# 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

Council of Europe Publishing

Edition française:

*Les normes juridiques, opérationnelles et techniques relatives au vote électronique*

ISBN 92-871-5634-4

Council of Europe Publishing
F-67075 Strasbourg Cedex

ISBN 92-871-5635-2
© Council of Europe, April 2005
Printed at the Council of Europe

1. Recommendation Rec(2004)11, adopted by the Committee of Ministers of the Council of Europe on 30 September 2004, was prepared by the Multidisciplinary Ad hoc Group of Specialists on legal, operational and technical standards for e-voting (IP1-S-EE).

2. The publication contains the texte of Recommendation Rec(2004)11 and the explonatory memorandum thereto.

# Recommendation Rec(2004)11

## of the Committee of Ministers to member states on legal, operational and technical standards for e-voting

*(Adopted by the Committee of Ministers on 30 September 2004 at the 898th meeting of the Ministers' Deputies)*

The Committee of Ministers, under the terms of Article 15.*b* of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members for the purpose of safeguarding and promoting the ideals and principles, which are their common heritage;

Reaffirming its belief that representative and direct democracy are part of that common heritage and are the basis of the participation of citizens in political life at the level of the European Union and at national, regional and local levels;

Respecting the obligations and commitments as undertaken within existing international instruments and documents, such as:

– the Universal Declaration on Human Rights;

– the International Covenant on Civil and Political Rights;

– the United Nations Convention on the Elimination of All Forms of Racial Discrimination;

– the United Nations Convention on the Elimination of All Forms of Discrimination against Women;

– the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5), in particular its Protocol No. 1 (ETS No. 9);

– the European Charter of Local Self-Government (ETS No. 122);

– the Convention on Cybercrime (ETS No. 185);

– the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108);

– Committee of Ministers Recommendation No. R (99) 5 on the protection of privacy on the Internet;

– the document of the Copenhagen Meeting of the Conference on the Human Dimension of the OSCE;

– the Charter of Fundamental Rights of the European Union;

– the Code of Good Practice in Electoral Matters, adopted by the Council for Democratic Elections of the Council of Europe and the European Commission for Democracy through Law;

Bearing in mind that the right to vote is one of the primary foundations of democracy, and that, consequently, e-voting system procedures shall comply with the principles of democratic elections and referendums;

Recognising that as new information and communication technologies are increasingly being used in day-to-day life, member states need to take account of these developments in their democratic practice;

Noting that participation in elections and referendums at local, regional and national levels in some member states is characterised by low, and in some cases steadily decreasing, turnouts;

Noting that some member states are already using, or are considering using e-voting for a number of purposes, including:

– enabling voters to cast their votes from a place other than the polling station in their voting district;

– facilitating the casting of the vote by the voter;

– facilitating the participation in elections and referendums of all those who are entitled to vote, and particularly of citizens residing or staying abroad;

– widening access to the voting process for voters with disabilities or those having other difficulties in being physically present at a polling station and using the devices available there;

– increasing voter turnout by providing additional voting channels;

– bringing voting in line with new developments in society and the increasing use of new technologies as a medium for communication and civic engagement in pursuit of democracy;

– reducing, over time, the overall cost to the electoral authorities of conducting an election or referendum;

– delivering voting results reliably and more quickly; and

– providing the electorate with a better service, by offering a variety of voting channels;

Aware of concerns about certain security and reliability problems possibly inherent in specific e-voting systems;

Conscious, therefore, that only those e-voting systems which are secure, reliable, efficient, technically robust, open to independent verification and easily accessible to voters will build the public confidence which is a pre-requisite for holding e-voting,

Recommends that the governments of member states, where they are already using, or are considering using, e-voting comply, subject to paragraph iv. below, with paragraphs i. to iii. below, and the standards and requirements on the legal, operational and technical aspects of e-voting, as set out in the appendices to the present Recommendation:

i. e-voting shall respect all the principles of democratic elections and referendums. E-voting shall be as reliable and secure as democratic elections and referendums which do not involve the use of electronic means. This general principle encompasses all electoral matters, whether mentioned or not in the appendices;

ii. the interconnection between the legal, operational and technical aspects of e-voting, as set out in the appendices, has to be taken into account when applying the Recommendation;

iii. member states should consider reviewing their relevant domestic legislation in the light of this Recommendation;

iv. the principles and provisions contained in the appendices to this Recommendation do not, however, require individual member states to change their own domestic voting procedures which may exist at the time of the adoption of this Recommendation, and which can be maintained by those member states when e-voting is used, as long as these domestic voting procedures comply with all the principles of democratic elections and referendums;

v. in order to provide the Council of Europe with a basis for possible further action on e-voting within two years after the adoption of this Recommendation, the Committee of Ministers recommends that member states:

– keep under review their policy on, and experience of, e-voting, and in particular the implementation of the provisions of this Recommendation; and

– report to the Council of Europe Secretariat the results of their reviews, who will forward them to member states and follow up the issue of e-voting.

In this Recommendation the following terms are used with the following meanings:

– authentication: the provision of assurance of the claimed identity of a person or data;

– ballot: the legally recognised means by which the voter can express his or her choice of voting option;

– candidate: a voting option consisting of a person and/or a group of persons and/or a political party;

– casting of the vote: entering the vote in the ballot box;

– e-election or e-referendum: a political election or referendum in which electronic means are used in one or more stages;

– electronic ballot box: the electronic means by which the votes are stored pending being counted;

– e-voting: an e-election or e-referendum that involves the use of electronic means in at least the casting of the vote;

– remote e-voting: e-voting where the casting of the vote is done by a device not controlled by an election official;

– sealing: protecting information so that it cannot be used or interpreted without the help of other information or means available only to specific persons or authorities;

– vote: the expression of the choice of voting option;

– voter: a person who is entitled to cast a vote in a particular election or referendum;

– voting channel: the way by which the voter can cast a vote;

– voting options: the range of possibilities from which a choice can be made through the casting of the vote in an election or referendum;

– voters' register: a list of persons entitled to vote (electors).

Appendix I

## Legal standards

### A. Principles

*I. Universal suffrage*

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

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

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

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

*II. Equal suffrage*

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

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

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

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

*III. Free suffrage*

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

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

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

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

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

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

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

*IV. Secret suffrage*

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

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

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

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

### B. Procedural safeguards

*I. Transparency*

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

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

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

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

*II. Verifiability and accountability*

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

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

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

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

*III. Reliability and security*

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

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

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

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

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

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

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

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

Appendix II

## Operational standards

### *I. Notification*

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

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

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

*II. Voters*

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

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

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

*III. Candidates*

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

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

*IV. Voting*

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

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

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

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

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

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

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

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

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

*V. Results*

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

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

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

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

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

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

*VI. Audit*

59. The e-voting system shall be auditable.

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

Appendix III

## Technical requirements

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

### A. Accessibility

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

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

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

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

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

### B. Interoperability

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

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

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

### C. Systems operation

(for the central infrastructure and clients in controlled environments)

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

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

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

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

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

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

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

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

## D. Security

*I. General requirements*
(referring to pre-voting, voting, and post-voting stages)

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

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

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

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

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

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

83. E-voting systems shall generate reliable and sufficiently detailed observation data so that election observation can be carried out. The time at which an

event generated observation data shall be reliably determinable. The authenticity, availability and integrity of the data shall be maintained.

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

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

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

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

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

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

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

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

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

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

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

93. Residual information holding the voter's decision or the display of the voter's choice shall be destroyed after the vote has been cast. In the case of

remote e-voting, the voter shall be provided with information on how to delete, where that is possible, traces of the vote from the device used to cast the vote.

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

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

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

*IV. Requirements in post-voting stages*

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

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

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

## E. Audit

*I. General*

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

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

*II. Recording*

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

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

*a*. all voting-related information, including the number of eligible voters, the number of votes cast, the number of invalid votes, the counts and recounts, etc.;

*b*. any attacks on the operation of the e-voting system and its communications infrastructure;

*c*. system failures, malfunctions and other threats to the system.

*III. Monitoring*

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

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

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

*IV. Verifiability*

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

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

*V. Other*

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

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

### F. Certification

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

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

# Explanatory memorandum

## Background

1. Common standards on e-voting, which reflect and apply the principles of democratic elections and referendums to the specificities of e-voting, are key to guaranteeing that all the principles of democratic elections and referendums are respected when using e-voting, and thus to building trust and confidence in domestic e-voting schemes.

2. Such common standards are also important for the interoperability of e-voting systems in order to ensure the development of secure and effective e-voting systems. While interoperability across borders in Europe may not seem necessary from a purely legal and operational point of view – at the time of adoption of the recommendation there were no cross-border common electoral procedures in place (notwithstanding data exchange procedures with respect to a limited group within the electorate for the European Parliament) – interoperable and open technical standards within and across member states' borders can both ensure the combined and continued use of e-voting systems supplied by different providers and reduce procurement costs for domestic authorities.

3. This set of standards consists of the legal, operational (mainly relating to organisational and procedural matters) and core technical requirements for e-voting. The legal standards are intended to apply the principles of existing Council of Europe and other international instruments relating to elections, to e-voting.

4. The recommendation has been developed by the Multidisciplinary Ad hoc Group of Specialists on legal, operational and technical standards for e-voting (IP1-S-EE). This intergovernmental group of all member states was set up by the Committee of Ministers and was entrusted with the task of developing a set of standards for e-voting that reflect the

differing circumstances of Council of Europe member states and should be followed by the information and computer technology (ICT) industry.

### Scope of the recommendation

5. The recommendation covers political elections and referendums, both of which are part of the European democratic heritage and require standards. Elections and referendums are held at different levels; in some countries no referendums are held, and in some countries not all the levels mentioned in the recommendation are affected.

### Reasons for introducing or considering the introduction of e-voting

6. The reasons for introducing or considering the introduction of e-voting in one or more stages of a political election or referendum can differ from country to country. In each country, the reasons depend on the specific domestic context.

### Competence of member states

7. The competence of the member states of the Council of Europe in electoral matters and regarding referendums is not affected by this recommendation. Where reference is made to the European Union level, the purpose is to include reference to elections to the European Parliament.

### Principles of democratic elections and referendums

8. Democracy is inconceivable without elections and referendums held in accordance with certain principles that lend them their democratic status. In 2002, the European Commission for Democracy through Law (Venice Commission) adopted a non-binding Code of Good Practice in Electoral Matters[1] in which five such principles are identified as fundamental: universal, equal, free, secret and direct suffrage. These

[1] Code of good practice in electoral matters: (Venice Commission – Opinion 190/2002_el), endorsed by Parliamentary Assembly Resolution 1320 (2003) and CLRAE Resolution 148 (2003), subject of a Declaration by the Committee of Ministers (114th session, 13 May 2004)).

five principles reflect Europe's democratic heritage[1] and are equally applicable to e-elections and e-referendums as to traditional elections and referendums.

9. Although no generally agreed definitions of these principles exist, their meaning can for the purposes of this explanatory memorandum be summarised as follows:

– *universal suffrage*: all human beings have the right to vote and to stand for election subject to certain conditions, for example age and nationality;

– *equal suffrage*: each voter has the same number of votes;

– *free suffrage*: the voter has the right to form and to express his or her opinion in a free manner, without any coercion or undue influence;

– *secret suffrage*: the voter has the right to vote secretly as an individual, and the state has the duty to protect that right;

– *direct suffrage*: the ballots cast by the voters directly determine the person(s) elected.

10. Although these principles are generally accepted, their implementation in the context of e-voting raises a number of questions that call for close scrutiny. However, specificities of e-voting do not give rise to such questions to the same extent in relation to all of the five principles. Whereas for the principles of universal, equal, free and secret suffrage special provisions with regard to e-voting are necessary, the principle of

[1] Point 7 of the Document of the Copenhagen Meeting of the Conference on the Human Dimension of the OSCE of 29 June 1990 clearly speaks of free, universal, equal and secret suffrage; point 6 of direct suffrage, albeit in a qualified form; Article 25(b) of the International Covenant on Civil and Political Rights expressly provides for all these principles except direct suffrage, although the latter is implied (Article 21 of the Universal Declaration of Human Rights); Article 3 of the Additional Protocol to the European Convention on Human Rights explicitly provides for the right to periodic elections by free and secret suffrage; the other principles have also been recognised in human rights case-law (universality: ECHR No. 9267/81, judgment in Mathieu-Mohin and Clerfayt v. Belgium, 2 March 1997, Series A vol. 113, p. 23; judgment in Gitonas and Others v. Greece, 1 July 1997, No. 18747/91, 19376/92; 19379/92, 28208/95 and 27755/95, *Reports of Judgments and Decisions*, 1997-IV, p. 1233; re. equality: aforementioned judgment in Mathieu-Mohin and Clerfayt, p. 23). The right to direct elections has been admitted by the Strasbourg Court implicitly (ECHR No. 24833/94, judgment in Matthews v. The United Kingdom, 18 February 1999, *Reports of Judgments and Decisions* 1999-I, paragraph 64).

direct suffrage does not call for special attention and is therefore not addressed in the recommendation.

11. The standards in the recommendation address only those matters that are of specific relevance to e-voting. The general principles of democratic elections and referendums are not repeated.

### Legal, operational and technical standards

12. Appendices I to III of the recommendation contain a set of legal, operational and technical standards. This set consists of minimum standards, which, if followed in an e-voting system, would facilitate compliance with the principles of democratic elections and referendums. However, compliance with these standards alone does not guarantee the democratic quality of the e-election or e-referendum. The e-election or e-referendum has to be judged as a whole and in detail, in the specific context. But compliance with the standards is an important element in enhancing the democratic quality of the e-voting system.

13. There is a close interconnection between the three categories of standards which need to be taken into account when applying the recommendation:

– the legal standards relate to the legal context in which e-voting is permitted;

– the operational standards relate to the manner in which e-voting hardware and software should be operated and maintained;

– the technical requirements relate to the construction and operation of e-voting hardware and software. The adoption of the technical requirements will ensure the technical security, accessibility and interoperability of e-voting systems.

The three categories of standards all include provisions relating to all stages of elections and referendums (that is, the pre-voting stage, the actual casting of the vote, and the post-voting stage). The interconnection can relate to one, two, or all stages.

#### *i. Introductory statement ("e-voting shall respect ...")*

14. This introductory statement covers a number of issues that are of general relevance in relation to e-elections and e-referendums.

15. Existing non-electronic voting systems have been developed in a way that ensures that the principles required for democratic elections and referendums are met. It is essential that these principles are not undermined by the introduction of new voting methods and, accordingly, e-voting systems must be designed and operated so as to ensure the reliability and security of the voting process, as is the case with the non-electronic voting systems in the state concerned.

16. In order to ensure that an e-voting system delivers an election or referendum that satisfies the principles overall, it may be necessary to give more attention to the application of one principle than to that of another. However, the result must still be to ensure that overall the principles are met.

17. The comparison with the non-electronic voting system in the state concerned does not imply that e-voting has to be as secure and reliable as all the non-electronic voting channels together. The underpinning principle of the recommendation is that a remote e-voting channel has to be – overall – as secure as an unsupervised remote non-electronic voting channel and a non-remote e-voting channel has to be as secure as a non-remote non-electronic voting channel.

18. Furthermore the comparison with non-electronic voting channels is not intended to prevent a state changing its non-electronic voting system, as long as the changes are in compliance with all the principles of democratic elections and referendums.

19. Comparing levels of reliability and security or other parameters, at the time when e-voting is introduced, with levels of non-electronic voting methods is not intended to freeze non-electronic voting levels, in particular when improvements in implementing the principles of democratic elections and referendums are possible and necessary.

