COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MINISTERS' DEPUTIES CM Documents CM(2017)50 2 June 2017[1]

1289th meeting, 14 June 2017

Democracy and political questions

2.3 Ad hoc Committee of Experts on Legal, Operational and Technical Standards for e-voting (CAHVE)

a. Draft Recommendation CM/Rec(2017)… of the Committee of Ministers to member States on standards for e-voting

Item considered by the GR-DEM at its meetings on 20 April and 1 June 2017.

Recommendation CM/Rec(2017)…
of the Committee of Ministers to member States
on Legal, Operational and Technical Standards for e-voting

(Adopted by the Committee of Ministers on …
at the …th meeting of the Ministers' Deputies)

Preamble

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 is part of that common heritage and is the basis of the participation of citizens in political life at the level of the European Union and at national, regional and local levels;

Having regard to 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 United Nations Convention on the Rights of Persons with Disabilities;
- the United Nations Convention against Corruption;
- the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5), in particular the Protocol thereto (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);
- the Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181);
- the Convention on the Standards of Democratic Elections, Electoral Rights and Freedoms in the Member States of the Commonwealth of Independent States (CDL-EL(2006)031rev);

[1] This document has been classified restricted at the date of issue; it will be declassified in accordance with Resolution Res(2001)6 on access to Council of Europe documents.

- Recommendation No. R (99) 5 of the Committee of Ministers to member States on the protection of privacy on the Internet;
- Recommendation Rec(2004)15 of the Committee of Ministers to member States on electronic governance (e-governance);
- Recommendation CM/Rec(2009)1 of the Committee of Ministers to member States on electronic democracy (e-democracy);
- 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 (Venice Commission) and supported by the Committee of Ministers, the Parliamentary Assembly and the Congress of Local and Regional Authorities of the Council of Europe;

Bearing in mind that the right to vote lies at the foundations of democracy, and that, consequently, all voting channels, including e-voting, shall comply with the principles of democratic elections and referendums;

Recognising that the use of information and communication technologies by member States in elections has increased considerably in recent years;

Noting that some member States already use, 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 citizens entitled to vote and 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;
- providing the electorate with a better service, by offering a variety of voting channels;

Valuing the experience gathered by the member States that have used e-voting in recent years and of the lessons learned through such experience;

Aware also of the experience resulting from the application of Recommendation Rec(2004)11 of the Committee of Ministers to member States on legal, operational and technical standards for e-voting, the Guidelines for developing processes that confirm compliance with prescribed requirements and standards (Certification of e-voting systems) and the Guidelines on transparency of e-enabled elections;

Reaffirming its belief that public trust in the authorities in charge of managing elections is a precondition to the introduction of e-voting;

Aware of concerns about potential security, reliability or transparency problems of 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 public confidence, which is a pre-requisite for holding e-elections;

Aware of the need for the member States to take into account the environment in which e-voting is implemented;

Aware that, in the light of recent technical and legal developments on e-enabled elections in Council of Europe member States, the provisions of Recommendation Rec(2004)11 need to be thoroughly revised and brought up to date;

Having regard to the work of the Ad Hoc Committee of Experts on Legal, Operational and Technical Standards for e-voting (CAHVE) set up by the Committee of Ministers with the task of updating Recommendation Rec(2004)11,

1. Recommends that the governments of member States when introducing, revising or updating, as the case may be, domestic legislation and practice in the field of e-voting:

i. respect all the principles of democratic elections and referendums;

ii. assess and counter risks by appropriate measures, in particular as regards those risks which are specific to the e-voting channel;

iii. be guided in their legislation, policies and practice by the standards included in Appendix I to this Recommendation. The interconnection between the above-mentioned standards and those included in the accompanying guidelines on the implementation of this Recommendation should be taken into account;

iv. keep under review their policy on, and experience of, e-voting, and in particular how and to what extent the provisions of this Recommendation are being implemented in order to provide the Council of Europe with a basis for holding review meetings on the implementation of this Recommendation at least every two years following its adoption;

v. share their experience in this field;

vi. ensure that this Recommendation, its accompanying explanatory memorandum and guidelines are translated and disseminated as widely as possible, and more specifically among electoral management bodies, election officials, citizens, political parties, domestic and international observers, NGOs, media, academics, providers of e-voting solutions and e-voting specific controlling bodies;

2. Agrees to regularly update the provisions of the guidelines accompanying this Recommendation;

3. Repeals Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting and the guidelines thereto.

APPENDIX I – E-VOTING STANDARDS

I. Universal suffrage

1. The voter interface of an e-voting system shall be easy to understand and use by all voters.

2. The e-voting system shall be designed, as far as is practicable, to enable persons with disabilities and special needs to vote independently.

