations of the Council of Europe (Appendix 11) and the current election process
6. The role of IT in the current election process
7. The new method of voting at polling stations
8. Potential tensions between roles in the election process: recommendations on the future allocation of Electoral Council responsibilities, Prof. M.J.W. van Twist & J.M. Schulz, 28 June 2007
9. Document of the Copenhagen Meeting of the Conference on the Human Dimension of the CSCE, 5 June - 29 July 1990
10. Code of good practice in electoral matters, European Commission for Democracy through Law, Venice 18-19 October 2002
11. Legal, Operational and Technical Standards for E-Voting, Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum
12. The Netherlands Parliamentary Elections 22 November 2006, OSCE/ODIHR Election Assessment Mission Report
13. List of organizations consulted
14. Reports of meetings:
 - 14.1 Stichting Burger@Overheid.nl (29 January 2007; 21 August 2007)
 - 14.2 Stichting Wijvertrouwenstemcomputersniet; 29 January 2007)
 - 14.3 Nederlandse Vereniging voor Burgerzaken (NVVB; 29 January 2007; 24 August 2007)
 - 14.4 Working visit to the Municipality of Amsterdam (7 March 2007)
 - 14.5 Council for the Disabled and Chronically Ill ((CG-Raad), Disability in the Community Task Force, Viziris (11 June 2007)
 - 14.6 Electoral Council (19 June 2007)
15. Letters:
 - 15.1 F.J.J.M. Andriessen (20 March 2007)
 - 15.2 Bureau voor verkiezingsuitslagen J.W. Groenendaal B.V. (14 March 2007)
 - 15.3 Council for the Disabled and Chronically Ill (CG-Raad; 20 February 2007)
 - 15.4 Van der Geest Spitstechniek (10 April 2007)
 - 15.5.1 Electoral Council (12 February 2007)
 - 15.5.2 Electoral Council (10 May 2007)
 - 15.6.1 Nedap Election Systems, N.V. Nederlandse Apparatenfabriek "Nedap" (12 April 2007)
 - 15.6.2 Nedap Election Systems, N.V. Nederlandse Apparatenfabriek "Nedap" (8 June 2007)
 - 15.7 Nederlands Meetinstituut (NMI B.V.; 1 March 2007)
 - 15.8 Nederlandse Vereniging voor Burgerzaken (NVVB; 5 February 2007)
 - 15.9 State Secretary for the Interior and Kingdom Relations (19 April 2007)
 - 15.10 C.B. de Sterke (5 April 2007)
 - 15.11.1 Stichting Burger@Overheid.nl (10 January 2007)
 - 15.11.2 Stichting Burger@Overheid.nl (12 February 2007)

- 15.12 Disability in the Community Task Force (2 August 2007)
- 16. Experience of a Voter Verifiable Paper Audit Trail (VVPAT)
- 17. Electronic counting. May 2007 electoral pilot schemes, The Electoral Commission, August 2007
- 18. Experience of optical vote scanning systems in the United States of America

Glossary of polling card terms

Voter registration card = single-station polling card

Voting pass = multi-station polling card

Voter's pass = single-station polling card (which may be made valid for one or more other stations on special application by the voter)

LETTER OF THE STATE SECRETARY FOR THE INTERIOR AND KINGDOM RELATIONS

To the Speaker of the House of Representatives of the States General

The Hague, 23 November 2007

Introduction

At the meeting of the Parliamentary Standing Committee and the Minister(s) on 12 October 2006⁶⁰ the House of Representatives asked for an independent commission to be set up to make recommendations on the future organization of the election process. The former Minister for Governmental Reform and Kingdom Relations agreed to the request and accordingly set up the Election Process Advisory Commission (hereinafter referred to as the Advisory Commission).

The Advisory Commission's remit was to examine the election process and make proposals to improve or change it in line with the principles of secret, free, reliable, practical and transparent elections that are equally accessible to everyone. The Advisory Commission, chaired by F. Korthals Altes, published its report, entitled 'Voting with confidence', on 27 September 2007. This letter is the Government's response to its conclusions and recommendations, indicating how the election process will be organized in future.

The Advisory Commission was not asked to consider the question of the right to stand for election; its report, and therefore this position document, is concerned solely with the organization of the election process, specifically:

- Determining eligibility to vote
- The preparations for the ballot
- The ballot
- The count
- Determining the results of the ballot
- Announcing the results

The Government's position document discusses the main arguments, conclusions and recommendations in the report that now require a guiding pronouncement.

The Government's view

Before discussing the Advisory Commission's recommendations specifically, the Government would like to indicate its position on a number of key points.

Free, secret and fair elections lie at the heart of the democratic system, and their importance is enshrined in the Dutch Constitution and international treaties. Voters (i.e.

⁶⁰ TK (proceedings of the House of Representatives) 2006-2007, 30 800 VII, No. 18.

persons registered as eligible to vote) have the right to cast their votes free from any influence and to keep the way they have voted to themselves. Participation in elections is a right that is not taken for granted in many parts of the world, hence it is up to everyone in Dutch society – including the various government bodies – to exercise it meaningfully.

Voting is not compulsory in the Netherlands, but it is vital to the democratic legitimacy of municipal and provincial councils, the House of Representatives and the European Parliament and their members that as many citizens as possible exercise their right to vote. It is essential, therefore, that there be as few obstacles to participation as possible. The Dutch electoral system lays down who is eligible to vote in what elections and limits each voter to one vote in each election. The election process must be organized in such a way as to ensure that these rules are complied with.

Lastly, the Government wants an election process where transparency, verifiability and fairness are paramount, as the great confidence the Dutch public have in the proper conduct of elections is not something that can be taken for granted but needs to be constantly reaffirmed.

The Government's position

Principles

As the view set out above indicates, the Government shares the Advisory Commission's opinion that the election process must be organized in such a way as to safeguard the following eight principles as defined by the Commission:

- **Transparency:** The structure and organization of the election process should be clear, so that everyone in principle can understand it. There must be no secrets in the election process: questions must be able to be answered and the answers must be verifiable.
- **Verifiability:** The election process should be objectively verifiable. The verification tools may differ, depending on the method of voting that is decided upon.
- **Fairness:** The election process should operate in a proper manner, and the results must not be capable of being influenced other than by the casting of lawful votes.
- **Eligibility to vote:** Only persons eligible to vote must be allowed to take part in the election.
- **Free suffrage:** Every elector must be able to choose how to vote in complete freedom, free from influence.
- **Secret suffrage:** It must be impossible to connect the identity of a person casting a vote to the vote cast. The process should be organized in such a way that voters have no documentary evidence of how they have voted.
- **Equal suffrage:** Each voter, given the Dutch election system, must be allowed to cast only one vote in each election, which is counted precisely once.
- **Accessibility:** Voters should be enabled as far as possible to participate directly in the election process. If this is impossible, there must be a way of taking part indirectly, i.e. by proxy.