### *ii. Review of domestic legislation*

20. The recommendation indicates that member states should consider reviewing their relevant domestic legislation when introducing e-voting. Careful thought needs to be given to aspects of law other than those relating simply to the electronic equipment needed and its use. The extent of the review advisable will depend upon the existing laws of the member state in question and it is not possible to set these out in a

comprehensive manner here. Examples include criminal laws relating to election matters, specific data protection laws and laws relating to election observation.

*iii. Localisation*

21. The purpose of this recommendation is to provide for common standards on e-voting. In some states holding elections and referendums involves certain procedures which are very specific to the state concerned. Where such specific procedures are applicable only in one or a very small number of member states, those procedures were identified as "localisms" and therefore not included in the recommendation, but referred to in the explanatory memorandum. States concerned can retain their "localisms" and, if they so wish, adapt them in the future, and are not expected to abandon or change their "localisms" as a consequence of the recommendation, as long as these are in compliance with the principles of democratic elections and referendums and any obligations and commitments undertaken by member states.

*iv. Sustainability*

22. E-voting is a new and rapidly developing area of policy and technology. Standards and requirements need to keep abreast of, and where possible anticipate, new developments. In recognition of this, paragraph v. recommends that each member state keep its own policy on e-voting under review and report back to the Council of Europe the results of any review that it has conducted. The Council of Europe may look again at this issue two years after the adoption of this recommendation and member states may bear this timing in mind when deciding whether, and if so when, a review is appropriate in their particular circumstances.

23. As part of the follow-up, a review of the recommendation may be considered as soon as member states have gained further experience with e-elections or e-referendums.

24. Technological developments, unforeseeable at the time of the adoption of the recommendation, cannot exclude that any system valid at that time, including Election Markup Language (EML), may one day not be the most appropriate system for e-elections or e-referendums, and thus not be recommended by individual, or groups of, countries.

## Interpretation

25. The interpretation paragraph contains definitions of terms used throughout the recommendation, including its appendices. The definitions should also be consulted when the recommendation or parts of it are translated into other languages. In Appendix 3 there is a separate technical glossary which contains additional definitions of terms used in that appendix.

## Definition of remote e-voting

26. E-voting can be conducted in remote and non-remote ways. Many electoral systems already include both non-remote and remote voting. Remote voting can be conducted in both supervised (for example voting at embassies or consulates, voting at post offices or municipal offices) and unsupervised (that is unsupervised by officials) environments (for example voting by mail). Each member state has its own established practice concerning the types of voting channels available to voters.[1] For the purpose of this recommendation, however, remote e-voting means exclusively e-voting where the casting of the vote is via a device not controlled by election officials.

[1] The European Commission for Democracy through Law (Venice Commission) has provided a report on the compatibility of remote voting and electronic voting with the requirements of the documents of the Council of Europe (adopted by the Venice Commission at its 58th Plenary Session (Venice, 12-13 March 2004). Study No. 260, 2003, Strasbourg, 18 March 2004, CDL-AD (2004)012 Or. Fr.). The conclusion by the Venice Commission is that remote voting is compatible with the Council of Europe's standards, provided that certain preventative measures are observed in the procedures for either postal voting or electronic voting.

Appendix I

## Legal standards

### A. Principles

### I. Universal suffrage

*Standard No. 1. "The voter interface of an e-voting system ..."*

27. No single voting system may ever be understandable and usable by every possible voter; for example, people with visual impairments may not be able to use a visual-only system. In order to ensure democratic elections and referendums, member states have to try to ensure that the voter interfaces of e-voting systems are usable and understandable by as many people as possible.

*Standard No. 2. "Possible registration requirements for e-voting ..."*

28. The purpose of this provision is to ensure that no voter is prevented from using e-voting because of difficult registration procedures.

*Standard No. 3. "E-Voting systems shall be designed ..."*

29. E-voting systems should be made accessible as far as possible and used in conjunction with other voting channels that together with the e-voting system provide accessibility for as many voters as possible. Not all persons with disabilities may be able to use e-voting. The design of the e-voting systems should, however, aim to maximise the potential of accessibility that these voting channels provide for disabled persons.

*Standard No. 4. "Unless channels of remote e-voting are ..."*

30. Adding additional electronic voting channels to traditional forms of voting may make elections and referendums more accessible, strengthening the principle of universality. However, using a single remote electronic voting channel in isolation restricts accessibility. This provision is to protect the voter from a situation where the only means offered for voting is one that is not effectively available to him or her.

31. In the case of non-remote e-voting it has to be left to member states to decide whether they want to offer other options of voting. As is the case with all non-remote voting, places where voting takes place and the e-voting system should comply with standards of accessibility.

## II. Equal suffrage

*Standards Nos. 5 and 6. "In relation to any election or referendum ..." and "The e-voting system ..."*

32. The whole voting system should prevent multiple votes being cast by any one person. This principle is consistent with voting systems that allow voters to choose more than one option, such as systems that allow preferential votes, or one vote for a national list and one vote for a regional list. The concept of multiple votes relates to the risk that there might be an attempt to cast more votes than a particular voter has a right to cast. This might arise if the voter tried to cast multiple votes him or herself or if another person tried to use the voter's identity in order to vote in the voter's name and the voter also voted.

33. In some member states practices are in force where it may appear that a voter is allowed to vote more than once. However, in these systems the voter may cast only one vote that is finally counted. Examples of this include:

*a*. In the case of Denmark and Sweden, the voting systems provide the legal opportunity for voters to submit an advance vote and change it later. In Denmark, several advance votes may be submitted. In Sweden, only one advance vote may be submitted. In both systems only the last vote is inserted into the ballot box and thus is the vote cast.

*b*. In the case of the United Kingdom, if a person enters a polling station to vote and finds that somebody else has already voted in that person's name, that person is entitled to cast a special vote – a tendered ballot. This ballot is sealed in an envelope, is not placed in the ballot box, and is only looked at in the case of an election petition and in accordance with a direction of a court. A similar provision applies where two postal votes are received for the same voter.

*Standard No. 7. "Every vote deposited ..."*

34. It is important that all votes cast by either electronic or non-electronic voting channels are counted.

## III. Free suffrage

*Standard No. 9. "The organisation of e-voting ..."*

35. Personal suffrage – the personal exercise of the right to vote – is a fundamental principle in many member states. As it is particularly vulnerable in the context of remote e-voting, special attention is drawn to this fact in the recommendation. However, this standard does not prevent remote e-voting.

36. There are some member states that allow for voting procedures where, in order to ensure accessibility, the principle of universality is given priority over the principle of personal suffrage and therefore, for example, proxy voting is allowed. This is also possible within the e-voting standards.

37. Where remote e-voting channels are provided, special attention has to be given to the provision of facilities that allow the voter to exercise the right to cast a vote in a supervised environment.

*Standard No. 10. "The way in which voters ..."*

38. "Without reflection" means without having had enough time to think about it.

*Standard No. 11. "Voters shall be able ..."*

39. Only the voter must have access to the vote. For example, the e-voting facilities should not enable the completed ballot to be stored on the voter's device and the vote cast later. No one other than the voter should have access to the vote, either on the device or during the transmission to the ballot box.

*Standard No. 12. "The e-voting system shall not permit ..."*

40. The e-voting system should be designed and operated in a way that ensures that all forms of manipulative influence are excluded. For example, sounds which can be associated with a candidate or an option, pop-up screens promoting a particular choice and similar devices should be prevented, as far as possible.

*Standard No. 13. "The e-voting system shall provide the voter ..."*

41. In non-electronic voting systems voters are able to cast a blank vote, that is, not to express a preference for the proposed choices. This standard provides that the possibility of leaving the ballot blank is maintained with e-voting.

42. It is a matter for each member state's domestic policy whether the intended spoiling of a ballot paper or intentional casting of a non-blank invalid vote is possible with e-voting as well.

*Standard No. 14. "The e-voting system shall indicate clearly ..."*

43. Generally speaking, the voting procedure is completed successfully when the electronic vote is deposited in the electronic ballot box. In the context of remote e-voting this means that the voting procedure is completed successfully only when the vote has been sent from the voter's voting device (PC, telephone,

etc.), over the Internet or another network and has reached its destination, that is the ballot box server.

44. The message confirms to the voter that his or her vote is deposited in the ballot box and thus will be counted. The voter then knows that he or she has cast his or her vote, which is important from the point of view of trusting the system and because of the principle that every vote cast has to be taken into account. Furthermore, the voter must be able to know at what moment the whole voting procedure is completed successfully and he or she can safely end the connection. Both messages (the successful casting of the ballot and the completion of the procedure) could be combined in one, if both events coincide.

## IV. Secret suffrage

45. All international obligations and commitments pertaining to secret suffrage that bind a member state need to be implemented with any e-voting system used by that state.

*Standard No. 16. "E-voting shall be organised in such a way ..."*

46. Secrecy must apply to the entire procedure: in the pre-voting stage (for example, the transmitting of PINs or electronic tokens to voters), during the completion of the ballot paper, the casting and transmission of the ballot and during counting and any recounting of the votes.

*Standard No. 17. "The e-voting system shall guarantee that votes ..."*

47. This standard provides that it must never be possible to reconstruct the content of any voter's vote and link it to the voter who cast it.

48. In the context of (remote) e-voting special attention has to be given to the principles of free and secret suffrage. Only entitled voters are allowed to cast a vote, which means that every voter has to be authenticated and his/her right to vote has to be checked. Domestic legislation may vary on the extent of identification (indication of the voter's name, showing of an ID card, etc.), but the basic principle remains the same: in order to prevent multiple votes being cast or other misuse, the voter has to be authenticated and a record must be made and checked in order to establish whether he or she has already cast a vote.

49. At a certain stage in the remote voting process the voter's identity and the voter's vote may be connected in some way. If the content of the vote were to be made known at that stage, or if the connection between voter and vote were

to be kept and the content of the vote made known at a later stage, the secrecy of the vote would be breached. In traditional voting systems the separation of voter identification and vote is made by physical separation. This physical separation can easily be controlled by election officials and election observers. In non-remote e-voting processes the voter authentication and the vote could also be separated physically, as is the case if the e-voting system is used only for the casting of the vote. With a remote electronic voting system this separation has to be made electronically. The electronic separation requires specific technical solutions. This fact has to be taken into account when introducing e-voting.

50. In voting systems that provide a legal opportunity for voters to submit an advance vote and change it later (for example, Sweden), it must be possible to identify a specific person's sealed vote to be able to retract that specific vote. The identification and retraction of such a vote must be done without jeopardising the secrecy of the vote; in other words, a vote must be completely sealed throughout the voting, storage and retraction processes. But the sealed vote must still be linked to a specific voter.

51. The moment of inserting a vote into the electronic ballot box is the latest point in time at which the vote must be separated from the information on who has cast it – without any possibility of ever reconstructing this link.

52. In some cases domestic law requires a permanent link between the voter and the vote to exist and to be maintained during the election or referendum and for a specific period thereafter (for example, in the United Kingdom). In such cases, it has to be assured that the link between a voter and his or her ballot paper is sufficiently protected throughout the period in order to ensure the secrecy of the vote. This is only revealed pursuant to an order of a competent judicial authority and it must be ensured, that even where the link is so revealed, no voter is compelled to reveal how he or she has voted.

*Standard No. 19. "Measures shall be taken to ensure ..."*

53. The necessary measures would include, for example, that the votes cast must be stored randomly in the electronic ballot box. The order in which they are stored must not make it possible to reconstruct the order in which they arrived.

### B. Procedural safeguards

54. The procedural safeguards ensure that all principles of democratic elections and referendums are implemented and maintained in an e-voting context.

## I. Transparency

*Standard No. 20. "Member states shall take steps to ensure that ..."*

55. Confidence by voters and candidates in the voting system(s) used is essential, not only to participation but also to the democratic system of the member state. Full understanding of the e-voting system(s) in use is the basis for this confidence.

56. Traditional voting methods are simple and well tried and tested in member states. Voters are familiar with voting systems using ballot papers and ballot boxes and understand the general rules that govern how they should vote and how their vote is collected and counted unaltered. The introduction of e-voting produces a new situation in which voters will be less familiar with the electoral process and perhaps less able to understand the safeguards built into the e-voting system. Accordingly, as e-voting systems are introduced, it is likely that, in order to maintain voter understanding and confidence, steps will have to be taken to introduce the system to voters. Over time, it may be necessary to continue to take such steps in order to secure the understanding and confidence of voters who are unfamiliar with e-voting.

57. Confidence can be enhanced by providing voters with as much information as possible about the method of e-voting being used.

*Standard No. 22. "Voters shall be provided with an opportunity to practise ..."*

58. A new e-voting system may cause voters anxieties of different kinds. In order to promote understanding and confidence in any new e-voting system, including in its transparency, opportunities to try out the system should be provided before, and separately from, the moment of casting an electronic vote. Special attention should be paid to any voters who are not familiar with the new e-voting method, for example the elderly.

*Standard No. 23. "Any observers, to the extent permitted by law ..."*

59. There are various international and domestic obligations on election observation: by representatives of candidates, as well as by independent domestic and/or international observers. All member states are bound to the commitments of the Document of the Copenhagen Meeting of the Conference on the Human Dimension of the OSCE of 29 June 1990 to "invite observers from any other OSCE participating state and any appropriate private institution and organisation who may wish to do so to observe the course of their national

election proceedings [… and …] facilitate similar access for election proceedings held below the national level".

60. Observers should be able to verify that the e-voting system itself is designed and operated in a way which respects the fundamental principles of democratic elections and referendums. Therefore, member states should have clear legal provisions on observers' access to the e-voting system documentation and audit data.

61. E-elections/e-referendums pose special challenges to observers, inherent in the electronic method of the election or referendum. Observers will thus have to be provided with an opportunity, in particular, to have access to relevant software information, to see physical and electronic safety measures for servers, to inspect and test certified devices, to have access to and test sites and information provided for remote e-voting, and to observe cast electronic votes entering the electronic ballot box and that votes are being counted. Security measures for telephone or Internet voting may, however, make it necessary not to allow the presence of observers in the computer room itself. In that case measures should be taken in order to give the observers the opportunity to monitor the activities.

### II. Verifiability and accountability

*Standard No. 24. "The components of the e-voting system …"*

62. Assessment that e-voting systems function correctly and that security is maintained is essential. This can be done by the independent evaluation or certification of the system as a whole or of its components, which requires disclosure of the critical system elements. The assessment can be carried out through, for example, disclosure of the system design, inspection of detailed documentation, source code disclosure, inspection of component evaluation and certification reports, in-depth penetration testing, etc. The actual level of disclosure of the system elements needed to achieve appropriate assurance depends on the specific features of the system, its components and the services provided.

*Standard No. 26. "There shall be the possibility for a recount."*

63. The recount is a procedure that verifies election and referendum results that have already been established. There are different possibilities for recounts in the case of e-voting, which differ in their complexity and in their contribution to accountability. A very simple method of recounting can be produced by instructing the e-voting system to perform a second count. A second option is to transfer the electronic ballot box to a similar but distinct e-voting system and perform the second count on that system. A third option is to let the recount be

carried out by a different system, which is interoperable with the e-voting system. A fourth option is to produce, at some stage of the voting process, paper ballots and to use these for recounting.

64. To verify the result, it may not be sufficient only to conduct a recount. Depending on the architecture of the system used, there may be further elements that contribute to the correctness of the result. The confirmation that all votes cast have been considered is an example.

*Standard No. 27. "The e-voting system shall …"*

65. If a re-run of an e-election or e-referendum becomes necessary, that re-run may not be possible without the support of the e-voting system that was used in the original election or referendum, even if that e-voting system is not to be used in the re-run itself. This may be the case if the persons who are entitled to vote can be identified only by using information that is available by means of that the original e-voting system.