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

4. Before casting a vote using a remote e-voting system, voters' attention shall be explicitly drawn to the fact that the e-election in which they are submitting their decision by electronic means is a real election or referendum.

II. Equal suffrage

5. All official voting information shall be presented in an equal way, within and across voting channels.

6. 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 result.

7. Unique identification of voters in a way that they can unmistakably be distinguished from other persons shall be ensured.

8. The e-voting system shall only grant a user access after authenticating her/him as a person with the right to vote.

9. The e-voting system shall ensure that only the appropriate number of votes per voter is cast, stored in the electronic ballot box and included in the election result.

III. Free suffrage

10. The voter's intention shall not be affected by the voting system, or by any undue influence.

11. It shall be ensured that the e-voting system presents an authentic ballot and authentic information to the voter.

12. The way in which voters are guided through the e-voting process shall not lead them to vote precipitately or without confirmation.

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.

14. The e-voting system shall advise the voter if he or she casts an invalid e-vote.

15. The voter shall be able to verify that his or her intention is accurately represented in the vote and that the sealed vote has entered the electronic ballot box without being altered. Any undue influence that has modified the vote shall be detectable.

16. The voter shall receive confirmation by the system that the vote has been cast successfully and that the whole voting procedure has been completed.

17. The e-voting system shall provide sound evidence that each authentic vote is accurately included in the respective election results. The evidence should be verifiable by means that are independent from the e-voting system.

18. The system shall provide sound evidence that only eligible voters' votes have been included in the respective final result. The evidence should be verifiable by means that are independent from the e-voting system.

IV. Secret suffrage

19. E-voting shall be organised in such a way as to ensure that the secrecy of the vote is respected at all stages of the voting procedure.

20. The e-voting system shall process and store, as long as necessary, only the personal data needed for the conduct of the e-election.

21. The e-voting system and any authorised party shall protect authentication data so that unauthorised parties cannot misuse, intercept, modify, or otherwise gain knowledge of this data.

22. Voters' registers stored in or communicated by the e-voting system shall be accessible only to authorised parties.

23. An e-voting system shall not provide the voter with proof of the content of the vote cast for use by third parties.

24. The e-voting system shall not allow the disclosure to anyone 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.

25. E-voting shall ensure that the secrecy of previous choices recorded and erased by the voter before issuing his or her final vote is respected.

26. The e-voting process, in particular the counting stage, shall be organised in such a way that it is not possible to reconstruct a link between the unsealed vote and the voter. Votes are, and remain, anonymous.

V. Regulatory and organisational requirements

27. Member States that introduce e-voting shall do so in a gradual and progressive manner.

28. Before introducing e-voting, member States shall introduce the required changes to the relevant legislation.

29. The relevant legislation shall regulate the responsibilities for the functioning of e-voting systems and ensure that the electoral management body has control over them.

30. Any observer shall be able to observe the count of the votes. The electoral management body shall be responsible for the counting process.

VI. Transparency and observation

31. Member States shall be transparent in all aspects of e-voting.

32. The public, in particular voters, shall be informed, well in advance of the start of voting, in clear and simple language, about:

- any steps a voter may have to take in order to participate and vote;
- the correct use and functioning of an e-voting system;
- the e-voting timetable, including all stages.

33. The components of the e-voting system shall be disclosed for verification and certification purposes.

34. Any observer, to the extent permitted by law, shall be enabled to observe and comment on the e-elections, including the compilation of the results.

35. Open standards shall be used to enable various technical components or services, possibly derived from a variety of sources, to interoperate.

VII. Accountability

36. Member States shall develop technical, evaluation and certification requirements and shall ascertain that they fully reflect the relevant legal and democratic principles. Member States shall keep the requirements up to date.

37. Before an e-voting system is introduced and at appropriate intervals thereafter, and in particular after any significant changes are made to the system, an independent and competent body shall evaluate the compliance of the e-voting system and of any information and communication technology (ICT) component with the technical requirements. This may take the form of formal certification or other appropriate control.

38. The certificate, or any other appropriate document issued, shall clearly identify the subject of evaluation and shall include safeguards to prevent its being secretly or inadvertently modified.