In Chapter 2 of its report the Advisory Commission points out that in practice it is a question of striking a balance between these principles. This exposes certain dilemmas and requires political choices to be made. The Commission rightly notes the unique nature of elections and the complexity that results from this.

Clear frameworks are needed so that it is clear to everyone what requirements the election process must meet. On the other hand, the frameworks must not be an obstacle to changes being made if they are found necessary. Change may be needed based on new social ideas and/or technological advances or as a result of practical experience. The Advisory Commission rightly concludes, therefore, that there must be regular systematic reviews of the process.

Duties and responsibilities

The Government intends to formalize the duties and responsibilities for the election process in legislation, so as to make it clear to everyone who is responsible for what. This includes the role of the Minister of the Interior and Kingdom Relations.⁶¹ The legislation will include the stipulation that certain duties in the election process must be exercised independently, as suggested by the Electoral Council in its response to the Advisory Commission's report.

Unlike in the past, and in accordance with the recommendation of the Voting Machines Decision-Making Commission, the Interior Minister will be made responsible for control over the election process and certain specific duties. One of these will be laying down the requirements for equipment used for voting at polling stations and elsewhere and for the calculation of results. The Interior Minister will also be responsible for organizing voting other than at polling stations for special groups of voters, including those permitted to vote from abroad.

A number of measures are needed to improve transparency and verifiability. The first of these is public scrutiny of certain parts of the election process. The following measures are envisaged (the list is not exhaustive):

- The requirements for aids (including software) and devices used in the organization of elections, ballots, counts and the determination of results should be public.
- All polling stations should use the same aids and devices, which comply with the requirements laid down and have been procured or designated by the Interior Minister.
- There will be frameworks for polling station committee procedures and for the information that must be recorded in the official reports to be drawn up by polling station committees.
- The official reports will be public and published on the Internet. As a minimum they will include the counts and any complaints lodged by persons present at the polling station.

⁶¹ Under the current distribution of portfolios the State Secretary for the Interior and Kingdom Relations.

- After each election the Ministry of the Interior and Kingdom Relations (MoIKR) will commission an external independent inquiry⁶² into the conduct of the election, from which lessons may be learned for the future. This should be seen as part of the ongoing scrutiny and review of the election process.

Furthermore, the new method of voting at polling stations proposed by the Advisory Commission has a high degree of transparency and verifiability, as anyone can check that the devices used for voting are working correctly.

Given the ‘public scrutiny’ and ‘control’ approach to be adopted henceforth by the Interior Minister, the Government takes the view that it is not necessary to carry out an audit after each election. It needs to be remembered that elections only take place occasionally (once a year on average) and that a whole host of people are involved, including many thousands of volunteers. It is impossible to organize the process so tightly that it is clear precisely how to act in any situation. As a tool, audits – the whole idea of which is to check, item by item, whether the process has been conducted as laid down in the appropriate documentation (regulations, administrative procedures, etc.) – are not ideally suited to a unique process such as the election process.

As regards the separation between government and the private sector, the Government wholly shares the Advisory Commission’s view. Organizing elections and conducting them are the responsibility of government. There is only a secondary role for the private sector here, as a supplier of the equipment the government wishes to use in elections. The MoIKR needs to ensure that it has sufficient expertise to weigh up the pros and cons (also in technical matters) and make choices, in full awareness of possible threats and risks. These deliberations and choices must be the result of the regular systematic review of the election process.

Voting in the future

Voting at polling stations

The Government wants a method of voting that guarantees the freedom and secrecy of the ballot. At present this can only be achieved with voting at polling stations, where a polling station committee supervises the conduct of the ballot, and the ballot and the count are public.

Having weighed up the methods of voting currently used in the Netherlands, the Advisory Commission took the view that voting using paper ballots at polling stations was the preferred option on the grounds of transparency and verifiability. This method, however, gives rise to a problem with the count, as manual counting is error-prone and takes a long time. It is also not suitable for voting at polling stations outside the voter's municipality.

⁶² This inquiry should not be confused with the survey of voters being conducted for the MoIKR by a group of universities, which is designed to poll voters’ opinions on various matters.

The proposal, then, is to introduce a method of voting where voters indicate their choice using an electronic device (a ballot printer). This prints the voter's choice on paper, and the voter places the printout in the ballot box himself. The votes in the ballot box can be counted electronically (by a vote counter) and by hand. The Advisory Commission recommends this method of voting because of its conceptual clarity and the unambiguous counts it is able to produce.

The Government agrees that paper ballots on which voters can check for themselves whether their choice is indicated correctly are preferable to a method of voting where they have to take it on trust that their choice has been recorded correctly. In addition, having paper ballots provides a transparent way of recounting the votes if necessary. The likelihood of errors when counting ballot papers manually and the time this takes should not be disregarded, however: the Government therefore wishes to go ahead and introduce the method of voting at polling stations proposed by the Advisory Commission.

This method, however, involves some practical aspects that need further consideration. One of these is 'compromising radiation' that might be intercepted. Like the current voting machines, ballot printers are vulnerable in this respect. It remains to be seen whether this vulnerability could be eliminated by laying down requirements for the design of ballot printers. The vote counters that could be used to count the paper ballots are also vulnerable devices: they will need to be error-free and fault-free in operation if they are to obviate the need to carry out manual counts at many if not all polling stations.

Some time is needed to check whether the proposed method is technically feasible. Further research on this point will take a few months. In tandem with this work, an external expert group chaired by Prof. B. Jacobs⁶³ will advise me on the Statement of Requirements for the ballot printer and the vote counter. The results of both these studies must in any event be available by 1 May 2008, so that the decision on the new method of voting can be finalized.