## III. Reliability and security

*Standard No. 28. "The member state's authorities shall ensure ..."*

66. The new voting channels need to be as reliable and secure as traditional voting methods. The member state has to guarantee that this is the case; the final responsibility can never be delegated to a voting system supplier.

*Standard No. 29. "All possible steps shall be taken ..."*

67. Throughout the whole electronic voting process, there must be no intervention unrelated to the voting which affects either the ballot and election or referendum server or the electronic ballot box server. The recommendation is not intended to suggest that every possible method of protection available must be used in every case. In each case a judgment will have to be made as to the nature and extent of the protection measures to be applied. This judgment will require a proper balance to be struck between different factors. For example, in a particular case a balance may need to be struck between the all-important need for security and the advisability of having systems that are easily usable by voters. In such a case usability must not override the need for high levels of security but may be a factor in determining which security measures should be adopted. A similar position might apply were a very small additional security benefit to be achievable but only at an excessively high cost.

*Standard No. 30. "The e-voting system shall contain measures to preserve …"*

68. An e-voting system should be protected against malfunction and breakdown. However, the possibility of a breakdown can never be entirely excluded (see Appendix III, Standard No. 77).

*Standard No. 31. "Before any e-election …"*

69. The standard requires that the correct functioning of an e-voting system is verified (cf. Standard No. 24). Furthermore, it has to be ensured that the verified e-voting system is actually being used during the e-election or e-referendum. Verification should prevent any e-voting system being installed where that system or any component of that system hasbeen tampered with or might have been replaced. The authority needs to ensure that the correct system is put into service.

*Standard No. 33. "While an electronic ballot box is open, any authorised intervention ..."*

70. "Any" indicates that, if election observers are allowed by domestic law, then they should have access. Security measures for telephone or Internet voting may make it necessary to prohibit the presence of observers in the computer room. In that case measures should be taken in order to give the observers the opportunity to monitor the intervention.

*Standard No. 34. "The e-voting system shall maintain …"*

71. From the moment the vote is cast, no one should be able to read or change it or relate the vote to the voter who cast it. This is achieved by the process of sealing the ballot box, and where the ballot box is remote from the voter, by sealing the vote throughout its transmission from voter to ballot box. In some circumstances, sealing has to be done by using encryption.

72. To seal any ballot box, physical and organisational measures are needed. These may include physically locking the box, and ensuring that more than one person guards it. In the case of an electronic ballot box, additional measures may be necessary, such as access controls, authorisation structures and firewalls.

73. To seal an electronic vote for its transmission from voter to the ballot box (remote from the voter), encryption is required in addition to physical and organisational measures.

74. A vote is sealed when its content has been subjected to measures ensuring that it cannot be read, changed, or related to the voter who cast it.

Appendix II

## Operational standards

### I. Notification

*Standard No. 36. " Domestic legal provisions governing ..."*

75. An e-election or e-referendum can differ from a traditional election or referendum with regard to the procedures that have to be followed by voters. Examples of potential differences are the period of time during which votes can be cast, the steps a voter has to take in order to participate in the e-election or e-referendum and the way the e-voting actually takes place. These differences should be communicated to the voter in order to avoid any misunderstanding of the procedures and in order to give the voter all the information necessary to be able to make an informed decision as to whether or not he/she wishes to use the available e-voting channels. Careful consideration should be given to deciding how much time the voter needs for this decision.

*Standard No. 37. "The period in which an electronic vote can ..."*

76. Communicating the period of time for voting is especially important where this period of time differs in the case of an e-voting channel. This difference arises particularly in the case of remote e-voting in which the choice may be made to have a different period of time for voting using the electronic voting channels, due to the specific nature of those channels.

*Standard No. 38. "The voters shall be informed ..."*

77. Communicating the procedures, and the steps the user has to take, is important because the use of electronic voting channels will in most cases mean that the voter has to have access to certain equipment in order to use a particular electronic voting channel. For example, in the case of the Internet as a channel, most personal computers that can connect to the Internet will be able to use this facility, but it is always possible that a small percentage of voters that use old computers or old software will not be able to use the Internet channel. Thus, it should be made clear what equipment is necessary in order to use a particular channel. Consideration should also be given to offering the voter the opportunity to try the suitability of his/her equipment before he/she decides to use a specific electronic voting channel. Consideration should also be given to allowing the voter to change his/her preferred electronic voting channel in the case that he/she cannot use that specific channel. For example, the voter could choose to switch from the Internet channel to the telephone channel, if both channels are being offered.

## II. Voters

*Standard No. 39. "There shall be a voters' register ..."*

78. It is necessary to check whether or not a specific person has the right to vote and whether or not a specific voter has cast a vote. There are a variety of means to perform this check in non e-voting situations. Such checks can involve measures ranging from physically marking in a register persons who have voted to registering by electronic means the fact that a person has actually cast his/her vote.

79. For these checks to be accurate, it is necessary that the registers in question contain up-to-date information as to those who have a right to vote at the election or referendum in question. Therefore these registers need to be updated before an election or referendum takes place. It should be noted that the use of the word "register" in the singular does not necessarily imply that there must be one single register that contains all the voters in a whole country or region.

80. In the case of remote e-voting, these checks are necessarily performed using registers. Although it is feasible that in some cases paper-based registers could be used, in most remote e-voting schemes, the registers will have to be electronic. Where remote e-voting channels are available to a voter in parallel with voting in polling stations, the polling station officials should be able to verify whether that voter has already cast a vote.

81. The registers in question will in practice be created by different procedures. In some countries population registers exist which include almost all the voters (but may, for example, not include expatriate voters). Using these population registers it is possible to derive, often by electronic means, the registers that specifically contain the persons who are entitled to vote (the voters' registers). In other countries where these population registers do not exist, voters' registers have to be prepared by a registration procedure that, among other things, involves persons applying to be registered as voters. These procedures will differ from country to country.

82. Persons claiming the right to vote should be able to check whether they are registered on the voters' register and whether their personal information is correct. In some member states the voters' register may be published (or accessible to the public). In other member states, personal data protection laws allow persons to check only their own registration.

*Standard No. 40. "The possibility of creating an electronic register …"*

83. It is conceivable that online registration will be offered to voters. This implies the existence of some means of electronic authentication through, for

example, a digital signature and the existence of electronic registers. It is also conceivable that voters are enabled to apply for remote e-voting in an online or electronic way, for example after they have registered themselves. It should be noted that, for both possibilities, a very substantial effort will be necessary in order to solve the problems of identification and authentication in a remote electronic way. Therefore, the standard only provides for online registration to be considered.

## III. Candidates

*Standard No. 43. "A list of candidates that is generated …"*

84. In order to offer the voters the voting options, complete lists of candidates must be created. These lists of candidates will be publicly presented in a variety of ways. Most common will be paper-based candidate lists. The use of new media, such as the Internet, for publicising this crucial information for the voter, is one of the ways in which more voters may be reached. Naturally, the Internet should not be the only way of publicising the candidate lists. If the Internet is used to create the candidate list (for example, by allowing online candidate nomination), it should be ensured that the lists of candidates generated are complete, accurate and authentic. This implies the use of digital signatures and certificating the website in an appropriate way.

85. In the case of non-remote e-voting, the voting machines in the polling station will probably contain all the information that is present on the ballot paper. With some types of voting machines, this information will be contained in a hardware display, for example on the physical buttons the voter has to press. In other situations, the information will be presented in digital form and one could speak of an electronic ballot.

## IV. Voting

*Standard No. 44. "It is particularly important, where remote e-voting takes place …"*

86. The system for checking voters must be such that it is permanently updated with regard to those who have already cast a vote. However, if some voters are allowed to cast a vote only in the polling station and a separate register is being kept for those voters, the register of the remote e-voting system does not have to be updated with regard to those voters. In such a case, other methods may be required in order to prevent voters voting both in a polling station and by the other means available.

87. The introduction of remote e-voting brings with it the question of how the periods of time for voting in the polling station and remote e-voting are related. At first sight, it would seem logical that, for both methods of voting the same periods of time should apply, in order to avoid complications and distinctions. However, reasons that can lead to different periods of time being used include:

– when casting a vote in a polling station is the fall-back option for voters who are within the national territory of the election or referendum in case the electronic voting channel breaks down, the closing time for the electronic voting channel may have to be before the closing time of the polling station.

– when the system is designed and operated in such a way that voters can choose between channels without prior registration and the channels used do not have a common register in which it is noted which voters have already cast their vote, the periods of time when these channels are available should in general not overlap.

88. Whatever the outcome of these architectural considerations, counting should only start after the closure of all the channels.

*Standard No. 45. "Remote e-voting may start and/or end at an earlier …"*

89. For various reasons, the period of remote e-voting may be longer than the period during which the polling stations are open. These reasons include providing a better service for citizens and enhancing accessibility.

90. However, remote e-voting should not continue after the end of the voting period at polling stations. In the case of the e-voting system being unavailable (for example in the case of a voter's PC not working due to a power failure), the voter, who is resident or staying within the country where the election or referendum takes place, should still be able to go to the polling station to cast his or her vote. If e-voting continued after polling stations had closed, the voter would not have this possibility. Future developments may, however, demonstrate that this recommendation as to the time at which e-voting should end is unnecessary. This is a matter that may be reviewed when the Council of Europe next considers the effects of this recommendation, and it would be beneficial if member states could include any experience they have of the issue in any reports they make to the Council on their consideration of e-voting or their e-voting experiences.

91. In order to accommodate possible delays in the transmission of electronic information, the acceptance of electronic votes cast before the end of the e-voting period should remain open for a sufficient period of time after the closure of the e-voting period (see Standard No. 96, Appendix III to the recommendation).

*Standard No. 46. "For every e-voting channel, support …"*

92. Support and guidance arrangements on voting procedures should be in place regardless of the specific channel used. In the case of electronic voting channels, for each electronic voting channel these arrangements will be available using at least the same electronic voting channel. That is, a website with help information and e-mail facilities should be in place when the Internet is the channel and a telephone hotline should be in place when voting by telephone is possible. Furthermore, fall-back arrangements on a different remote channel should be provided for situations in which one of the electronic voting channels is out of order. For example, a telephone hotline might be a suitable alternative to remote e-voting over the Internet.

93. These support and guidance arrangements should not endanger the secrecy of the vote.

*Standard No. 47. "There shall be equality in the manner of presentation …"*

94. Each voting option should be equally accessible to the voter within each channel. Equality of presentation may not be possible or appropriate between different channels. Mobile phone screens, digital TV screens, and PC screens display information in different ways.

95. It should be recognised that, although the arrangement of candidate names on screens might seem to be a purely technical matter, it is of a far more important nature and thus cannot be left solely to the technical designers of the e-voting system.

96. In order to ensure equality, it is also necessary to provide protection measures to prevent the omission of information that should appear on the electronic ballot. In the absence of such measures there would be a risk that the result of the election or referendum would be affected because a possible choice for the voter had been omitted from some or all of the ballots cast by electronic means.

*Standard No. 48. "The electronic ballot by which …"*

97. During the casting of the vote, the voter's immediate environment should be free from objects and information that could influence his/her choice in a partisan way. In the case of the Internet, this environment includes, in particular, the screens that are generated on a voter's computer when accessing the e-voting website. These screens should not contain more information about the choices than paper ballots, such as pop-up screens that promote a specific candidate or audio elements that are associated with a particular candidate or point of view.

98. “Other messages” means partisan messages that may influence the voter, other than those allowed by domestic legal provisions. It does not prevent the display of, for example, official information on voting options.

*Standard No. 49. “If it is decided that information about voting options will be …”*

99. This standard does not conflict with the previous standard. It deals with the process of decision making, whereas the previous standard deals with the process of casting a vote.

*Standard No. 50. “Before casting a vote using a remote e-voting system …”*

100. Voting using the Internet is not currently a common practice. Unless the attention of members of the public is specifically drawn to the fact that Internet voting is real voting at a real election or referendum there is a risk that they may mistakenly imagine that they are taking part in a fake election or referendum or a test. On the other hand, if too little attention is drawn to the fact that people are participating in a demonstration or test version, they could get the impression that they have already voted. Also, an election or referendum might be confused with an opinion poll or vice-versa.

*Standards Nos. 51 and 52. “A remote e-voting system …” and “In a supervised environment …”*

101. In a supervised environment, the e-voting system should include provision for the disappearance of any information that could be used as proof of the content of the vote cast. If the national electoral legislation requires that the e-voting system supplies the voter with a paper proof of his/her electronic vote, this proof should be subject to the same secrecy requirements as a paper ballot. The voter should not be able to show this proof to any other person, or take it out of the polling station. For instance, the voter could be required to deposit the paper proof in a box in the polling station, or in a device which destroys it.

102. In a remote e-voting system using the Internet, the voter has to be able to delete information connected to his or her vote from the device used to cast the vote. One of the features of the most common way to use the Internet, that is by means of a “browser” on the voter’s machine and a “server” on the side of the election officials, is that the display and storage of information on the voter’s side cannot entirely be controlled by the “server”. This makes it necessary to pay specific attention to the way in which the anonymity and secrecy of the vote is realised in e-voting systems. There are at least three layers to be considered. The first one is the web application level. The second level is that of the browser. The third level is that of the utility software on the computer of the voter.

– the web application should not allow the user to retain a copy of his or her vote. This means that the application should not offer the functionality of printing, saving or storing the vote or (part of) the screen on which the vote is visible.

– the browser also should not offer the option of printing the screen on which the vote is visible. It should be noted that browsers can and do retain information in several ways. For example, by using the "back" button on a browser, one or more previous screens can be displayed. As far as possible, this generic functionality of browsers should be disabled by the web application. At the very least, there should be no storing of information after the voter has finished casting the vote.

– the third level that has to be accounted for is pieces of software that can record in some way what actions a specific user of a computer has performed. Three rather common examples are screen shot utilities, utilities that make films of the sequence of screens and utilities that record the key strokes a user makes. The e-voting system may not be able to prevent the use of such utilities.

*Standard No. 55. "Any decoding required for the counting …"*

103. The encryption of votes may be necessary to secure the anonymity of voting. In many cases the vote is encrypted before starting the transmission via networks, is held encrypted in the ballot box and is decoded before counting. The counting is carried out with decoded votes, which cannot be related to any voter.

104. However, there are encryption methods that do not require decoding before votes are counted (homomorphic encryption). Counting can then be performed without disclosing the content of encrypted votes. In some cases it may even be necessary for counting to be performed while votes are in the encrypted state, in order to secure anonymity.

Appendix III

## Technical requirements

### Introduction to technical requirements

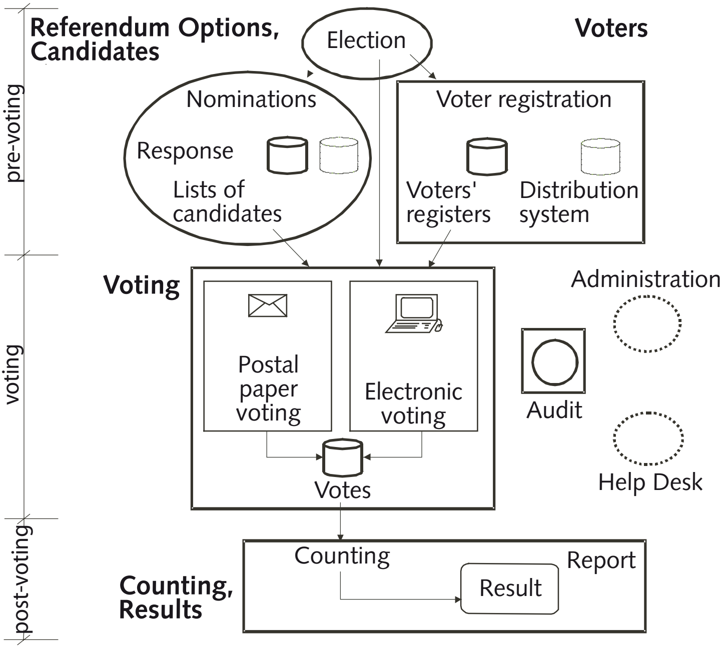
105. Electronic systems can be used to assist one or more of the different stages of an election or referendum. When considering the use of electronic systems for election or referendum purposes, it is necessary to confirm the complete and proper functioning of these systems. To this end, this document provides a set of technical requirements to help those who want to create such a system.