39. The e-voting system shall be auditable. The audit system shall be open and comprehensive, and actively report on potential issues and threats.

VIII. Reliability and security of the system

40. The electoral management body shall be responsible for the respect for and compliance with all requirements even in the case of failures and attacks. The electoral management body shall be responsible for the availability, reliability, usability and security of the e-voting system.

41. Only persons authorised by the electoral management body shall have access to the central infrastructure, the servers and the election data. Appointments of persons authorised to deal with e-voting shall be clearly regulated.

42. Before any e-election takes place, the electoral management body shall satisfy itself that the e-voting system is genuine and operates correctly.

43. A procedure shall be established for regularly installing updated versions and corrections of all relevant software.

44. If stored or communicated outside controlled environments, the votes shall be encrypted.

45. Votes and voter information shall be kept sealed until the counting process commences.

46. The electoral management body shall handle all cryptographic material securely.

47. Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment shall immediately inform the electoral management body.

48. 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.

49. The e-voting system shall identify votes that are affected by an irregularity.

APPENDIX II – GLOSSARY OF TERMS

In this Recommendation and explanatory memorandum the following terms are used with the following meanings:

- access control: the prevention of unauthorised use of a resource;
- assessment: an evaluation of persons, hardware, software and procedures to verify if they are suitable for the fulfilment of certain tasks;
- audit: an independent pre- or post-election evaluation of a person, organisation, system, process, entity, project or product which includes quantitative and qualitative analysis;
- authentication: the provision of assurance of the claimed identity of a person or data;
- availability: the state of being accessible and usable upon demand;
- ballot: the legally recognised means by which the voter can express his or her vote;
- candidate: a voting option consisting of a person, a group of persons and/or a political party;
- casting of the vote: entering the vote in the ballot box;
- certificate: a document which is the result of a formal certification wherein a fact is certified or attested;
- certification: a process of confirmation that an e-voting system is in compliance with prescribed requirements and standards and that it includes, at the minimum, provisions to ascertain the correct functioning of the system. This can be done through measures ranging from testing and auditing through to formal certification. The end result is a report and/or a certificate;
- certification body (or certifier): an organisation entitled to conduct a certification process and to issue a certificate upon completion of the process;
- certification report: a document which explains what a certificate has certified and how it is certified;
- chain of trust: a process in computer security which is established by validating each component of hardware and software from the bottom up. It is intended to ensure that only trusted software and hardware can be used while still remaining flexible;
- component testing: a method by which individual units of the system code are tested to determine if they are fit for use;
- confidentiality: the state characterising information that should not be made available or disclosed to unauthorised individuals, entities or processes;
- controlled environment: premises supervised by election officials, e.g. polling stations, embassies or consulates;
- e-election: a political election or referendum where e-voting is used;
- electoral management body (EMB): institution in charge of managing elections in a given country at national or lower level;
- electronic ballot box: the electronic means by which the votes are stored pending being counted;
- e-vote: electronically cast vote;
- e-voting: the use of electronic means to cast and/or count the vote;
- e-voting system: the hardware, software and processes which allow voters to vote by electronic means in an election or referendum;
- formal certification: certification carried out by official authorities, only before election day and leading to the issuance of a certificate;
- guidelines: any document that aims to streamline particular processes according to a set routine. By definition, guidelines are not legally binding;

- non-disclosure agreement (NDA): a legal contract between two or more parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to by parties not bound by the contract;
- open access: access online to material that is free for all to read, and possibly to use (or reuse) within certain limits;
- protection profile: an implementation-independent set of security requirements for a category of products that meet the specific security needs of consumers;
- requirement: a singular documented need of what a particular product or service should be or perform;
- remote e-voting: the use of electronic means to cast the vote outside the premises where voting takes place in general;
- 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, including through encryption;
- stakeholder: a person, group, organisation, or system that has an impact on, or can be affected by, a government's or organisation's actions. These include citizens, election officials, political parties, governments, domestic and international observers, media, academics, (I)NGOs, anti-e-voting organisations and specific e-voting certification bodies;
- standard (legal): refers to provisions contained in Appendix I to Recommendation CM/Rec(2017)xx;
- standard (technical): an established norm usually in the form of a formal document that establishes uniform engineering or technical criteria, methods, processes and practices;
- testing: the process of verifying that the system works as expected;
- 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).