Voting at any polling station (VAPS) within the voter's municipality

Experiments with voting at any polling station (VAPS) within the voter's municipality have taken place since 2004. As the experience has been overwhelmingly positive, the previous Government already decided to make VAPS possible in all municipalities.⁶⁴ The Advisory Commission confirmed that we should go ahead with this. The Government intends to adopt the Commission's solutions to the problems found with the VAPS experiments.

At present the election system does not include any requirement for voters to identify themselves when casting their votes at polling stations. As a result it is not certain that the person voting is actually the elector in question. This needs to change. Compulsory identification will therefore be introduced, as recommended by the Advisory Commission

⁶³ Prof. B.P.F. Jacobs (Professor of Computer Security at Radboud University, Nijmegen and Eindhoven University of Technology) was a member of the Election Process Advisory Commission.

⁶⁴ TK 2005-2006, 30569, p. 5.

and the Electoral Council. The Association of Netherlands Municipalities, in its response to the Commission's report, also underlined the importance of introducing compulsory identification.

The evaluations of the VAPS experiments drew attention to the possibility of counterfeiting voting passes. The type of voting pass used in the experiments so far has only marginal protection against forgery, so the proposal to provide it with one or more authenticity features could make for a substantial improvement here. This proposal is in line with provisions already included in the Voting at Any Polling Station bill.⁶⁵

Voting at any polling station outside the voter's municipality

The MoIKR's Remote Voting Project was based on the intention to make it possible for voters to vote at any polling station outside their municipality as well. Voters would be able to cast their votes on polling day anywhere in the Netherlands. The Advisory Commission noted that the proposed method of voting at polling stations would be suitable for this and indicated what equipment would be needed at polling stations and elsewhere to implement this. The Commission recommended, however, that VAPS outside the voter's municipality should not be introduced until the authorities responsible for organizing elections and the public are accustomed to the new system of voting at polling stations, as introducing all the changes at once would be too risky.

The Government agrees with this view. Whether we go ahead with VAPS outside the voter's municipality will depend on (a) whether the new method of voting at polling stations is feasible and (b) whether there is a real demand for this extension.

Voting by proxy

The Netherlands has a system of proxy voting which enables voters to authorize someone else to vote on their behalf. In its report the Advisory Commission mentions the reservations that could be made regarding this method of voting, and OSCE/ODIHR observers have also recently drawn attention to this point again.

There is still a demand for proxy voting, however: data from various municipalities shows that 15% of votes on average are cast by proxy. There are good reasons, though, for building in special safeguards to prevent abuse of the proxy voting facility.

The Government adopts the proposal that a copy of the identity document of the voter issuing the authorization be produced along with the proxy document. This will provide an additional deterrent to relatively simple types of misuse of voting passes left lying around. The Advisory Commission rightly points to the risks of family voting involved in the proxy voting facility (as also demonstrated recently in the report by the Municipality of Amsterdam's ombudsman). It is still very necessary, therefore, to educate voters about the importance and the strictly personal nature of the individual's right to vote. The

⁶⁵ TK 2005-2006, 30569, p. 5.

Government adopts the suggestion of including this in assimilation courses, so that these values are instilled in immigrants.

Voting for voters with impairments

At present, voters with impairments are faced with too many barriers to participating in elections. They are often dependent on proxy voting, and this needs to change. They too should be given the opportunity to vote for themselves wherever possible. The Government intends to lay down in the new legislation an obligation on municipalities to designate polling stations, distributed throughout the municipality, that provide access for voters with impairments. Municipalities must actively inform voters about the locations of these polling stations.

On top of this, when the new method of voting at polling stations is introduced, the Government intends to equip ballot printers with audiovisual aids to enable visually impaired people to use them to make their choice. These aids will also be useful to voters who cannot read.

The Government acknowledges that even with this package of measures there will still be voters who are not able to attend a polling station. They will still have the possibility of voting by proxy. The question is whether another new method of voting should be introduced for this particular group.

The Advisory Commission did indeed recommend this, suggesting that telephone voting be introduced. To define the group eligible to use this facility it proposed using the ICF classification ‘totally dependent’ under ‘walking and moving’ and ‘moving around using transportation’. The Government has reservations about the feasibility of this proposal, as it would result in a substantial group of voters (about 0.5% of the electorate⁶⁶) having to register for each election. The Electoral Council and the Association of Netherlands Municipalities, in its response to the Commission’s report, have also cast doubts on the feasibility of the proposal.

As the ICF classification is personal and not permanent, voters wishing to be registered for the facility would have to prove before each election that the ICF classification applied to them. If an application for registration is rejected, an appeal could be lodged against the decision with the Council of State.⁶⁷ It goes without saying that this would involve a substantial administrative burden, not only for the person wishing to use the facility but also for the authorities. Further consultations will take place on this with the Council for the Disabled and Chronically Ill (CG-Raad), the Disability in the Community Task Force and Viziris.

The proposal to permit voters with a mental condition to be offered assistance by the polling station committee at polling stations will be included in the proposed new

⁶⁶ This information is from the Council for the Disabled and Chronically Ill (CG-Raad), the Disability in the Community Task Force and Viziris.

⁶⁷ Similarly with voters eligible to vote from abroad (Elections Act, Section J9).

legislation. The method of voting at polling stations proposed by the Advisory Commission would seem to offer good opportunities for implementing this. As no votes are stored in the ballot printer, the polling station committee could demonstrate its use to any voters at the polling station so requiring.

Mobile polling stations

The Elections Act lays down that persons eligible to vote who are lawfully deprived of their liberty on polling day shall exercise their right to vote by voting by proxy. Having weighed up the pros and cons, the Advisory Commission proposed that consideration be given to whether special mobile polling stations could be opened for part of a day in prisons. Each station would need to have a ballot printer and a ballot box which could be used by both inmates and staff. The count and the determination of the result would have to take place later, at a public place.

The Government has some reservations about this proposal. Many prison inmates are not registered as electors in the municipality where the prison is located, and mobile polling stations do not provide a solution to this problem, as pointed out by the Electoral Council in its response to the Advisory Commission's report.

Also, setting up and using a mobile polling station in a penal institution would have a major effect on the orderly conduct of the institution. It needs to be remembered that penal institutions differ substantially in terms of both regime and organization, hence uniform rules on the organization of such mobile polling stations would not be feasible. In view of this the Government considers that priority must be given to the undisturbed execution of sentences or orders, the maintenance of order and security, and uniform rules on the exercise of the right to vote by prisoners. The possibility of voting by proxy will be retained, as stated above.