106. It may be that in a given election or referendum, not all stages will be conducted by electronic means. It is therefore important that functionalities are ordered in such a way that the main election or referendum stages are implemented as separate units.

107. Traditionally these main stages, as shown in the following figure, are:

- announcement of election or referendum,
- voter registration,
- candidate nomination and registration, or determination of referendum options,
- voting,
- counting,
- declaration of the result,
- audit.

*Figure 1: EML process model (simplified; from EML v4.0a, Figure 2B)*



108. The elements displayed above are the fundamental elements of an election or referendum system, which should be ordered in a way that makes it easy to associate them with their traditional counterparts. These elements are:

– the voters' register,

– the candidates list or options list (which the voter may choose from),

– the electronic ballot box,

– the counting of results.

109. The technical requirements cover six different areas: accessibility, interoperability, system operation, security, auditing and certification. Each area is detailed in a separate chapter both in the recommendation and in the explanatory memorandum. After the last one, certification, there is a description of a methodology for risk analysis.

### A. Accessibility

*Standard No. 61. "Measures shall be taken to ensure ..."*

110. In order to guarantee accessibility and ease of use of e-election or e-referendum systems, consideration must be given to different user-related constraints linked to age, language, disability and lifestyle.

111. For example, individuals with a visual impairment or with dyslexia may need screen reading devices, sharply contrasting text and backgrounds, as well as the possibility of adjusting the text size in their Web browsers or on voting machines. Users with communication impairments may prefer graphically presented information. Those with co-ordination impairments may prefer using a keyboard rather than a mouse. Kiosks need to be adapted to the needs of mobility impaired users.

112. Voters should be supplied with appropriate instructions, which are easy to understand and follow.

*Standard No. 62. "Users shall be involved in the design of e-voting systems …"*

113. The need for accessibility of e-voting systems means that systems should be designed in such a way that as many voters as possible, and ultimately all voters, can use them.

114. Products and services must be functional, suitably adapted to the age-range and needs of the public, yet without unnecessarily complicated or expensive features that only provide slight benefits.

115. Both these requirements might be achieved with a collaborative approach involving the development team and a users' panel.

*Standard No. 63. "Users shall be supplied, …, with additional facilities …"*

116. The World Wide Web Consortium was created in October 1994 to lead the World Wide Web to its full potential by developing common protocols that promote its evolution and ensure its interoperability. W3C has around 400 member organisations from all over the world and has earned international recognition for its contributions to the growth of the Web. The W3C develops interoperable technologies (specifications, guidelines, software and tools) and is a forum for information, commerce, communication, and collective understanding.

117. To promote a high degree of usability for people with disabilities, the W3C started the Web Accessibility Initiative (WAI). In co-ordination with organisations around the world, the WAI pursues Web accessibility through five main areas of work: technology, guidelines, tools, education and outreach, and research and development. The WAI has already produced a set of standards and guidelines in support of accessibility (for example Web contents accessibility guidelines, authoring tools accessibility guidelines, user agent accessibility guidelines, XML accessibility guidelines, etc.). More information is available from the WAI website: http://www.w3.org/WAI.

*Standard No. 64. "Consideration shall be given, …, to their compatibility with existing …"*

118. It is a constant in system development that a new version may be so different from the previous one that they are incompatible. To avoid such a situation, it might be helpful to create and maintain a list of compatible systems, products and specific equipments. International bodies like OASIS (see Interoperability) may be helpful in this respect.

*Standard No. 65. "The presentation of the voting options shall be optimised for the voter."*

119. Products and services must be adaptable to the users' functional restrictions and specific circumstances without infringing the equality principle. This can be achieved by offering different versions of the same product, changes to key parameters, modular design, ancillaries or other methods.

## B. Interoperability

*Standard No. 66. "Open standards shall be used …"*

120. In order to be able to use e-voting systems or services from different suppliers, these must be interoperable. Interoperability means that the input and output conform to open standards and especially open standards for e-voting.

121. The main benefits of using open standards are:

– greater choice of products and suppliers,

– less dependency on a single supplier,

– avoidance of proprietary lock-in,

– stability or reduction in costs,

– easier accommodation of future changes.

*Standard No. 67. "At present, the Election Markup Language (EML) …"*

122. The Organization for the Advancement of Structured Information Standards (OASIS) set up the Election and Voter Services Technical Committee in the spring of 2001 to develop standards for election and voter services information using XML. Further information about the membership and work of the committee is available at http://www.oasis-open.org/committees/election.

123. The Election Markup Language (EML), the first XML specification of its kind, is at present the only standard for the structured interchange of data among hardware, software, and service providers who engage in any aspect of providing election or voter services. Its function is to ensure open, secure, standardised and interoperable interfaces between the components of election systems. EML is a set of data and message definitions described as XML schemas. It is continually evolving to meet the needs of different voting systems based on experience gained from successive e-elections and e-referendums. The newest available version at the time when the recommendation is adopted is the version that is to serve as a reference to every member state that wants to use EML when implementing an e-voting system. The way this reference will be updated in the future should be defined.

124. Technological developments, unforeseeable at the time of the adoption of the recommendation, may mean that any system valid at that time, including EML, may one day not be the most appropriate system for e-elections or e-referendums, and thus not be used by individual or groups of countries.

*Standard No. 68. "In cases which imply specific election or referendum data requirements …"*

125. As electoral provisions differ between member states, it must be possible to adapt the standard to local needs. EML, being XML-based, provides for a localisation procedure that allows, for instance, additional data or a particular structure. There are several methods of localising XML schemas, for example Schematron. It should be borne in mind that any localisation should not prevent

an equivalent module from another supplier from working in the localised environment.

### C. Systems operation

126. This section refers to equipment, infrastructure and software running in a controlled environment. These include servers, communication devices, kiosk machines and their related operating systems and other pieces of software. This excludes voters' personal devices like PCs, organisers, mobile phones and their related software as well as public network equipment, devices and software.

*Standard No. 69. "The competent electoral authorities shall publish …"*

127. Constant development in information and communication technologies makes it necessary for those in charge of the infrastructure to keep up to date with hardware and software. This calls for recurrent adaptations to central systems and voting facilities used in a controlled environment (for example, voting machines). Any adaptation will need to be certified according to the rules in force in each state before it can be brought into operation.

128. It is essential that electronic voting systems remain as transparent as possible for authorities and citizens alike. Exact, full, up-to-date descriptions of the hardware and software components should be published, thus enabling interested groups to verify for themselves that the systems in use correspond to the ones certified by the competent authorities. The results of certification should be made available to the authorities, political parties and, depending on legal provisions, citizens.

*Standard No. 70. "Those responsible for operating the equipment shall draw up a contingency procedure …"*

*Standard No. 71. "Sufficient backup arrangements shall be in place …"*

*Standard No. 72. "Those responsible for the equipment shall use special procedures to ensure …"*

129. An electronic voting system, more so than any other electronic system in public use, must possess reliability to the highest degree – hence the need to formalise the procedures for dealing with special cases and problems and to provide adequate resources for troubleshooting the infrastructure.

130. The electoral authorities must define a specific service level before running the system. Based on the desired service level, a risk analysis should be made and

scenarios should be established. These will imply procedures, backup arrangements, resources reservation and so on.

*Standard No. 73. "Before each election or referendum, the equipment shall be checked and approved …"*

131. As it is not possible for every member of the electorate to exercise his/her right to transparency of the ballot personally, the competent authorities, the candidates and any observers (where relevant), should be able to have the whole or part of the system inspected by a specialist entity.

132. A clear distinction should be made between checking done on a regular basis after each election or referendum, and the checking done whenever the system is modified in any respect. In the first case, employees of the entity running the election or referendum system might do the checking. However in the second case an external body should do the checking, as the check is closer to being a certification procedure. See the certification section below for more information.

*Standard No. 74. "All technical operations shall be subject to a formal control procedure …"*

133. All work done on hardware or software carries intrinsic technical and human risks, which should be kept to a minimum while an operation is in progress. That is why automatic controls are to be preferred and limits placed on remote manipulations without official supervision. If it is necessary to intervene, these risks (of intrusion, human error, sabotage, etc.) are to be reduced as far as possible. This should be done by establishing a working procedure to be followed and validated, which restricts the number of persons authorised to do the work to a small supervised group and requires the verification of each act through the physical presence of two or more qualified persons. Those persons should comply with the security rules laid down by the competent authority.

134. The electoral authorities must be made aware of all critical changes made on the system in order to anticipate any consequences and choose the appropriate policy to communicate such changes.

*Standard No. 75. "Key e-election or e-referendum equipment shall be located …"*

135. For their safekeeping, it is highly desirable that the central systems be installed in secure, controlled locations. Physical access should be restricted. To be able to react after a physical disaster, an alternative location solution should also be planned, with the appropriate equipment pre-reserved.

136. All election or referendum data that has to be stored should be stored in a secure manner. This means several copies of data will be needed on several types of information support (hard disk, tapes, USB memory key, and printout) and they should be stored in different locations.

*Standard No. 76. "Where incidents that could threaten the integrity of the system occur …"*

137. It is important that any incident be reported to the competent authorities, who are responsible for specifying communication rules in keeping with the applicable legislation and ensuring that political parties and voters are properly informed.

### D. Security

#### Introduction

138. Appropriate security measures are essential prerequisites for e-voting. As with any technical system, an e-voting system may be exposed to errors and deliberate or unintended attempts to circumvent security measures. Attacks need to be prevented and the cardinal principles of universal, equal, free, secret and direct suffrage need to be maintained. Particular attention is to be paid to possible systematic attacks, as these can particularly affect results. In general, e-elections and e-referendums involving the use of e-voting should be as reliable and secure as elections or referendums which do not involve the use of electronic means (see recommendation, paragraph i.).

139. Technical security requirements of the recommendation follow accepted IT security practices and are based on a risk analysis (see F below). The requirements are based on the following criteria:

– technology neutrality: the purpose is to develop the technical security recommendations in a technology neutral approach, and not to restrict solutions to a limited set of technologies or voting channels (for example solely concentrating on the Internet);

– sustainability: the security requirements are to outlast rapid technological changes. This is closely related to technology neutrality;

– methodology: accepted practices and standards are to be followed to develop the security requirements in order to provide confidence in the result;

– versatility: the requirements are applicable to all forms of e-elections and e-referendums, that is voting machines at polling stations, kiosk voting in controlled environments, and remote e-voting in uncontrolled environments;

– EML: the technical security requirements have been based on the Election Markup Language (EML) process model that is a basis of work carried out in the subgroup on core technical standards.

### IT security terms

140. The following IT security terms are frequently used in this section. The definitions have mainly been taken from relevant ISO standards.

| | |
|---|---|
| Access control | The prevention of unauthorised use of a resource (ISO 7498-2:1989) |
| Authentication | The provision of assurance of the claimed identity of an entity (ISO/IEC 10181-2:1996) |
| Availability | The property of being accessible and usable upon demand (TR 13335-1:1996) |
| Confidentiality | The property that information is not made available or disclosed to unauthorised individuals, entities, or processes (ISO 7498-2:1989) (TR 13335-1:1996) |
| Protection profile | An implementation-independent set of security requirements for a category of products that meet specific consumer needs (ISO 15408) |
| User or actor | An entity that is authorised to interact with the e-voting system as a whole or with its components. This includes, *inter alia*, voters, candidates, auditors, etc. |

### I. General requirements

*Standard No. 77. "Technical and organisational measures shall be taken …"*

141. Service level agreements (SLAs) usually lay down availability and failure rates. A certain level of service degradation may be acceptable during failure periods, for example when a server in a cluster breaks. In registration processes even short periods of service disruptions or maintenance periods may be tolerable. The system developers, however, need to consider deliberate denial of service attacks and shall document the contingency reserve in system performance

that has been designated. Independent penetration tests can reduce the probability of successful deliberate service disruption.

142. The services whose availability must be ensured depend on the stage: pre-voting, voting, or post-voting. In the pre-voting stage, nominations, the registration processes and its services are to be available, in the voting stage the voting processes and its services, and in the post-voting stage the counting and reporting processes and its services. Auditing processes need to be available for all stages. The pre-defined limits for SLAs, tolerable failure rates or service degradation may, however, be different for the various stages or services.

*Standard No. 78. "The e-voting system shall maintain the privacy of individuals …"*

143. Depending on national practices there may be further confidentiality requirements with respect to the candidate's decision. In that case those requirements must be met.

*Standard No. 79. "The e-voting system shall perform regular checks …"*

*Standard No. 80. "The e-voting system shall restrict access …"*

*Standard No. 81. "The e-voting system shall protect authentication data …"*

144. The objective refers to all subjects. Services, such as information services for the voter prior to entering the voting process, which clearly do not need authentication, are outside the scope of this document.

*Standard No. 82. "Identification of voters and candidates in a way that they can unmistakably be distinguished …"*

145. Unique identification refers to validating the identity of a specific person by means of one or more features so that the person can unmistakably be distinguished from all other persons. The voters' registers therefore need to provide means to avoid digital twins – that is, persons holding the same identification data. In cases where central voters' registers are used, unique identification may implicitly be given by the entry of the person in the database, while with interconnected voters' registers additional means may be necessary.

146. As someone may be both a voter and a candidate or both an administrator and a voter, it is important to prevent the same person having the same identification in the system for all his or her roles. Authentication can be identity-based or role-based. While identity-based authentication is advisable for voters registering or casting a vote, or candidate nomination, it might be sufficient to have role-based authentication for administrators, auditors and others.

*Standard No. 83. "E-voting systems shall generate reliable and sufficiently detailed observation data …"*

*Standard No. 84. "The e-voting system shall maintain reliable synchronised time sources …"*

147. There may be different accuracy requirements for different consumers of the time source, such as different tolerances for the registration event and casting a vote. This may lead to multiple time sources or a single time source that provides the highest accuracy. The term "time mark" has been used as an indication for marking the data. There are several means depending on the situation. Secure time stamps might be needed for critical events, whereas, for example, continuous sequence numbers or preserving the sequence may be sufficient for log entries. Note that time stamps on votes may jeopardise the confidentiality of the vote, and thus careful consideration should be given as to how and if they should be used in relation to ballots or votes.

*Standard No. 85. " Electoral authorities have overall responsibility …"*

148. The electoral authorities have responsibility for ensuring that the e-voting system is in compliance with the security standards. The notion of an independent body to assess compliance with the security standards covers both independence from the system manufacturer or service provider, and independence from political interference. The former shall provide assurance that the technical security measures are effective and correctly implemented. The latter shall provide confidence that there is no inappropriate political influence in the evaluation of the e-voting system. The independent body may be a governmental organisation, such as an agency in charge of national IT security certification, or the electoral authority itself; or a private or international organisation such as evaluation laboratories or certification bodies, for instance those that are accredited for national or international evaluation schemes such as BS7799/ISO17799, Common Criteria, or ITSEC. Designation of an independent body shall be transparent.

149. If evaluated and certified Common Criteria / ISO 15408 Protection Profiles are developed based on these security recommendations, independent assessment is given under the Common Criteria scheme.

