COUNCIL OF EUROPE
COMMITTEE OF MINISTERS

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).

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.

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 Cooperation for Accreditation (EA), the International Laboratory Accreditation Cooperation (ILAC), the International Accreditation Forum (IAF) and other bodies of a similar nature.