Voting from abroad

Voters eligible to vote from abroad have had the right to vote by post since 1983. The MoIKR experimented with Internet voting for this group in 2004 and 2006. The Advisory Commission proposed that Internet voting be made available to this group on a regular basis, and that postal voting also be permitted in the case of voters who are unwilling or unable to vote via the Internet.

The Government is in favour of this proposal in principle, albeit the voting service for Internet voting will have to safeguard the principles of transparency, verifiability, fairness, equal suffrage and eligibility to vote. There are also some reservations about the cost of Internet voting: on this point see the evaluations⁶⁸ of the experiments conducted in 2004 and 2006.

⁶⁸ TK 2004-2005, 29800 VII No. 1 and TK 2006-2007, 30800 VII No. 62 respectively.

The cost of the experiment in 2006 was over €90 per registered Internet voter. The cost of postal voting is about €1669 per elector (excluding the postage charges that have to be borne by the elector). The difference between the cost of Internet voting and postal voting is thus substantial, and it is therefore reasonable to ask whether the cost outweighs the benefit, i.e. the extent to which access is improved.

Access for this group of voters is substantially affected by the registration procedure before each election. It was clear from the evaluations of the experiments conducted by the MoIKR in 2004 and 2006 that the registration procedure causes irritation. The Government is willing to revise the procedure, taking the Advisory Commission's proposals into account.

Legislation and regulations on the election process

As already indicated in various parts of this Government position document, new legislation will be introduced to regulate the organization of the election process. Whereas under the Elections Act the principles, in particular of verifiability and transparency, are implemented in detailed regulations, the new legislation will provide a system that lays down the essential principles and rights at statutory level, with the power to lay down more detailed rules at a lower level. Once the frameworks within which the lower-level regulations are to be issued are laid down by law, it will no longer be necessary to enshrine all the procedures in detail in statute law, as is currently the case with the Elections Act.

The aim is to have legislation that is technically independent of the technology used and provides the possibility of responding to new or changing ideas and preferences among the public, while explicitly laying down the framework within which these changes are to take place. The bill itself, therefore, will not stipulate that a particular technology must be used but will outline the principles that any method of voting – using pencil and paper or otherwise – must comply with. A flexible formulation of the statute law, with the power to lay down specific rules by Order in Council, or Ministerial Regulation if necessary, will make it easier to maintain and where necessary overhaul the election process. It is vital here, as the Advisory Commission indeed points out, that the principles always be weighed up in full public view and that political choices be made based on the results of this.

Funding

In Chapter 11 of its report the Advisory Commission gave some indications of the possible cost of the proposed method of voting at polling stations. These were not based on quotations or consultations with suppliers. A number of cost items, including the possible cost of measures to combat compromising radiation, were not estimated, nor were the management and administration costs.

⁶⁹ This amount is based on an audit by Deloitte Accountants, which was carried out at the end of 2005.

The Government can only regard this estimate as a rough indication of cost. A more precise estimation of the budgetary consequences will be made in the period ahead. The Government will discuss these consequences in its subsequent position document in the spring, including all the costs of the election process incurred by the various tiers of government and who should bear which costs. If the Government decides to introduce the new method of voting it will also consider when the desired standardization can be implemented.

A.T. B. Bijleveld-Schouten

STATE SECRETARY FOR THE INTERIOR AND KINGDOM RELATIONS

TEMPEST

specifications and test methods for e-voting machines

Contents

1. Introduction.....	93
1.1 Background.....	93
1.2 Purpose.....	93
1.3 Scope and applicability	94
2. TEMPEST specifications.....	95
3. Test methods	99
3.1 Test setup	99
3.2 Test procedure.....	100
3.3 Frequency of testing.....	103
4. Guidelines for manufacturers and other conditions	105
4.1 Guidelines for manufacturers.....	105
4.2 Software guidelines.....	106
4.3 Guidelines for the environment	106
5. Appendices.....	108
Appendix A.....	108
Appendix B	110
Appendix C	113

This document was developed by GBS mbH (Gesellschaft für Beratung und Schulung mbH – Company for economic consultancy and training).

Authors:

Dr. Markus Kuhn
Gerhard Friedrichs
Ahmet Aksoy
Enrico Koch
Lars Friedrichs

1. Introduction

This document formulates requirements for e-voting systems from a TEMPEST perspective. The document also describes corresponding test methods and gives guidelines to manufacturers of e-voting systems.

1.1 Background

All IT-devices, also the IT-devices in an e-voting machine, emanate electromagnetic rays containing information; in technical terminology these are referred to as compromising radiation or compromising emanation. This emanation contains data that is presently being processed. Neither firewall nor antivirus software prevents a data spy from receiving compromising emanations and from reading out sensitive data in this way, which is referred to as a TEMPEST attack. Where information is regarded as confidential, this type of eavesdropping should be prevented. As national law and international treaties demand that elections be held by secret ballot, the individual votes in an election should be regarded as confidential. It is therefore desirable that electronic voting machines be protected against eavesdropping by means of capturing emitted radiation.

Military standards exist which specify requirements in the field of TEMPEST. There are two reasons why a new set of requirements has been developed. Firstly, the existing military regulations are secret and therefore not usable for the application area. More specifically, the requirements to be defined here will be made publicly available, so that interested people are able to relate to this matter. Secondly, the military standards were developed with a specific point of view towards PC and other IT equipment. The military standards make some assumptions which are not necessarily fulfilled in the e-voting situation. Consequently, the military standards are not immediately applicable to e-voting systems.

1.2 Purpose

This document defines limits for the level of radiation by electronic voting machines, as well as the corresponding test procedures for determining whether a machine satisfies the requirements. In order to define these limits, assumptions

on the level of capability of the attacker are made. More specifically, assumptions are made regarding the antenna equipment a possible attacker has available and the distance from the e-voting machine at which the equipment can be placed without being detected.

Further, guidelines for voting machines are described that are helpful to meet the requirements. Additionally, guidelines for polling stations and voting software will be formulated.

These requirements with all details will be publicly available.

1.3 Scope and applicability

These requirements are applicable to all electrical, electronic, electromechanical and electro-optical equipment which is used to select and/or cast a vote in an election process, either in an analogue or digital form. These requirements are not applicable to the process of counting votes.

This document is intended to be used by local and national election officials, manufacturers, service providers and accreditation organisations. Voting systems can be tested against these requirements. After servicing or modifying a voting system, the voting system needs to be tested again.