**II. Requirements in pre-voting stages**

*Standard No. 86. "The authenticity, availability and integrity of the voters' registers …"*

150. Data-origin authentication can be provided, for example, by electronic signatures in fully electronic processes. In semi-electronic processes, data-origin

authentication may also employ conventional security measures, such as manual signatures, seals and couriers.

*Standard No. 87. "The fact that candidate nomination and, …"*

151. This can be ensured by, for example, time marks or by confirmation of a trustworthy system.

*Standard No. 88. "The fact that voter registration …"*

152. This can be ensured by, for example, time marks or by confirmation of a trustworthy system.

### III. Requirements in the voting stage

*Standard No. 89. "The integrity of data communicated from the pre-voting stage …"*

153. Depending on the approach followed, the data actually needed in the voting stage may vary. For example, lists of candidates are required in the voting stage if the ballot is dynamically generated in that stage, whereas an alternative is to generate ballots in the pre-voting stage and to communicate the ballots to the voting stage. Therefore, Standard No. 89 does not list the data whose integrity and authenticity are to be retained, but refers generally to "data communicated".

154. The voters' register may not be required if in two-phase models an anonymous voting token is used to establish the right to vote. Note that voters' registers in the polling station might be needed to prevent multiple votes (electronically and on paper-ballot) or where voting is compulsory and thus a list of those who have voted is essential.

*Standard No. 90. "It shall be ensured that the e-voting system presents …"*

155. Aspects to be considered are that fraudulent servers may be introduced, for example faking an official server by tampering with the domain name system (DNS), using a similar domain name to that of the official server, by "man-in-the-middle" attacks, or Trojan horses in the voter's system replacing the original ballot or fading in counterfeit ballots. Electronic signatures applied to the ballot by the electoral authority allow for verification of the ballot. This shall, however, not violate the confidentiality of the vote.

*Standard No. 91. "The fact that a vote has been cast …"*

156. This can be ensured by, for example, time marks or confirmation of a trustworthy system. A time mark attached to the vote may not, however, leave data trails that can reveal the vote.

*Standard No. 92. "Sufficient means shall be provided to ensure …"*

157. In remote voting environments, such as Internet voting, usually the voter or third parties control the environment. There are limited means by which the e-voting system can control whether a secure environment exists. Provision should be made to enable voters to have confidence in the system, such as measures to ensure that genuine software is used, or recommendations on how to protect the system environment.

*Standard No. 93. "Residual information holding the voter's decision …"*

158. During the process of casting a vote, information carrying the voter's decision may be kept in various locations for technical reasons. For example, in Internet voting scenarios using a PC, data carrying the voter's decision may be kept in the PC's memory, the browser cache, the video memory, swap files or temporary files. Depending on the system, other storage locations may need to be considered. The term "residual information" refers to information that remains accessible at the various locations after the vote has been cast and which may reveal the voter's decision. The standard advises the system developers or service providers to design the e-voting system in such a way that this information may be deleted after the vote has been cast. However, technically there may be limited means to ensure this in a remote voting environment. Nevertheless, every measure possible shall be taken to delete such residual information when the vote has been cast.

*Standard No. 94. "The e-voting system shall at first ensure …"*

159. In cases where anonymous voting tokens prove that a voter is eligible to vote, identification of the voter may not be required. Multiple votes under anonymous authentication need to be prevented.

*Standard No. 96. "After the end of the e-voting period, …"*

160. In remote voting scenarios, a higher load on the services might occur in the short period just before close of the poll. This may lead to increased load and delays before a cast vote enters the electronic ballot box. Votes that have been cast in time, however, shall not be discarded as a result of such delays. Thus, a period of grace shall be given in order to overcome overload periods right before the close of the poll. In other words, the processing of the votes must not be shut down immediately with the closing time of the service, if such increased delays are to be expected.

### IV. Requirements in post-voting stages

*Standard No. 97. "The integrity of data communicated during the voting stage …"*

161. Data-origin authentication can be ensured, for example by electronic signatures in fully electronic processes. In semi-electronic processes, data-origin authentication may also employ conventional security measures, such as manual signatures and couriers. Cast votes and any results derived from those votes are the most valuable assets in an election or referendum. Thus, technical measures are preferable in order to protect these assets in transfer.

*Standard No. 98. "The counting process shall accurately count the votes …"*

162. To gain confidence, it is most important that the counting process can be reproduced and that this can be done with a different system from a different source.

*Standard No. 99. "The e-voting system shall maintain the availability and integrity of the electronic ballot box …"*

163. The information kept in the electronic ballot box must be securely saved for as long as this is necessary to permit any recount or legal challenge or for the period after the election required by the electoral process in the member state in question.

## E. Audit

### I. General requirements

*Standard No. 100. "The audit system shall be designed and implemented …"*

*Standard No. 101. "End-to-end auditing of an e-voting system …"*

164. Auditing of the election or referendum processes is the means by which, in particular, the processes used to collect and count the vote can be examined, in order to confirm the authenticity of the result.

165. Auditing of the system operation, resources and communication infrastructure is the means by which trust and confidence can be established in operation of the ICT system(s) used for e-voting. This requires integrity and authenticity of the audit information and trust in the deployed auditing systems.

166. The greatest danger to e-voting systems is if attacks on systems are not detected and the attack affects the result of the vote. This is why independent and extensive security monitoring, auditing, cross-checking and reporting are a critical part of e-voting systems.

167. E-voting systems should therefore have audit facilities for each of the main components (for example vote and count). Audit facilities should be present on different levels of the system: logical, application, technical.

168. Audit facilities on the logical level should report upon the use that is being made of the system.

169. Audit facilities on the application level should give information on the activities that the system supports in order to enable reconstruction of the system's operation.

170. Audit facilities on the technical level should provide information on the activities that the infrastructure that is being used supports. This varies from routine information on, for example, specific load information and system malfunction, to specific information on the signals an intrusion detection system (IDS) gives with regard to possible attacks.

## II. Recording

*Standard No. 102. "The audit system shall be open and comprehensive …"*

171. Audit trails are critical for e-voting systems, so they must be as comprehensive as possible and open to scrutiny by authorised third parties. Audited data shall be provided at various points and levels within an electronic voting system; for example data can be audited at the EML, IT system or communications infrastructure levels.

172. At the EML level there are many standardised open interface points; data flows at these interface points can be easily observed and monitored. Audit systems shall also cover non EML interfaces, for example interfaces within the communications infrastructure, databases and system management functions.

173. There should be procedural requirements specified for the use of audit systems while running election or referendum systems and predetermined procedures for rapid response scenarios.

*Standard No. 103. "The audit system shall record times, events and actions …"*

174. Automated tools and system procedures shall enable the data to be analysed and reported on in a fast and accurate manner, thus enabling rapid corrective action.

175. The audit system shall provide verifiable reports on:

- – cross-checks of data, including EML-based data,
- – system or network attacks,
- – intrusion detection and reporting,

– data manipulation,

– fraud and fraud attempts.

176. The audit system shall maintain records of any attacks on the operation of the election or referendum system or its communications infrastructure. The system shall include a functionality that detects and reports attempts at hacking, intrusion or manipulation. Detection of attacks on the voting system shall be logged, reported and acted on immediately.

177. The audit system shall log all counts and recounts, including all decisions made, actions taken, or exceptions made during the counting process.

### III. Monitoring

*Standard No. 104. "The audit system shall provide the ability to oversee the election …"*

178. The audit system should provide the ability for any observer to monitor the real time progress of the election or referendum without revealing the potential end count/result. For example, observers should be able to see the total number of ballots being cast in real time, so that independent cross-checks can be performed.

*Standard No. 105. "Disclosure of the audit information to unauthorised persons shall be prevented."*

*Standard No. 106. "The audit system shall maintain voter anonymity all times."*

179. Audit systems by their very nature gather a lot of information. However, if too much information is kept, the confidentiality of the vote may be compromised. Clearly, an audit system should maintain voter anonymity at all times, except when specifically required otherwise under domestic legal provisions. In all cases the information gathered by the audit system has to be protected against unauthorised access.

### IV. Verifiability

*Standard No. 107. "The audit system shall provide the ability to cross-check and verify …"*

180. The audit system shall be able to detect voter fraud and provide proof that all counted votes are authentic. All occurrence of attempted voter fraud shall be logged; the audit system logs shall contain data that provides the ability to cross-check credentials giving the right to vote and shall ensure that all counted votes

were cast by a voter with a right to do so and that all authentic votes have been counted as such.

181. The audit system shall include all election or referendum data required by electoral officials to cross reference and account for all cast ballots, thereby verifying the correct operations of the voting system and the legitimacy of the result. A count of ballots is required to match the total votes cast, including valid and invalid votes. The audit system shall give information to facilitate an independent cross-check and verify the correct operation of the e-election or e-referendum system and the accuracy of the result. The audit system shall be able to ensure that no authentic votes are lost and that there are no votes that are unaccounted for.

182. Cross-checking of independent audit information increases the likelihood of detection of hidden attacks on e-voting systems, as the attack has to be hidden in a consistent way on both the e-voting system and the independent audit information.

*Standard No. 108. "The audit system shall provide the ability to verify that an e-election …"*

183. The audit system shall provide the ability for any observer to be able to directly or indirectly observe the election or referendum and verify that the number of votes cast is accurate. This, therefore, requires the system to provide open, standard interfaces with comprehensive observation facilities subject to the needs of confidentiality of the vote.

184. The audit system shall be publicly verifiable. It may be necessary to prove to the public that the principles of democratic elections and referendums have been upheld and that the results are correct.

185. This requires the ability to prove to third parties that the results are a true and accurate representation of the authentic votes cast and meet the legal requirements under which the election or referendum was held.

## V. Other

*Standard No. 109. "The audit system shall be protected against attacks …"*

186. The audit system shall meet the same security requirements specified for the implementation of the e-voting system itself.

187. The audit system shall itself be protected against attacks intended or likely to corrupt, alter or lose records. Detection of any insider or outsider attacks on the audit system shall be reported and acted on immediately.

*Standard No. 110. "Member states shall take adequate steps to ensure that …"*

188. It is not enough simply to protect the information gathered by the audit system against unauthorised access. It is also necessary to take legal and organisational measures to control the persons in charge or having access to the audit system. Accordingly, anyone having access to the audit system should be subject to an accreditation process.

### F. Certification

*Standard No. 111. "Member states shall introduce certification processes …"*

189. Election officials should consider the use of techniques ranging from testing to formal certification in order to ensure, before the election or referendum takes place, that the system does exactly what it is supposed to do.

190. In the future there may be a number of e-voting systems available as well as individual components. It might become very hard for any electoral authority to make sure a particular product is ready to be used, will operate correctly and will produce the right results. A certification process will be very useful in this respect as it should provide evidence as to the effectiveness of the components and thus may reduce the testing required when building a complete system.

*Standard No. 112. "In order to enhance international co-operation …"*

191. Where agencies participate in international organisations that provide mutual recognition arrangements, member states can benefit from their work and hence reduce their costs of testing and certification.

### Risk analysis – methodology

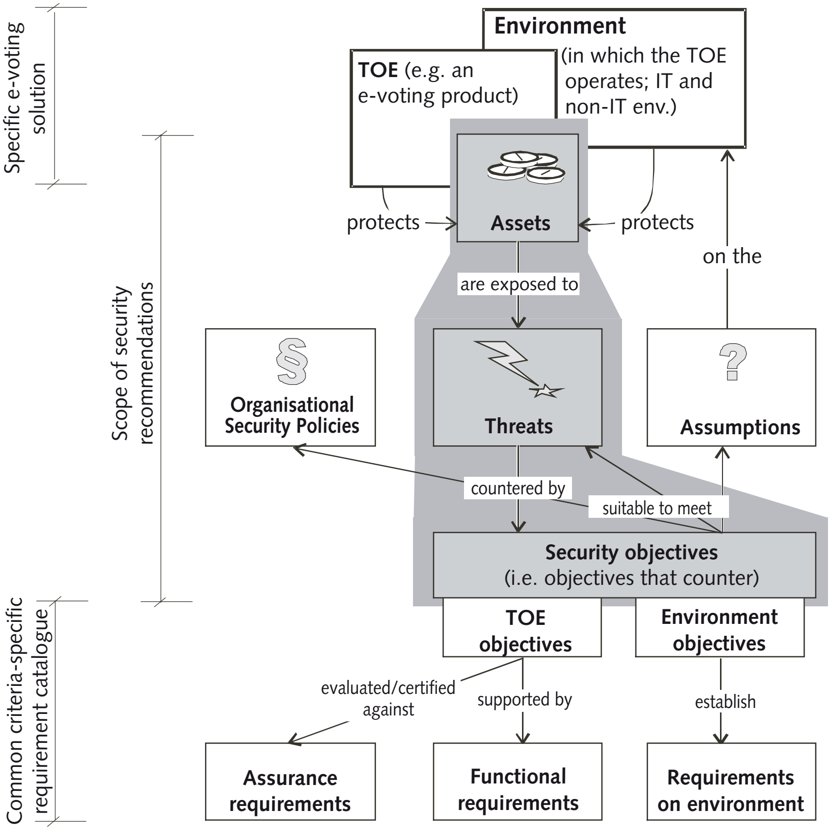
The technical security recommendations have been developed along the Common Criteria CC/ISO 15408. This offers a methodical approach to defining the security objectives in the same way that CC Protection Profiles (PPs) are a means of describing security requirements in a technology neutral manner. Moreover, CC is an IT security product evaluation scheme that is internationally accepted[1] and thus following this standard will enable the security recommendations to be developed into PPs that can be taken up by the industry.

[1] The CC Mutual Recognition Agreement (MRA) has been signed by several Council of Europe member states. As of June 2004, the MRA signatory nations are Austria, Australia, Canada, Finland, France, Germany, Greece, Hungary, Israel, Italy, Japan, the Netherlands, New Zealand, Norway, Spain, Sweden, Turkey, the United Kingdom, and the United States of America.

The document, however, does not represent an actual complete PP, rather it "borrows" from CC by using that methodology to develop the requirements. This serves to demonstrate the completeness and effectiveness of the principles underpinning technical security recommendations. This methodology is explained in the following paragraphs.

Figure 2 below illustrates the CC basics. This shall introduce the ideas used in developing the technical security recommendations to readers unfamiliar with schemes like CC. Those elements actually used in this document are shaded in grey.

*Figure 2: Common Criteria methodology overview and scope of draft security recommendations (shaded grey)*


Specific e-voting solution
Scope of security recommendations
Common criteria-specific requirement catalogue
Environment
(in which the TOE operates; IT and non-IT env.)
TOE (e.g. an e-voting product)
protects
Assets
protects
on the
are exposed to
Organisational Security Policies
Threats
Assumptions
countered by
suitable to meet
Security objectives
(i.e. objectives that counter)
TOE objectives
Environment objectives
evaluated/certified against
supported by
establish
Assurance requirements
Functional requirements
Requirements on environment

The CC defines a security product (for example an e-election system as a whole or a component of it) to be assessed as a target of evaluation (TOE). The TOE together with its environment protects the "assets". By clearly defining the assets the elements needing protection are identified. This forms the basis for a comprehensive threat analysis by examining the assets that are stored or communicated. From these threats, security objectives can be derived and an analysis can be made as to whether the objectives are complete and effectively counter the threats (this approach has been used for developing the technical security recommendations for e-voting).

No organisational policies and related objectives have been defined in the current stage.

The distinction between a product and its environment has not been followed, as this is assumed to be too prescriptive for the purpose of Council of Europe recommendations and related rather to the evaluation of actual products. However, it should be noted that usually not all threats can be countered by technical means – leading to assumptions in CC terms. For example, it seems virtually impossible to avoid family voting in unattended remote voting scenarios by technical means.

Moreover, further elaboration of the security objectives by mapping functional requirements and assurance requirements using the CC catalogues has been omitted.

In summary, the methodology that has been "borrowed" from CC will generate a complete set of security objectives that lead to security recommendations. This document adopts some formal constraints from CC, even though only some underlying basics of CC have been used. This will assist developers to develop actual CC Protection Profiles or Security Targets and thus encourages independent evaluations of products.

### Assets

Given the process model shown in Figure 1 the following assets can be identified:

*General (all stages)*

1. *Authentication data*: information used to verify the claimed identity of a user (authentication data must be maintained in confidentiality).

2. *System integrity*: the authenticity of the e-election system or its components that carry out the intended functions (integrity of the e-election system or its components must be maintained).

3. *Verifiability and observability*: the information used to audit the correct functioning of the e-election or e-referendum system or components of it and information to carry out observation of the election or referendum event (availability and integrity of audit logs and observation information must be maintained).

*Pre-voting stage*

1. *Candidate decision*: the decision to accept/decline a nomination, if provided by domestic law (there might be privacy requirements with respect to the nominee's decision).

2. *List of candidates*: see the main body of the recommendation for a definition of terms (availability and integrity of the list of candidates must be maintained; there might be confidentiality requirements until nominations are accepted or declined).

3. *Voters register*: the list of those eligible to vote at an election or referendum (integrity of the voters' register must be maintained; depending on the domestic legislation there may be confidentiality requirements for privacy reasons).

4. *Nomination process*: the process of nominating candidates, recording the candidate decision, if provided by domestic law, and establishing the lists of candidates (availability of the nomination process must be maintained).

5. *Privacy, data-protection*: the e-election system holds personal data, such as the voters' register or the candidates' decisions. This data may not be disclosed to unauthorised third parties (different domestic legislation may vary between member states as to publication/disclosure of voters' registers).

Application note: one aspect to be considered is the legal requirement of whether the voters' register has to be public (as in the United Kingdom) or not (as in Denmark). However, even if the voters' register is public information, granting unrestricted electronic access has privacy implications (for example a national register of citizens and residences which can be misused). Thus, the means by which public access is granted should be considered.

6. *Registration process*: the process for registration of voters or establishing voters' registers (availability of the registration process must be maintained).

7. *Right to vote*: the voter's right to vote – including any provision preventing multiple voting by one voter (the right to vote must be maintained).

8. *Nomination period*: the period during which nomination can take place (the fact that a nomination has become effective within the eligible time frame shall be ascertainable).

9. *Registration period*: the period during which registration can take place (the fact that a registration has been performed within the eligible timeframe shall be ascertainable).

*Voting stage*

1. *Ballot*: see definitions in the recommendation (the correct ballot must be presented to the voter, the integrity of the ballot must be maintained).

2. *List of candidates* (if required, for example for generating the ballot): communicated from the pre-voting stage (see Pre-voting stage above, see Glossary for the definition)(availability and integrity of the list of candidates must be maintained).

3. *Vote*: see definitions in the recommendations (availability, integrity and confidentiality of the votes must be maintained until the counting process and beyond for recounting purposes).

4. *Voters' registers*: communicated from the pre-voting stage (see Pre-voting stage above); the list of those eligible to vote at an election or referendum (integrity of the voters' register must be maintained; depending on the domestic legislation there may be confidentiality requirements for privacy/data-protection reasons). Regarding application: the voters' register may not be required if in two-phase models an anonymous voting token establishes the right to vote. Note that voters' registers in the polling station might be needed to prevent multiple votes (electronically and on paper-ballot) or where voters are required to vote.

5. *Right to vote*: the voter's right to vote – including any provision preventing multiple voting by one voter (the right to vote must be maintained).

6. *Voting period*: the timeframe in which voting is permitted (the fact that a vote has been cast in the voting period must be ascertainable).

7. *Voter's decision to vote*: the vote entered in the e-election system (the voter's decision must remain a secret when examining a vote or residual data at the election-system; confidentiality and integrity of the voter's choice must be maintained).

Application note: the data to be protected is, as a minimum, the vote. However, further data may be present while making the choice or after the vote has been cast.

8. *Voter's privacy, data protection*: the e-election system holds voters' personal data, such as the voters' register. This data may not be disclosed to unauthorised third parties (confidentiality of the voters' register, different domestic legislation on publication/disclosure of voters' registers may exist).

Application note: one aspect to be considered is the legal requirement of whether the voters' register has to be public (as in the United Kingdom) or not (as in Denmark). However, even if the voters' register is public information, granting unrestricted electronic access has privacy implications (for example a national register of citizens and residences which can be misused). Thus, the means by which public access is granted should be considered.

9. *Casting of a vote*: the process by which an individual casts a vote (availability of the voting process must be maintained).

*Post-voting stage*

1. *List of candidates* (if required, for example for generating the election result or the election report): communicated from the pre-voting stage (see Pre-voting stage above); see definitions in the recommendation (availability and integrity of the list of candidates must be maintained).

2. *Vote*: communicated from the voting stage; see definitions in the recommendation (see Voting stage above). The main assets are the votes (availability, integrity and confidentiality of the votes must be maintained until the counting process and beyond for recounting purposes).

3. *Counting process*: the process of turning votes into the results of an election/referendum (availability of the counting process must be maintained).

4. *Election report*: the report generated by the e-election system (integrity of the report needs to be maintained).

5. *Counting result*: the result of counting votes and the prevention of premature partial results (counting needs to be correct, timely, and integrity of the result must be maintained).

6. *Reporting process*: the process generating an election or referendum report (availability of the reporting process must be maintained).

| Subject | Definition |
|---|---|
| Administrator | A person that performs initialisation, operation or other administrative e-election system functions |
| Auditor | A person, internal or external, responsible for assessing the condition, reliability and security of the e-election system (authenticates as person eligible to access audit logs) |
| Authority | An entity, both a person or process, authorised by the electoral authority(authenticates to initiate election – or referendum – related events, such as initiating an event, generating voters' registers, generating results, etc.) |
| Candidate | A voting option consisting of a person and/or a group of persons and/or a political party |
| Observer | A person authorised to observe an election or a referendum (authenticates as observer) |
| Proposer | A user – an individual, a group, entities such as political parties or an authority – nominating a candidate or candidates (authenticates as user eligible to nominate) |
| Voter | A person who is entitled to cast a vote in a particular election or referendum |
| **Threat agent** | **Definition** |
| Attacker | A human or process, both internal or external, mounting an attack to the e-election system or to parts of it. Also a subject authenticated as such but acting outside its role (internal attack, e.g. an administrator aiming to gain access to the voter's decision) acting outside its role. The main goal of an attacker is to access, modify or insert sensitive information or to disrupt services |
| Malfunction | An external event that disrupts services or internal failure or breakdown of the e-election system or its services |

### Threats

This section describes the threats to the assets. The threats are elaborated for each stage (pre-voting, voting and post-voting), as defined in the EML process model, illustrated in Figure 1, respectively. This gives a certain level of modularity, which allows investigation of the threat analysis for each process stage. General threats that are common to all process stages are given in a separate section. Threats that are common to two process stages are indicated as such.

*General (all stages)*

**T.Audit_Forgery** – *Forgery of audit data*

An attacker generates, modifies, inserts or deletes audit data. This affects verifiability and observability.
Application note: audit is addressed in Appendix III in a specific audit section, and in a specific audit section in this explanatory memorandum, respectively.

**T.Auth_Disclose** – *Disclosure of authentication data*

An attacker gains access to authentication data, enabling the attacker to impersonate a legitimate user (administrator, auditor, authority, candidate, observer, proposer, or voter) of the e-election system.

**T.Hack** – *Hacking of the e-election or e-referendum system*

An attacker, internal or external, interacts with the e-election or e-referendum system, its interfaces or parts of it to exploit vulnerabilities. This may arbitrarily compromise security and affects all assets.
Application note: hacking usually refers to external attackers trying to break into the system. However, an attacker has been defined as internal and external, and an authenticated user such as an administrator acting beyond its legitimate role may also exploit vulnerabilities.

**T.Observ_Forgery** – *Forgery of observation data*

An attacker generates, modifies, inserts or deletes observation information. This affects verifiability and observability.

**T.System_Forgery** – *Forgery of system components*

An attacker replaces the e-election system, or parts of it, with counterfeit elements or presents false components as genuine system parts. This threatens system integrity, but may also result in arbitrary compromise of assets.
Application note: the threat is also vital if in remote e-voting scenarios the attacker redirects the voter to counterfeit systems, such as Internet voting servers that look similar to the original official servers. One example is if the attacker controls the domain name service (DNS) and redirects connections to an official server – for example www.voting.official.at – to a different Internet address. A similar situation can occur if the attacker owns a domain name that is spelled similarly – for example www.voting.oficial.at (note the typo).

*Pre-voting stage*

**T.CandList_Disclose** – *Disclosure of list of candidates information*

An attacker prematurely gains knowledge of the list of candidates, or parts of it, or the candidate's decision.
Application note: there may be different domestic requirements governing whether a candidate's decision may be disclosed.

**T.CandList_Modify** – *Impersonating during candidate nominations*

An attacker impersonates a proposer nominating a candidate. An attacker impersonates a candidate accepting/declining a nomination. An attacker modifies or deletes the list of candidates.

**T.Malfunction_pre** – *Malfunction of systems or services in pre-voting stage*

A malfunction irrecoverably destroys the list of candidates, or the voters' register or the services provided by the nomination process or the registration process. Destruction of the voters' register also affects the right to vote.

**T.Nomin_DOS** – *Denial-of-service against the nomination process*

An attacker disrupts the nomination process or its services; therefore the availability of the process during the nomination period is not ensured. An attacker prevents generation of a list of candidates. Disruption of the service also affects the candidate's ability to make a candidate decision.

**T.Nomin_Time** – *Manipulation of nomination period/time*

An attacker compromises the time source of the nomination process or alters the recorded time when a nomination occurred in such a way that either persons nominated outside the nomination periods are accepted or those nominated within this eligible timeframe are disqualified. This affects the nomination period, the list of candidates, and the timeliness of the candidate's decision.

**T.Privacy** – *Disclosure of personal data*

An attacker reveals voters' or candidates' personal data.
Application note: different domestic legislation on publication/disclosure of voters' registers or candidates' decisions may exist.

**T.Registr_DOS** – *Denial-of-service against the registration process*

An attacker disrupts the registration process or its services; therefore, the availability of the process during the registration period is not ensured. An attacker prevents generation of voters' registers. This also affects the right to vote.

**T.Registr_Time** – *Manipulation of registration period/time*

An attacker compromises the time source of the registration process or alters the recorded time when a registration occurred, in such a way that either those registering outside the registration period are accepted or registrations within this eligible timeframe are disqualified. This affects the time period, the voters' register, and the right to vote.

**T.VotReg_Disclose** – *Disclosure of voters' register information*

An attacker gains knowledge of the voters' register or parts of it.
Application note: there may be different domestic requirements governing which entities have access to the voters' register or whether the voters' register is confidential at all.

**T.VotReg_Modify** – *Impersonating during voter registration*

An attacker impersonates an entity eligible to be registered for voting and registers/de-registers voters. An attacker modifies or deletes the voters' register. This affects the right to vote.

*Voting stage*

**T.Ballot_Forgery** – *Forgery of the ballot or the vote*

An attacker forges the vote carrying the voter's decision or presents a forged ballot to the voter. This affects the vote, as an unintended decision is represented in the vote.

**T.CandList_Modify** *(see Pre-voting stage)*

The threat arises if the list of candidates is required in the voting stage, for example to generate the ballot. If the ballot is generated from a forged or modified list of candidates, the vote and the voter's decision are affected, as a forged ballot is generated (see T.Ballot_Forgery).

**T.CommD_Avail_pre** – *Availability/Integrity of data from pre-voting stage*

An attacker modifies or disrupts data communicated from the pre-voting stages. This results in incorrect or missing lists of candidates or voters' registers in the election or referendum stage. A modified voters' register affects the voter's right to vote.
Refinement: the threat arises if the list of candidates or option list are required in the voting stage, for example to generate the ballot.
Refinement: the threat arises if the ballot is generated from a forged or modified list of candidates. The vote and the voter's decision are affected, as a forged ballot is generated (see T.Ballot_Forgery).
Application note: the voters' register may not be required if in two-phase models an anonymous voting token establishes the right to vote. Note that voters' registers in the polling station may be needed to prevent multiple votes being cast by the same voter (electronically and on paper-ballot) or in case of a requirement that voters must vote.

**T.CommD_Sec_pre** – *Confidentiality of communicated data*

An attacker gains knowledge of communicated voters' registers.
Application note: there may be different domestic requirements governing which entities have access to the voters' register or whether the voters' register is confidential at all.
Application note: the voters' register may not be required if in two-phase models an anonymous voting token establishes the right to vote. Note that voters' registers in the polling station might be needed to prevent multiple votes being cast (electronically and on paper-ballot) or in case of a requirement that voters must vote.

**T.Malfunction_elect** – *Malfunction of systems or services in voting stage*

A malfunction irrecoverably destroys the list of candidates, the voters' register, votes, or the services provided by the voting process. This also affects the voter's right to vote. If the ballot is generated from the modified voters' register, the vote and the voter's decision are affected, as a forged ballot is generated. A malfunction prevents a vote entering the electronic ballot box without the voter being aware or notified of the fact.
Refinement: the threat arises if the list of candidates or option list is required in the voting stage, for example to generate the ballot.
Application note: the voters' register may not be required if in two-phase models an anonymous voting token establishes the right to vote. Note that voters' registers in the polling station might be needed to prevent multiple votes being cast (electronically and on paper-ballot) or in case of a requirement that voters must vote.

**T.Vote_Confidentiality** – *Confidentiality of the voter's decision*

An attacker gains knowledge of a vote. An attacker discovers the identity of the voter from the vote.

**T.Vote_DOS** – *Denial-of-service against the voting process*

An attacker disrupts the voting process or its services; therefore, the availability of the process during the voting period is not ensured. An attacker prevents a voter casting a vote using the e-election system, which affects the voter's right to vote. Denial of service attacks or system overload delay the transmission of the vote and prevent the vote entering the electronic ballot box before the end of the voting period.

**T.Vote_Modify** – *Availability and integrity of votes*

An attacker modifies votes, which results in a vote that does not reflect the voter's decision, or an attacker irrecoverably destroys votes.

**T.Vote_Multiple** – *Impersonating an eligible voter*

An attacker or a voter casts multiple votes via a particular voting channel or by using multiple voting channels. This affects the right to vote, which also covers the provision preventing multiple votes being cast.

**T.Vote_Time** – *Manipulation of voting time/period*

An attacker compromises the time source of the voting process or alters the recorded time when a vote has been cast, such that either a vote cast outside the voting period is accepted or a vote cast within the voting period is disqualified. This affects the right to vote.

**T.Vote_Trail** – *Compromising data trails*

An attacker gains access to data trails that establish a link between a vote and the voter's identity. This compromises the voter's decision.

**T.Voter_Impers** – *Impersonating an eligible voter*

An attacker impersonates an eligible voter. This affects the right to vote, as well as the voter's decision and the vote, as a vote which is different from the intention of the legitimate voter is cast.

**T.Voter_Privacy** – *Disclosure of personal data*

An attacker reals a voter's personal data.
Application note: different domestic legislation on publication/disclosure of voters' registers may exist.

**T.VotReg_Disclose** *(see Pre-voting stage)*

Application note: the voters' register may not be required if in two-phase models an anonymous voting token establishes the right to vote. Note that voters' registers in the polling station might be needed to prevent multiple votes being cast (electronically and on paper-ballot) or in case of a requirement that voters must vote.