This document is not intended for quality test of individual components of which specific equipment is composed and also not for the used voting software.

2. TEMPEST specifications

An e-voting machine is regarded as “TEMPEST – proof” if the compromising emanation from it cannot be caught by any interested people under the following assumptions:

- The eavesdropper is not able to place an antenna with an aperture larger than 1 square metre closer to the eavesdropping target than 5 metres (or four times that aperture area at twice that distance or $\frac{1}{4}$ of the aperture at half the distance etc. This is only a clue to show the problems of an eavesdropper. It is not possible to define an exact mathematical correlation between distance and aperture of an antenna. The aperture of the antenna is also dependent on the range of the antenna used by an eavesdropper.)
- The eavesdropper performs his attack in a normal environment and not inside any especially shielded room, and is therefore exposed to the minimum level of atmospheric background noise that can normally be expected at a quiet receiver site according to the reference data given in ITU-R Recommendation P.372.

The TEMPEST specifications have to be met by all electronic machines, tested before they come in use. To fulfill TEMPEST specifications it is necessary to meet the requirements described below and the European standards for electromagnetic compatibility (EMC, here defined by the EMV Standard 89/336/EEG and EMV Standard 2004/108/EG)⁷⁰. The most restrictive requirement will prevail in case the EMC standards and the requirements in this document allow different emanation levels.

This section specifies five emanations lines. These indicate upper limits for the strength of radiated electromagnetic signals that are allowed to be emitted by e-voting systems. The emanations lines (also referred to as e-voting lines) are specified in figures 1 and 2. The requirements concern emanations in the range of 10 KHz up to 10 GHz.

Figures 1 and 2 should be read as follows. Upper limits are defined on the field strength of emitted radiation in a certain bandwidth B around a centre frequency f. Figure 1 shows the bandwidth B which is considered for each centre frequency. Figure 2 then shows the maximum field strength that is allowed in frequency band $f \pm \frac{1}{2} B$.

The so defined lines are an upper limit on the electromagnetic field strength of an e-voting machine. Equipment that has been found to not exceed the maximum

⁷⁰ An European manufacturer has to affirm that a new machine fulfils the requirements of this regulation

field-strength limits is believed to be sufficiently protected against the risk of electromagnetic eavesdropping, under the assumptions stated above.

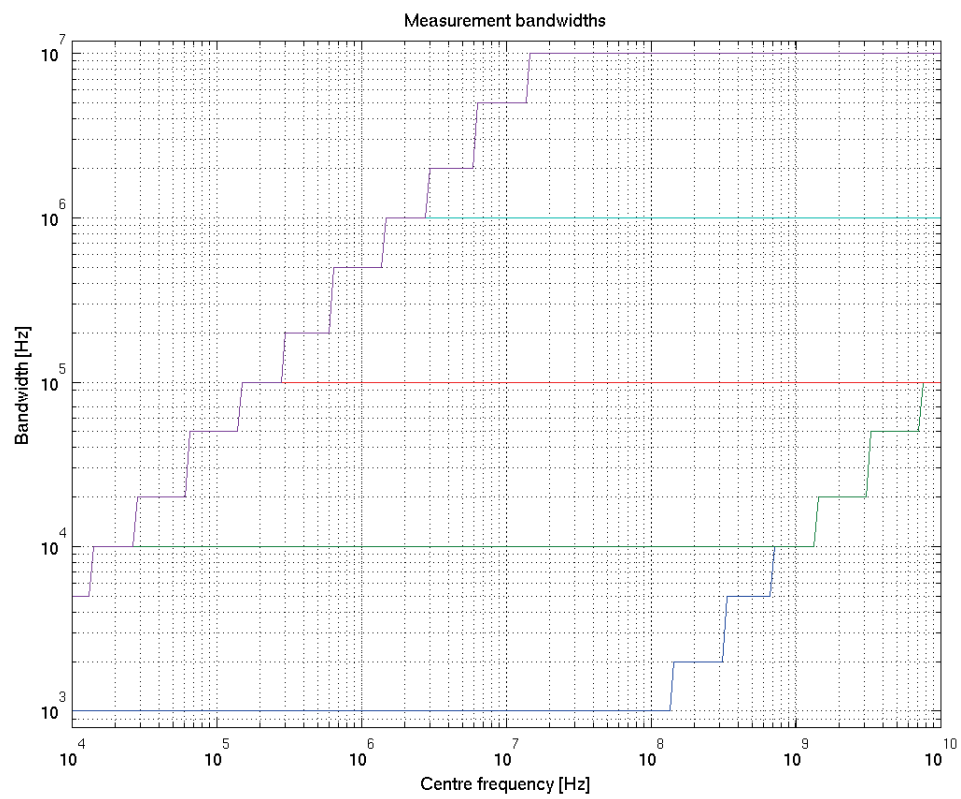


Figure 1

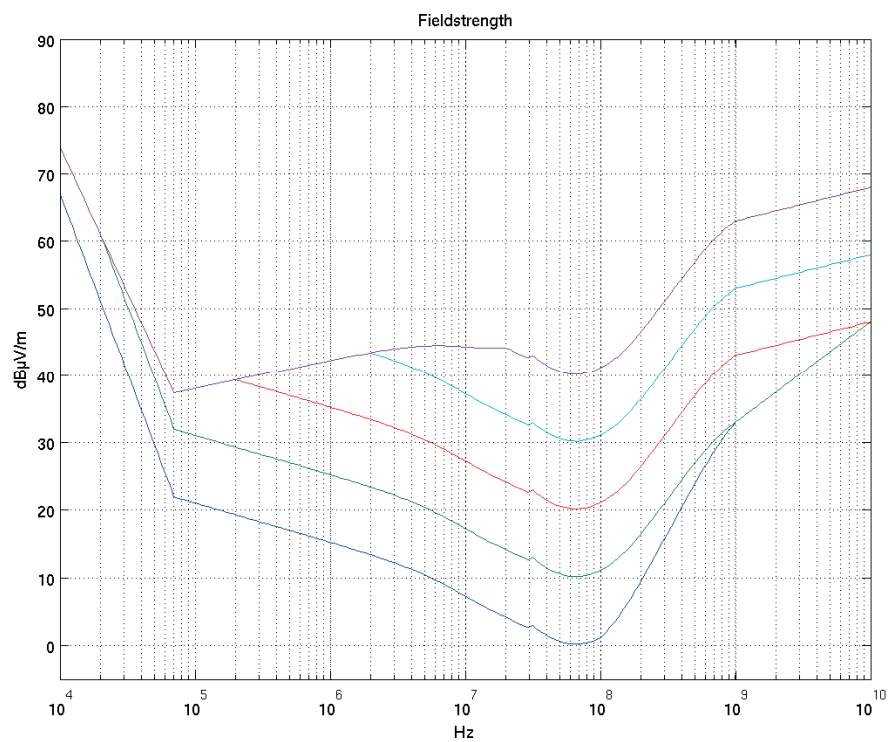


Figure 2

3. Test methods

The test methods and procedures to demonstrate conformity with the TEMPEST specifications in this document are generically applicable regardless of the type of voting machine or the implemented TEMPEST countermeasures by the manufacturer.