**T.VotReg_Modify** *(see Pre-voting stage)*

Application note: the voters' register may not be required if in two-phase models an anonymous voting token establishes the right to vote. Note that voters' registers in the polling station might be needed to prevent multiple votes being cast (electronically and on paper-ballot) or in case of a requirement that voters must vote.

*Post-voting stage*

**T.CommD_Avail_elec** – *Availability/Integrity of data from voting stage*

An attacker modifies or disrupts data communicated from the voting stages. This results in incorrect or missing votes – thus an incorrect result – or incorrect or missing lists of candidates.

Application note: the list of candidates or options may be required to generate the result or the election or referendum report.

**T.CommD_Sec_elec** – *Confidentiality of communicated data from voting stage*

An attacker gains knowledge of communicated votes.

**T.Count_DOS** – *Denial-of-service against the counting process*

An attacker disrupts the counting process or its services, thus the availability of the counting result is not ensured.

**T.Malfunction_post** – *Malfunction of systems or services in the post-voting stage*

A malfunction irrecoverably destroys votes, disrupts the counting process or leads to errors in the counting process which affects the result. A malfunction disrupts the ability to generate an election or referendum report or irrecoverably destroys the report.

**T.MisCount** – *Incorrect counting*

An attacker interferes with the counting process, which leads to incorrect results.

**T.Partial_Count** – *Partial counting*

An attacker initiates counting of disaggregated sub-sets of the votes which may reveal the vote on the basis of data trails.

**T.Premature_Count** – *Premature counting or disclosure of partial results*

An attacker initiates counting before the desired time and gains access to partial or premature results. Partial results also affect the confidentiality of votes on the basis of data trails.

**T.Report_DOS** – *Denial-of-service against the reporting process*

An attacker disrupts the reporting process or its services; therefore, the availability of the election or referendum report is not ensured.

**T.Report_Modify** – *Modification of the election or referendum report*

An attacker modifies the election or referendum report.

**T.Result_Modify** – *Modification of the result*

An attacker modifies the result.

**T.Vote_Confidentiality** *(see Voting stage)*

**T.Vote_Duplicates** – *Modification of the result*

An attacker or a malfunction generates duplicates of votes that cannot be detected as such, which affects the result.

**T.Vote_Modify** *(see Voting stage)*

**T.Vote_Trail** *(see Voting stage)*

The following Tables 1 to 3 give an overview of which threat affects which asset in each of the process stages. Assets and threats that appear in several process stages (besides the general assets/threats) are marked *.

*Table 1: Assets and threats in the pre-voting stage*

| Assets / Threats | | General | | | Pre-voting stage | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Authentication data | Verifiab./Observab. | System integrity | Candidate decision | List of candidates* | Voters' register* | Nomination process | Nomination period | Privacy* | Registration process | Registration period | Right to vote* |
| General | T.Audit_Forgery | | X | | | | | | | | | | |
| | T.Auth_Disclose | X | | | | | | | | | | | |
| | T.Hack | X | X | X | X | X | X | X | X | X | X | X | X |
| | T.Observ_Forgery | | X | | | | | | | | | | |
| | T.System_Forgery | X | X | X | X | X | X | X | X | X | X | X | X |
| Pre-voting stage | T.CandList_Disclose | | | | X | X | | | | X | | | |
| | T.CandList_Modify * | | | | X | X | | | | | | | |
| | T.Malfunction_pre | | | | | X | X | X | | | X | | X |
| | T.Nomin_DOS | | | | X | X | | X | | | | | |
| | T.Nomin_Time | | | | X | X | | | X | | | | |
| | T.Privacy | | | | X | X | X | | | X | | | |
| | T.Registr_DOS | | | | | | X | | | | X | | X |
| | T.Registr_Time | | | | | | X | | | | | X | |
| | T.VotReg_Disclose * | | | | | | X | | | X | | | |
| | T.VotReg_Modify * | | | | | | X | | | | | | X |

*Table 2: Assets and threats in the voting stage*

| Threats | Assets | General | | | Voting stage | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Authentication data | Verifiab./Observab. | System integrity | Ballot | List of candidates* | Voters' register* | Right to vote* | Vote* | Voter's decision* | Voter's privacy | Voting period | Casting of a vote |
| | T.Audit_Forgery | | X | | | | | | | | | | |
| | T.Auth_Disclose | X | | | | | | | | | | | |
| | T.Hack | X | X | X | X | X | X | X | X | X | X | X | X |
| | T.Observ_Forgery | | X | | | | | | | | | | |
| | T.System_Forgery | X | X | X | X | X | X | X | X | X | X | X | X |
| General | T.Ballot_Forgery | | | | X | | | | X | X | | | |
| | T.CandList_Modify * | | | | X | X | | | X | X | | | |
| | T.CommD_Avail_pre | | | | | X | X | X | | | | | |
| | T.CommD_Sec_pre | | | | | | X | | | | | | |
| | T.Malfunction_elect | | | | X | X | X | X | X | X | | | X |
| | T.Vote_Confidentiality* | | | | | | | | X | X | | | |
| | T.Vote_DOS | | | | | | | X | | | | | X |
| | T.Vote_Modify * | | | | | | | | X | X | | | |
| Voting stage | T.Vote_Multiple | | | | | | | X | | | | | |
| | T.Vote_Time | | | | | | | X | | | | X | |
| | T.Vote_Trail * | | | | | | | | | X | | | |
| | T.Voter_Impers | | | | | | | X | X | X | | | |
| | T.Voter_Privacy | | | | | | X | | | | X | | |
| | T.VotReg_Disclose * | | | | | | X | | | | X | | |
| | T.VotReg_Modify * | | | | | | X | X | | | | | |

*Table 3: Assets and threats in the post-voting stage*

| **Assets**<br>**Threats** | | General | | | Post-voting stage | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Authentication data | Verifiab./Observab. | System integrity | List of candidates* | Counting process | Counting result | Election report | Vote | Reporting process |
| | T.Audit_Forgery | | X | | | | | | | |
| | T.Auth_Disclose | X | | | | | | | | |
| | T.Hack | X | X | X | X | X | X | X | X | X |
| | T.Observ_Forgery | | X | | | | | | | |
| | T.System_Forgery | X | X | X | X | X | X | X | X | X |
| General | T.CommD_Avail_elec | | | | X | | X | | X | |
| | T.CommD_Sec_elec | | | | | | | | X | |
| | T.Count_DOS | | | | | X | X | | | |
| | T.Malfunction_Post | | | | | X | X | X | X | |
| | T.MisCount | | | | | | X | | | |
| | T.Partial_Count | | | | | | | | X | X |
| Post-voting stage | T.Premature_Count | | | | | | X | | X | X |
| | T.Report_DOS | | | | | | | X | | |
| | T.Report_Modify | | | | | | | X | | |
| | T.Result_Modify | | | | | | X | | | |
| | T.Vote_Confidentiality* | | | | | | | | X | X |
| | T.Vote_Duplicates | | | | | | X | | X | |
| | T.Vote_Modify * | | | | | | X | | X | |
| | T.Vote_Trail * | | | | | | | | X | X |

**Security objectives**

This section identifies and defines the security objectives for e-voting. The objectives reflect the stated intent and counter the identified threats. The security objectives given in this section represent the security requirements that are listed under “Security” in Appendix III.

*General objectives*

**O.Access_Cntrl** – *Access control*

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

**O.Assessment** – *Independent assessment*

Election authorities have overall responsibility for compliance with these security requirements which shall be assessed by independent bodies.
Application note: in case evaluated and certified CC/ISO 15408 Protection Profiles are developed based on these security recommendations, independent assessment is given under the CC scheme.

**O.Auth_User** – *User authentication*

The e-voting system shall protect authentication data so that unauthorised entities cannot misuse, intercept, modify, or otherwise gain knowledge of authentication data or part of it. In uncontrolled environments, authentication based on cryptographic mechanisms is advisable.
Application note: the objective refers to all subjects. Services such as information services for the voter prior to entering the voting process, which clearly do not need authentication, are outside the scope of this document.

**O.Avail** – *Availability of the e-election processes*

Technical and organisational measures shall be taken to ensure that no data will be permanently lost in the event of a breakdown or a fault affecting the e-voting system. The e-voting system shall contain measures to preserve the availability of its services during the e-voting process. It shall resist, in particular, malfunction, breakdowns or denial of service attacks.
Application note: service level agreements (SLAs) usually lay down availability and failure rates. A certain level of service degradation may be acceptable during failure periods, for example when a server in a cluster breaks. In registration processes short periods of service disruptions or maintenance periods may be tolerable. The system developer, however, needs to consider deliberate denial of service attacks and shall document the contingency reserve in system performance that has been designated. Independent penetration tests can reduce the probability of successful deliberate service disruption.
Refinement: the services to be preserved in availability depend on the stage –

pre-voting, voting, post-voting. In the pre-voting stage, the nomination and the registration processes and its services are to be available; in the voting stage the voting processes and its services; and in the post-voting stage the counting and reporting processes and its services. Auditing processes need to be available in all stages. The pre-defined limits for SLAs, tolerable failure rates, or service degradation may, however, be different for the various stages or services.

**O.Ident_User** – *Identity-based user authentication*

Identification of voters and candidates in a way that they can unmistakably be distinguished from other persons (unique identification) shall be ensured.
Application note: authentication can be identity-based or role-based. While identity-based authentication is advisable for voters registering or casting a vote, or candidates accepting/declining a nomination, it might be sufficient to have role-based authentication for administrators, auditors, etc.

**O.Observation_Data** – *Observation data*

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

**O.Privacy** – *Privacy of voters and candidates*

The e-voting system shall maintain the privacy of individuals. Confidentiality of voters' registers stored in or communicated by the e-voting system shall be maintained.
Refinement: when stored in or communicated to uncontrolled environments, the voters' registers should be sealed.
Application note: depending on domestic practices, there might be further confidentiality requirements with respect to the candidate's decision. In that case confidentiality is required.

**O.Reliable_Time** – *Reliable time source*

The e-voting system shall maintain reliable synchronised time sources. The accuracy of the time source shall be sufficient to maintain time marks for audit trails and observation data, as well as for maintaining the time limits for registration, nomination, voting, or counting.
Application note: there may be different accuracy requirements for different consumers of the time source, such as different tolerances for the registration event and casting a vote. This may lead to multiple time sources or a single time source that provides the highest accuracy. The term "time mark" has been used as an indication for marking the data. There are several means depending on the situation: secure time stamps might be needed for critical events, whereas continuous sequence numbers, or preserving the sequence, for example, may be sufficient for log entries. Note that exact time stamps on votes may also jeopardise the confidentiality of the voter's decision.

**O.Secure_Oper** – *Secure operation and system integrity*

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

*Pre-voting stage*

**O.Data_Sec** – *Availability and integrity of the election or referendum, options, lists of candidates*

The authenticity, availability and integrity of the voters' registers and lists of candidates shall be maintained. The source of the data shall be authenticated. Provisions on data protection shall be taken into account.
Refinement: depending on domestic requirements, practice with respect to confidentiality/publication of candidate's decision or the voters' register may differ.
Application note: data-origin authentication can be provided by, for example, electronic signatures in fully electronic processes. In semi-electronic processes, data-origin authentication may also employ conventional security measures, such as manual signatures, seals and couriers.

**O.Time_Nominate** – *Timely nomination*

The fact that candidate nomination and, if required, the decision of the candidate and/or the competent electoral authority to accept a nomination has happened within the prescribed time limits shall be ascertainable.
Application note: this can be provided by, for example, time marks or a confirmation of a trustworthy system.

**O.Time_Register** – *Timely registration*

The fact that voter registration has happened within the prescribed time limits shall be ascertainable.
Application note: this can be provided by, for example, time marks or a confirmation of a trustworthy system.

*Voting stage*

**O.Authentic_Vote** – *Ensure authentic vote*

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

**O.Ballot_Correct** – *Present an authentic ballot*

It shall be ensured that the e-voting system presents an authentic ballot to the voter. In the case of remote e-voting, the voter shall be informed about the means to verify that a connection to the official server has been established and the authentic ballot been presented.
Application note: aspects to be considered are that counterfeit servers may be given, such as: faking an official server by tampering the domain name system

(DNS); using a similar domain name to that of the official server; "man-in-the-middle" attacks; or Trojan horses on the voter's system replacing the original ballot or introducing counterfeit ballots. Electronic signatures applied to the ballot by the electoral authority enable the ballot to be verified. This must, however, not violate the confidentiality of the voter's decision. Therefore, the data used to prove an authentic ballot shall not lead to uniquely identifiable ballots, nor shall such unique data be removed when the voter casts the vote.

**O.Delayed_Vote** – *Accept delayed votes*

After the end of the e-voting period, no voters shall be allowed to gain access to the e-voting system. However, the acceptance of electronic votes into the electronic ballot box shall remain open for a sufficient period of time to allow for any delays in the passing of messages over the e-voting channel.
Application note: in remote voting scenarios, there may be a higher load on the services in the short period right before closing the poll. This may lead to increased load and increased delays until a cast vote enters the electronic ballot box. Votes that have been cast in time, however, shall be accepted. Thus, the server shall not be shut down immediately at the closing time of the service, if such increased delays are to be expected.

**O.Sec_Transfer_pre** – *Secure transfer of communicated data*

Data communicated from the pre-voting stage (for example voters' registers and lists of candidates) shall be maintained in their integrity. Data-origin authentication shall be carried out.
Refinement: lists of candidates are required in the voting stage, if the ballot is generated in the election stage.
Refinement: the voters' register may not be required if in two-phase models an anonymous voting token establishes the right to vote. Note that voters' registers in the polling station might be needed to prevent multiple votes being cast (electronically and on paper-ballot) or in case of a requirement that voters must vote.
Application note: data-origin authentication can be provided, for example, by electronic signatures in fully electronic processes. In semi-electronic processes, data-origin authentication may also employ conventional security measures, such as manual signatures, seals and couriers.

**O.System_Secure** – *Secure voting system*

Sufficient means shall be provided to ensure that the systems used by the voters to cast the vote can be protected against influence that can modify the vote.
Refinement: in unattended remote voting environments, such as Internet voting, usually the voter or third parties control the environment. There are limited means by which the election or referendum system can control whether a secure environment exists. Means that allow the voters to gain confidence in the system must be provided, such as means to ensure that genuine software is used, or recommendations on how to protect the system environment.

**O.Residual_Info** – *Destroy residual information*

Residual information holding the voter's decision or the display of the voter's choice shall be destroyed when the vote has been cast. In the case of remote e-voting, the voter shall be provided with information on how to delete, where that is possible, from the device used to cast the vote.
Application note: residual information may be given in the cache of Internet browsers, data swapped to disks, temporary files, etc. There are some means to develop Internet applications in such a way that certain types of residual information can be avoided. However, the effectiveness of such measures is dependent on the application used by the voter, and its configuration. In remote voting environments, such as Internet voting, usually the voter or third parties control the environment. There are limited means by which the e-election system can control whether a secure environment exists. Means that allow the voters to gain confidence in the system may be provided, such as means to ensure that genuine software is used, or recommendations on how to protect the system environment.

**O.Time_Vote** – *Timely casting of a vote*

The fact that a vote has been cast within the prescribed time limits shall be ascertainable.
Application note: this can be provided by, for example, time stamps or a confirmation of a trustworthy system. A time-stamp attached to the cast vote, however, may not leave data trails that can reveal the voter's decision (see O.Vote_Confidentiality).

**O.Vote_Confidentiality** – *Confidentiality of a voter*

Votes and voter information shall remain sealed as long as the data is held in a manner where they can be associated. Authentication information shall be separated from the voter's decision at a pre-defined stage in the e-election or e-referendum.
Note: this objective gives rise to technical requirements. It is, however, represented in the "Reliability and security" legal standard 35.

**O.Vote_Secure** – *Availability, confidentiality and integrity of cast votes*

The e-voting system shall maintain the availability and integrity of the votes. It shall also maintain the confidentiality of the votes and keep them sealed until the counting process. If stored or communicated outside controlled environments, the votes shall be encrypted.
Note: this objective gives rise to technical requirements. It is also, however, represented in the "Reliability and security" legal standard 34.
Application note: encryption is the technology of choice to seal a vote, particularly in remote voting scenarios or when cast votes are transmitted via public channels. For voting machines in polling stations physical protection may also serve to seal a vote. The explanation for sealing (see recommendation)

distinguishes between encryption and, for example, closed channels. In uncontrolled environments the highest level of security measures is required in order to protect the votes, which are the primary asset of an e-election, and the confidentiality of the choice made by voters, which is probably their main concern. Accordingly, this requirement explicitly calls for encryption.

**O.Voter_Eligible** – *Authentication of a voter eligible to cast a vote*

The e-voting system shall at first ensure that a user who tries to vote is eligible to vote. The e-voting system shall authenticate the voter and shall ensure that only the appropriate number of votes per voter is cast and stored in the electronic ballot box.
Refinement: in cases where anonymous voting tokens are used to prove that a voter is eligible to vote, authentication of the voter may not be required. However, even in such cases it is still necessary to ensure that the casting of multiple votes is prevented.

*Post-voting stage*

**O.Count_Correct** – *Correctness and reproducibility of the counting result*

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

**O.Result_Secure** – *Availability and integrity of ballot box and result*

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

**O.Sec_Transfer_vote** – *Secure transmission of communicated data*

The integrity of data communicated from the voting stage (for example votes, voters' registers, lists of candidates) shall be maintained. Data-origin authentication shall be carried out.
Application note: data-origin authentication can be provided by, for example, electronic signatures in fully electronic processes. In semi-electronic processes, data-origin authentication may also employ conventional security measures, such as manual signatures and couriers. Cast votes or partially counted results are, however, the most valuable asset in an election or referendum. Thus, it is preferable to provide technical measures to protect these assets during the transmission.

**O.Vote_Confidentiality** – *see Voting stage*

**O.Vote_Secure** – *see Voting stage*

The following Tables 4 to 7 map the objectives to the threats that are countered. Threats that appear in several process stages (besides the general assets/threats) are marked *.

*Table 4: Mapping of objectives to threats. General objectives – all stages*

| | Objectives<br>Threats | O.Access_Cnrtl | O.Assessment | O.Auth_User | O. Avail | O.Ident_User | O.Observation_Data | O.Privacy | O.Reliable_Time | O.Secure_Oper |
|---|---|---|---|---|---|---|---|---|---|---|
| General | T.Audit_Forgery | X | Independent assessment does not directly counter threats, but provides confidence in the correctness. In other words, threats are indirectly countered. | X | | | | | X | |
| | T.Auth_Disclose | X | | X | | | | | | |
| | T.Hack | X | | X | X | | | | | X |
| | T.Observ_Forgery | X | | X | | | X | | X | |
| | T.System_Forgery | X | | X | | | X | | | X |
| Pre-voting stage | T.CandList_Disclose | X | | X | | | Observation assists in correct operation of the election event. In other words, indirectly counters threats. | X | | |
| | T.CandList_Modify * | X | | X | X | | | | | |
| | T.Malfunction_pre | | | | X | | | | | X |
| | T.Nomin_DOS | | | | X | | | | | X |
| | T.Nomin_Time | X | | X | | | | | X | |
| | T.Privacy | X | | X | | X | | X | | |
| | T.Registr_DOS | | | | X | | | | | X |
| | T.Registr_Time | X | | X | | | | | X | |
| | T.VotReg_Disclose * | X | | X | | | | X | | |
| | T.VotReg_Modify * | X | | X | X | X | | | | |
| Voting stage | T.Ballot_Forgery | | | | | | | | | X |
| | T.CandList_Modify * | X | | X | | | | | | |
| | T.CommD_Avail_pre | X | | X | X | | | | | |
| | T.CommD_Sec_pre | X | | X | | | | X | | |
| | T.Malfunction_elect | | | | X | | | | | X |
| | T.Vote_Confidentiality* | | | | | | | | | |
| | T.Vote_DOS | | | | X | | | | | X |
| | T.Vote_Modify * | X | | X | | | | | | |
| | T.Vote_Multiple | | | | | X | | | | |
| | T.Vote_Time | X | | X | | | | | X | |
| | T.Vote_Trail * | | | | | | | | | |
| | T.Voter_Impers | X | | X | | X | | | | |
| | T.Voter_Privacy | X | | X | | | | X | | |
| | T.VotReg_Disclose * | X | | X | | | | X | | |
| | T.VotReg_Modify * | X | | X | | | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Post-voting stage | T.CommD_Avail_elec | X | | X | | | | | | |
| | T.CommD_Sec_elec | X | | X | | | | | | |
| | T.Count_DOS | | | | X | | | | | X |
| | T.Malfunction_Post | | | | X | | | | | X |
| | T.MisCount | | | | | | | | | |
| | T.Partial_Count | X | | X | | | | | | |
| | T.Premature_Count | X | | X | | | | | X | |
| | T.Report_DOS | | | | X | | | | | X |
| | T.Report_Modify | X | | X | | | | | | |
| | T.Result_Modify | X | | X | | | | | | |
| | T.Vote_Confidentiality* | | | | | | | | | |
| | T.Vote_Duplicates | | | | | | | | | |
| | T.Vote_Modify * | X | | X | | | | | | |
| | T.Vote_Trail * | | | | | | | | | |

*Table 5: Mapping of objectives to threats. Pre-voting stage*

| **Objectives** / **Threats** | | General | Pre-voting stage | | |
|---|---|---|---|---|---|
| | | | O.Data_Sec * | O.Time_Nominate | O.Time_Register |
| General | T.Audit_Forgery | See Table 4 | | | |
| | T.Auth_Disclose | | | | |
| | T.Hack | | | | |
| | T.Observ_Forgery | | | | |
| | T.System_Forgery | | | | |
| Pre-voting stage | T.CandList_Disclose | See Table 4 | X | | |
| | T.CandList_Modify* | | X | | X |
| | T.Malfunction_pre | | | | |
| | T.Nomin_DOS | | | | |
| | T.Nomin_Time | | | X | |
| | T.Privacy | | X | | |
| | T.Registr_DOS | | | | |
| | T.Registr_Time | | | | X |
| | T.VotReg_Disclose * | | X | | |
| | T.VotReg_Modify* | | X | X | |

*Table 6: Mapping of objectives to threats. Voting stage*

| Objectives / Threats | | General | Voting stage | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | O.Authentic_Vote | O.Ballot_Correct | O.Delayed_Vote* | O.Residual | O.Sec_Transfer_pre | O.System_Secure | O.Time_Vote | O.Vote_Confidentiality | O.Vote_Secure | O.Voter_Eligible |
| General | T.Audit_Forgery | see Table 4 | | | | | | | | | | |
| | T.Auth_Disclose | | | | | | | X | | | | |
| | T.Hack | | | | | | | X | | | | |
| | T.Observ_Forgery | | | | | | | | | | | |
| | T.System_Forgery | | | | | | | X | | | | |
| Voting stage | T.Ballot_Forgery | see Table 4 | X | X | | | X | X | | | | |
| | T.CandList_Modify * | | | | | | X | | | | | |
| | T.CommD_Avail_pre | | | | | | X | | | | | |
| | T.CommD_Sec_pre | | | | | | X | | | | | |
| | T.Malfunction_elect | | X | | | | | X | | | | |
| | T.Vote_Confidentiality* | | X | | | X | | X | | X | X | |
| | T.Vote_DOS | | X | | X | | | | X | | | |
| | T.Vote_Modify * | | X | X | | | | X | X | | X | |
| | T.Vote_Multiple | | | | | | | | | | | X |
| | T.Vote_Time | | | | | | | | X | | | |
| | T.Vote_Trail * | | | | | X | | | X | X | | |
| | T.Voter_Impers | | | | | | | X | | | | X |
| | T.Voter_Privacy | | | | | | | | | X | X | |
| | T.VotReg_Disclose * | | | | | | X | | | | | |
| | T.VotReg_Modify * | | | | | | X | | | | | |

*Table 7: Mapping of objectives to threats. Post-voting stage*

| **Objectives** / **Threats** | | General | Post-voting stage | | | | |
|---|---|---|---|---|---|---|---|
| | | | O.Count_Correct | O.Result_Secure | O.Sec_Transfer_vote | O.Vote_Confidentiality | O.Vote_Secure |
| General | T.Audit_Forgery | see Table 4 | | | | | |
| | T.Auth_Disclose | | | | | | |
| | T.Hack | | | | | | |
| | T.Observ_Forgery | | | | | | |
| | T.System_Forgery | | | | | | |
| post-voting stage | T.CommD_Avail_elec | see Table 4 | | | X | | |
| | T.CommD_Sec_elec | | | | X | | |
| | T.Count_DOS | | | | | | |
| | T.Malfunction_Post | | | | | | |
| | T.MisCount | | X | | | | |
| | T.Partial_Count | | | X | | X | |
| | T.Premature_Count | | | | | | |
| | T.Report_DOS | | | | | | |
| | T.Report_Modify | | | | X | | |
| | T.Result_Modify | | | X | X | | |
| | T.Vote_Confidentiality* | | | | | X | X |
| | T.Vote_Duplicates | | X | | | | |
| | T.Vote_Modify * | | | | | | X |
| | T.Vote_Trail * | | | | | X | |

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

**BELGIUM/BELGIQUE**
La Librairie européenne SA
50, avenue A. Jonnart
B-1200 BRUXELLES 20
Tel.: (32) 2 734 0281
Fax: (32) 2 735 0860
E-mail: info@libeurop.be
http://www.libeurop.be

Jean de Lannoy
202, avenue du Roi
B-1190 BRUXELLES
Tel.: (32) 2 538 4308
Fax: (32) 2 538 0841
E-mail: jean.de.lannoy@euronet.be
http://www.jean-de-lannoy.be

**CANADA**
Renouf Publishing Company Limited
5369 Chemin Canotek Road
CDN-OTTAWA, Ontario, K1J 9J3
Tel.: (1) 613 745 2665
Fax: (1) 613 745 7660
E-mail: order.dept@renoufbooks.com
http://www.renoufbooks.com

**CZECH REPUBLIC/**
**RÉPUBLIQUE TCHÈQUE**
Suweco Cz Dovoz Tisku Praha
Ceskomoravska 21
CZ-18021 PRAHA 9
Tel.: (420) 2 660 35 364
Fax: (420) 2 683 30 42
E-mail: import@suweco.cz

**DENMARK/DANEMARK**
GAD Direct
Fiolstaede 31-33
DK-1171 COPENHAGEN K
Tel.: (45) 33 13 72 33
Fax: (45) 33 12 54 94
E-mail: info@gaddirect.dk

**FINLAND/FINLANDE**
Akateeminen Kirjakauppa
Keskuskatu 1, PO Box 218
FIN-00381 HELSINKI
Tel.: (358) 9 121 41
Fax: (358) 9 121 4450
E-mail: akatilaus@stockmann.fi
http://www.akatilaus.akateeminen.com

**FRANCE**
La Documentation française
(Diffusion/Vente France entière)
124, rue H. Barbusse
F-93308 AUBERVILLIERS Cedex
Tel.: (33) 01 40 15 70 00
Fax: (33) 01 40 15 68 00
E-mail: commandes.vel@ladocfrancaise.gouv.fr
http://www.ladocfrancaise.gouv.fr

Librairie Kléber (Vente Strasbourg)
Palais de l'Europe
F-67075 STRASBOURG Cedex
Fax: (33) 03 88 52 91 21
E-mail: librairie.kleber@coe.int

**GERMANY/ALLEMAGNE**
**AUSTRIA/AUTRICHE**
UNO Verlag
Aujust Bebel Allee 6
D-53175 BONN
Tel.: (49) 2 28 94 90 20
Fax: (49) 2 28 94 90 222
E-mail: bestellung@uno-verlag.de
http://www.uno-verlag.de

**GREECE/GRÈCE**
Librairie Kauffmann
28, rue Stadiou
GR-ATHINAI 10564
Tel.: (30) 1 32 22 160
Fax: (30) 1 32 30 320
E-mail: ord@otenet.gr

**HUNGARY/HONGRIE**
Euro Info Service
Hungexpo Europa Kozpont ter 1
H-1101 BUDAPEST
Tel.: (361) 264 8270
Fax: (361) 264 8271
E-mail: euroinfo@euroinfo.hu
http://www.euroinfo.hu

**ITALY/ITALIE**
Libreria Commissionaria Sansoni
Via Duca di Calabria 1/1, CP 552
I-50125 FIRENZE
Tel.: (39) 556 4831
Fax: (39) 556 41257
E-mail: licosa@licosa.com
http://www.licosa.com

**NETHERLANDS/PAYS-BAS**
De Lindeboom Internationale Publikaties
PO Box 202, MA de Ruyterstraat 20 A
NL-7480 AE HAAKSBERGEN
Tel.: (31) 53 574 0004
Fax: (31) 53 572 9296
E-mail: books@delindeboom.com
http://home-1-worldonline.nl/~lindeboo/

**NORWAY/NORVÈGE**
Akademika, A/S Universitetsbokhandel
PO Box 84, Blindern
N-0314 OSLO
Tel.: (47) 22 85 30 30
Fax: (47) 23 12 24 20

**POLAND/POLOGNE**
Głowna Księgarnia Naukowa
im. B. Prusa
Krakowskie Przedmiescie 7
PL-00-068 WARSZAWA
Tel.: (48) 29 22 66
Fax: (48) 22 26 64 49
E-mail: inter@internews.com.pl
http://www.internews.com.pl

**PORTUGAL**
Livraria Portugal
Rua do Carmo, 70
P-1200 LISBOA
Tel.: (351) 13 47 49 82
Fax: (351) 13 47 02 64
E-mail: liv.portugal@mail.telepac.pt

**SPAIN/ESPAGNE**
Mundi-Prensa Libros SA
Castelló 37
E-28001 MADRID
Tel.: (34) 914 36 37 00
Fax: (34) 915 75 39 98
E-mail: libreria@mundiprensa.es
http://www.mundiprensa.com

**SWITZERLAND/SUISSE**
Adeco – Van Diermen
Chemin du Lacuez 41
CH-1807 BLONAY
Tel.: (41) 21 943 26 73
Fax: (41) 21 943 36 05
E-mail: info@adeco.org

**UNITED KINGDOM/ROYAUME-UNI**
TSO (formerly HMSO)
51 Nine Elms Lane
GB-LONDON SW8 5DR
Tel.: (44) 207 873 8372
Fax: (44) 207 873 8200
E-mail: customer.services@theso.co.uk
http://www.the-stationery-office.co.uk
http://www.itsofficial.net

**UNITED STATES and CANADA/**
**ÉTATS-UNIS et CANADA**
Manhattan Publishing Company
2036 Albany Post Road
CROTON-ON-HUDSON,
NY 10520, USA
Tel.: (1) 914 271 5194
Fax: (1) 914 271 5856
E-mail: Info@manhattanpublishing.com
http://www.manhattanpublishing.com

**Council of Europe Publishing/Editions du Conseil de l'Europe**
F-67075 Strasbourg Cedex
Tel.: (33) 03 88 41 25 81 – Fax: (33) 03 88 41 39 10 – E-mail: publishing@coe.int – Website: http://book.coe.int