After the TEMPEST measurement it is advisable to seal the e-voting system so that it is impossible to open the machine in an unobservable way. An unbroken seal in combination with a certificate showing that the e-voting system is approved by an accredited laboratory provides the guarantee of the integrity of the e-voting machine from the viewpoint of TEMPEST.

This chapter will describe the procedures and test equipment setup required to perform the tests.

3.1 Test setup

Before the test, the e-voting system will be loaded with test software. The test software does not simulate a voting process but causes a situation where the e-voting machine emits as much radiation as possible. Thus the e-voting machine equipped with e-voting software will not be able to cause stronger emanations than the tested e-voting machine i.e. the voting machine loaded with test software.

The aim is to measure if the machine equipped with test software does not exceed the maximum field-strength limits indicated by the e-voting lines. If the measured radiations are below the e-voting lines then it is concluded that the e-voting machine is sufficiently protected against the risk of electromagnetic eavesdropping. The test software is not only necessary for the accreditation measurement new but also for the following compliance tests (see section 3.2).

The test setup consists of antennas for different frequencies, a measurement receiver / spectrum analyzer and a PC with printer.

The measurement receiver / spectrum analyzer should have the following specifications:

- frequency range from 10 KHz to 10 GHz; in this range are usually found the activities, to obey under the aspects of TEMPEST. Therefore it is specially necessary to test this range in the accreditation measurement.

- Intermediate Frequency bandwidths (RBW) from 10 Hz to 500 MHz in steps of 1/2/5; these RBW are converted to measurement curves in figure 1 and 2
- noise figure less than 3 dB; a noise figure higher than 3 dB may be possible. The experience in TEMPEST periphery shows that a low noise is more helpful; therefore 3 dB is recommended for TEMPEST measurements
- frequency resolution 0,1 Hz. The experience in TEMPEST periphery leads to this frequency resolution; more may be possible, but less helpful

The peak-hold detection mode is to be used, and the sweep time adjusted to set the required dwell time. The dwell time on each frequency is at least 50 ms, or twice as long as the outer loop interval of the test software, whichever is longer.

The antennas must be able to measure in a frequency range from 10 kHz up to 10 GHz. The measurement antennas are connected to the measurement receiver / spectrum analyzer and this machine is connected to the PC / printer.

The measurement receiver / spectrum analyzer will be controlled while running the test by a connected PC, also responsible for keeping the records.

Measurements need to be performed in a cabinet, shielded up to 18 GHz. This is usual for TEMPEST measurement cabinets. An outdoor measurement is not fit for purpose.

3.2 Test procedure

The measurement procedure consists of two phases namely an accreditation measurement and a compliance measurement.

The accreditation measurement takes place for each type of e-voting system. If changes to an e-voting machine are made that is regarded as a new type and a new accreditation measurement is needed.

These changes include:

- new type of the main board or revision of the main board
- different display panel size, different type of the display, revision of the display, other manufacturer of the display.
- different housing design
- different printer model or revision of the printer
- any other electrical or shielding component change

An accreditation measurement incorporates a full test: it is measured if the radiated emanations are below the five emanation lines specified by figures 1 and 2.

Subsequently, for each e-voting machine of the same type only a compliance measurement is performed. The compliance measurement will take significantly less time than the accreditation measurement. Below more details are given on the two measurement processes.

A. Accreditation measurement

- each measurement process will be done twice, once for the vertical and once for the horizontal polarisation of the antenna
- emanations from the e-voting machine to be tested will be measured from two sides: emanations will be measured when the antenna is standing in front of the machine and when the antenna is standing behind the machine.
- the following distances in the measurement cabinet should be taken into account while performing the measurements:

the distance between the equipment under test and the walls is not less than 1m

the distance between the antenna and the walls is not less than 1 m

the distance between the closest side of the equipment under test and the calibration point of the antenna = 1 m

- the e-voting machine has to boot up the test software and run the test mode
- the test run is to be logged by a PC outside the measurement cabinet
- the result of the measurement is to be documented by a hardcopy which shows the defined voting line as nominal value and the result of the measurement as a graph.
- this measurement requires about four hours

B. Compliance measurement

In the compliance measurement the same procedure is to be followed as in the accreditation measurement with the following exceptions:

- it is only tested if the radiated emanations are below the line for the broadband emanations (the red line in figures 1 and 2) and below two lines for the narrowband emanations (the green and blue lines in the figures 1 and 2);
- the measurement with the vertical polarisation of the antenna is not executed;
- the measurement where the antenna is located behind the e-voting machine is not executed.
- this measurement requires about 25 minutes

3.3 Frequency of testing

The compliance test of E-Voting machines is necessary for each machine; this is based on the following reasons:

- identical components of e-voting machines of the same type may show different behaviour under TEMPEST aspects. Thus, machines of the same type may show different behaviour under TEMPEST aspects, even if the construction and functionality is exactly the same. Some machines of the type may meet the TEMPEST regulations, whereas others do not.

- if the guidelines for the polling stations formulated in section 4.3 cannot be guaranteed, the failure of a single machine to meet the requirements may endanger the secrecy of the ballot. Especially if no guarantees can be given on polling stations, it is therefore essential to test each machine. Only a statistical measurement of machines does not make not sure that the protection is complete

It is necessary to retest all machines within a period of two years with a compliance measurement to be sure that the machine is still compliant with the TEMPEST regulations.

A TEMPEST measurement shows just in the moment of the measurement that the tested machine fulfils the regulations of the defined TEMPEST lines. These characteristics can be changed by several activities:

- a component of the machine, like an electrical capacitor, may be subject to small changes over time. These may not lead not to a malfunction of the whole machine, but may still cause a failure with respect to the TEMPEST regulations.

- it might be possible to come to a failure with respect to the TEMPEST regulations due to transport or other handling of the machine. Each TEMPEST laboratory will exclude liability in this respect.

4. Guidelines for manufacturers and other conditions

The following chapter gives advices for manufacturers in order to help them to build e-voting systems that are in accordance with the TEMPEST standard. Advice for the situation in and around the polling station is given as well.

4.1 Guidelines for manufacturers

These guidelines specify points of attention when designing e-voting hardware in order to prevent compromising emanations. Implementing these guidelines, however, does not guarantee compliance with the TEMPEST requirements specified in this document. In order to load test software on the e-voting machine for the TEMPEST testing, the machine needs to be equipped with a DVD or other 'read only' device.

- The e-voting machine is to be built out of conductible metal, only the touch screen, the data links, the power lines and the opening to the removal box for the ballot paper are necessary apertures
- The printer should be integrated into the e-voting machine
- From the viewpoint of TEMPEST special technical components and assemblies should be chosen for the printer, touch screen and headphones of the e-voting machine.
- The polling station authority is not allowed to open the e-voting machine except the printer to refill paper, only the sector for voting activities is to be sealed.
- The paper size should not be bigger than A6.
- Apertures in e-voting machines should be avoided as far as possible. In case there are apertures these should be rounded. It is advised to protect apertures like the removal box for the ballot paper with a flap.
- Power lines are to be shielded. Communication between the e-voting machine and the poll workers panel should be done via fiber optic cables or via a shielded cable.

- Headphones, connected with the e-voting machine, are possible under consideration of the following:
 - * the connector of the headphone is formed as a screw, not pluggable
 - * the cable is shielded
 - * the earphones themselves are shielded
- USB connections are to be shielded

4.2 Software guidelines

These guidelines specify points of attention for designing the software to be used in the voting process. Although these measures will not improve test performance, they may significantly reduce the risk of advanced TEMPEST attacks. As operating system a Linux version with a special minimized design should be considered: Linux allows superfluous operating system functionality to be left out.

- Software is to be programmed which (slightly) changes the colours displayed on the screen (not noticeable to the voter). This can be done by creating a single frame of “white noise” in each colour’s least significant 5 bits.
- Software is to be programmed leading to an “anti aliasing” system. The software causes small displacements or rotations of the buttons displayed on the screen which can be pushed by a voter. The difference in locations of the buttons on the screen are not noticeable to the voter.
- Definition of rustling routines, which (slightly) change the position or font size of characters displayed on the screen (not noticeable to the voter).

4.3 Guidelines for the environment

This section will describe additional guidelines for the environment of the e-voting devices, i.e. guidelines for a polling station.

- The e-voting machine is to be placed best at the opposite side from the windows.

- No further technical equipment in the polling room should be used (also mobile telephones should be switched off)
- A policy for a secure check of the sealed machine in case of a necessary change of an e-voting machine is to be defined

5. Appendices

Appendix A

Design rationale

While performing compromising-emanations measurements, particular consideration has to be given to the bandwidth. If the measurement bandwidth is too large, then a weak narrowband signal that an eavesdropper could detect with a suitably chosen narrow receiver IF bandwidth cannot be distinguished from measurement noise during the compliance test. If the measurement bandwidth is too small, then a broadband impulse signal that an attacker could detect with a suitably chosen wide bandwidth cannot be distinguished during the compliance test either. Since an eavesdropper may find useful signals over a wide range of bandwidths that typically spans 1 kHz to several tens of MHz, there is no single measurement bandwidth that could adequately detect both narrowband and wideband signals.

Therefore, several sweeps with different threshold curves and measurement bandwidths have to be performed. The choice of 1 kHz as the lowest bandwidth covers the types of signals that an eavesdropper using an AM audio receiver may be able to receive. The choice of 10 MHz as the highest bandwidth covers in particular video signals. In between these, an eavesdropper looking for a signal of a bit or symbol rate f will usually get the best results with measurement bandwidths in the range $f/2$ to $5f$. A set of sweeps in which successive bandwidths differ by a factor of 10 represents a good compromise between covering all bandwidths that an attacker might choose and permitting the compliance measurement to complete in reasonable time.

Each sweep begins at 10 kHz and increases the bandwidth (typically in a 1-2-5-10 sequence) such that the bandwidth is never larger than half the centre frequency or smaller than one ten-thousandth of it. The first limit avoids combinations of tuning frequency and bandwidth in which the noise performance of some spectrum analyzers might be decreased, the second limit reduces the scanning time. Where two sweeps overlap in both frequency and bandwidth, the measurement does not have to be repeated, because the corresponding threshold curves overlap as well.

The threshold curves were determined as follows

- We first calculate the minimum atmospheric or galactic noise values that can be expected at a quiet receiver site according to ITU-R Recommendation P.372-7 (continuous line in Figures 2 and 3), or an antenna noise temperature of 290 K, whichever is larger (to take into account that an eavesdropping target will usually have a room-temperature background).

- We then compensate for the fact that the measurement antenna is at 1 m distance, whereas the eavesdropper's antenna is at least 5 m away.
- We then compensate for the fact that the eavesdropper may be using not only a simple dipole, but also a Yagi-Uda, horn or parabolic antenna, each with a maximum aperture of 1 square metre (at 5 m distance).
- We also take into consideration the sensitivity limit of available active antenna kits of the type that is usually used for compromising-emanations measurements.
- We also allow for receiver noise.
- Taking all these factors into consideration, we set the threshold limits such that the eavesdropper cannot expect to achieve a better than 20 dB signal-to-noise ratio, where noise is measured with a root-mean-square detector, while the signal is measured with a peak detector.

Magnetic measurements are not necessary, because the distance between the e-voting machine and an eavesdropper is such that the magnetic field strength versus the electromagnetic field strength is negligible. Magnetic emanations are only effective in the near field, which means not more than five meters.

Appendix B

MATLAB code for generating the threshold curves

```
% Derivation of compromising-emanations e-field limit curves

% sample frequencies
curves = 1:2;
freqs = logspace(4, 10, 200);
[f, curve] = meshgrid(freqs, curves); % [Hz]

d0 = 1; % measurement distance [m]
logfreqs = log10(freqs);
curves = 1:5;
[f, curve] = meshgrid(freqs, curves); % [Hz]
bw = max(f/1e5, [ min(1e3, freqs/2) ; ...
                  min(1e4, freqs/2) ; ...
                  min(1e5, freqs/2) ; ...
                  min(1e6, freqs/2) ; ...
                  min(1e7, freqs/2) ]);
bwr = roundl25(bw, [1 2 5 10]);

% thermal noise at 290 K [dBµV/m] (lambda/2 dipole)
thermalnoise = 20 * log10(f/1e6) + 10 * log10(bw) - 96.8;

% SNR loss of eavesdropper compared to measurement antenna
d = 5; % distance of eavesdropping antenna [m]
pathgain = 20*log10(fieldstrength(d,f)./fieldstrength(d0,f));
receivernoise = (log10(f)-7)*5; % ITT Radio Engineers Handbook
sensitivity = sensitivity_am524(f, bw) + 20; % 20 dB above best R&S antenna kit

figure(1);
semilogx(freqs, ...
          dbpwradd(itunoise(f, bw, 1) - pathgain ...
                  - antennagain(f, bw, 1), ...
                  receivernoise + sensitivity));
title('Fieldstrength');
ylim([-5 90]);
xlabel('Hz');
ylabel('dBµV/m');
grid on;
saveas(gcf, 'limitcurves.png');
saveas(gcf, 'limitcurves.eps');

figure(2);
loglog(freqs, bwr);
title('Measurement bandwidths');
ylim([0.8e3 1.2e7]);
xlabel('Centre frequency [Hz]');
ylabel('Bandwidth [Hz]');
grid on;
saveas(gcf, 'limitcurvesbw.png');
saveas(gcf, 'limitcurvesbw.eps');

% add up decibel power levels
function s = dbpwradd(a,b)
s = 10*log10(sum(10.^(cat(3,a, b)./10),3));
```

```

% output normalized field-strength value (covering both far field
% and lower alternative near field) of frequency f [Hz] at distance
% r [m] from an emitting short dipole or small loop antenna
function e=fieldstrength(r,f)
lambda = 3e8 ./ f; % wavelength [m]
e = abs(1./(r.*lambda) .* (1 + 1./(j*(2*pi*r./lambda)) +
0./(j*(2*pi*r./lambda)).^2));

% Routine for estimating the gain of practical antennas or arrays
% with centre frequency f [Hz], bandwidth b [Hz], maximum dimension l [m]
function gain=antennagain(f,bw,l)

% auxiliary variables
rb = bw ./ f; % relative bandwidth [1]
lambda = 3e8 ./ f; % wavelength [m]

% collect achievable gains as a factor (i.e., not dB)
% (along gains along dimension 3, while dimension 1 and 2 are reserved
% frequency and bandwidth, respectively)

% Dipole antennas (lambda/2 or shorter):
% Directivity: 1.5
% Passive lambda/2 usable if aperture > 0.13*lambda^2 (otherwise active)
% Ref: Kraus/Marhefka: Antennas. 3rd ed., McGraw-Hill, 2002, p. 35.
% Rothammels Antennanbuch. 11th ed., Franckh-Kosmos, 1995, p. 422.
gains = (f > 0) .* 1.63;

% Single Yagi-Uda
% Ref: UCAM-CL-TR-577, p. 95
yagigain = 10.^((7.8 * log10(1./lambda) + 11.3)./10);
gains = cat(3, gains, yagigain);

% parabolic antennas
% ref: Rothammel, p. 728
gains = cat(3, gains, 0.5 .* (pi .* 1./ lambda) .^ 2);

[g, t] = max(gains, [], 3);

figure(4); semilogx(f(1,:), t); figure(1);

gain = 10 * log10(g);

% Terrestrial ITU-R P.372 minimum noise [dBuV/m] at frequency f, bandwidth b,
% and antenna gain g
% (Ref: Kuhn, UCAM-CL-TR-577, p. 92)
% We set Fa >= 0, as we assume that the background temperature
% will not drop below 290 K for terrestrial targets
function e=itunoise(f,b,g)
itu = interp1(log10([1e4, 7e4, 1.5e8, 10e9]), [148, 86, 0, 0], log10(f));
e = max(0, itu - 10 * log10(g)) + ...
20 * log10(f/1e6) + 10 * log10(b/1e6) - 36.8;

% Fieldstrength sensitivity of R&S AM524 active antenna system in dBuV/m
% for bandwidth b [Hz] (Ref: AM524 data sheet)
function s = sensitivity_am524(f, b)
s = interp1(log10([1e2 1e3 1e4 1e5 1e6 3e6 1e7 3e7 1e8 2e8 6e8 1e9]), ...
[ 0 -20 -34 -43 -48 -50 -50 -51 -54 -50 -40 -37], log10(f),
'spline');
bcfi = find(f > 3e7 & f < 2e8); % biconical antenna frequency index
s(bcfi) = interp1(log10([3e7 1e8 2e8]), [-50 -54 -50], log10(f(bcfi)),
'spline');
s(find(f > 1e9)) = -37; % extrapolated (horn)
s = s + 10*log10(b); % adjust for bandwidths other than 1 Hz

```

```

% round to the nearest s-series member (e.g., [1 2 5 10] or [1 3 10])
function y = roundl25(x, s)
e = floor(log10(x));
m = x ./ 10.^e;
y = 10.^(e+interp1(log10(s), log10(s), log10(m), 'nearest'));

```


Appendix C

1. Estimated costs

a. Production costs

The production costs may be in the dimension of 3800,00 € without tax; this includes the box, TFT, printer, cabling, IT basic equipment

b. Measurement costs

An accreditation measurement will be priced to 5000 € and in case of identical construction this type of measurement will take place only once time

The compliance measurement will be priced to 400 €; this price is only for the measurement including working time and documentation of the measurement

2. Estimated time for measurements

The accreditation measurement will need about ten days with preparation, measurement and the necessary documentation.

The compliance measurement will last for about 40 minutes only for the measurement; all further steps of work, transportation, packaging, documentation and so on can be done by other people and these steps are not time-critical.

Assuming that it will be possible to use two measurement cabinets, to have two shifts of working and it is a normal 5 day – week, it will last about 50 weeks to measure 10.000 machines.

In case of three shifts of working it will last about 33 weeks.