COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MINISTERS' DEPUTIES | CM Documents | CM(2017)50-add2final | 14 June 2017

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)

b. Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting

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

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);
- 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;

Adopts the following guidelines on e-voting standards to serve as a practical tool for the governments of the member States in endorsing, adopting, implementing and monitoring the e-voting approach described therein and adapting their e-voting systems;

Invites the governments of the member States to ensure that the guidelines are widely disseminated among electoral management bodies, election officials, citizens, political parties, domestic and international observers, non-governmental organisations (NGOs), media, academics, providers of e-voting solutions and specific e-voting controlling bodies.

Introduction

1. The present guidelines are the updated version of 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. The original two guidelines were approved in 2011 with the aim of providing guidance on how to implement the provisions on certification and transparency of Recommendation Rec(2004)11 of the Committee of Ministers to member States on legal, operational and technical standards for e-voting of 30 September 2004.

2. The Recommendation Rec(2004)11 and the original guidelines were reviewed and updated in 2015 and 2016 by the Ad hoc Committee of Experts on Legal, Operational and Technical Standards for e-voting (CAHVE), set up by the Committee of Ministers on 1 April 2015.

3. The present guidelines provide guidance on the implementation of the provisions of the Recommendation CM/Rec(2017)5. Each of the guidelines is identified by a number, which refers to the corresponding provision in the recommendation.

4. The present version of the guidelines is a work in progress that will be further completed to address all forms of e-voting covered by Recommendation CM/Rec(2017)5. Therefore, on-going developments in the legal and technical fields will require that the provisions of the guidelines be updated on a regular basis.

5. The guidelines are designed for use in political elections and referendums at all tiers of governance. They are not intended as a strict set of rules for member States, imposing a particular way of implementing the provisions of the updated recommendation, but are intended to provide guidance and to support member States on the subject.

6. The guidelines, like the updated recommendation, are not an exhaustive regulatory framework for e-voting. Member States need to further develop these provisions to take account of national specificities in the electoral field. The guidelines also include examples of effective implementation of standards in specific contexts, called “good practice. Examples of good practice are included for information purposes.

I. Guidelines for the implementation of universal suffrage recommendations

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

a. The presentation of the voting options on the device used by the voter should be optimised for the average voter who does not have specialised computer knowledge.

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

b. Voters should 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.

Accessibility implies that systems are designed in such a way that as many voters as possible can use them. IT- Products and services must be functional and take into account the needs of the public, without being unnecessarily complicated. Such requirements might be achieved with a collaborative approach involving the development team and a representative panel of users.

c. Consideration should be given, when developing new IT-products, to their compatibility with existing ones.

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

a. Voters should be supplied, whenever required and possible, with additional facilities, such as special interfaces or other equivalent resources, such as personal assistance.

E-voting can be an alternative way of voting that provides additional possibilities to people with disabilities and special needs to vote independently. An acceptable balance should be found between providing such access possibilities and respecting other requirements, namely those on the security of e-voting.

b. Internet voting interfaces should comply as much as possible with the guidelines set out in the Web Accessibility Initiative (WAI).

The World Wide Web Consortium (W3C) was created in 1994 to lead the World Wide Web (WWW) to its full potential by developing common protocols. It initiated the WAI to promote a high degree of accessibility for people with disabilities. The WAI pursues web accessibility through five main areas of work: technology, guidelines, tools, education and outreach, and research and development. WAI has produced a set of standards and guidelines in support of accessibility (for example, web content accessibility guidelines, authoring tools, accessibility guidelines, user agent, accessibility guidelines, XML accessibility guidelines). More information is available from the WAI web site at http://www.w3.org/WAI.

WAI is commonly used in the context of browser-based solutions for internet voting. Even when internet voting uses alternative solutions (for example, the voting application is a separate unique "browser" in itself), WAI general principles can be followed.

II. Guidelines for the implementation of equal suffrage recommendations

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

a. The electronic ballot used for e-voting should be free from any information about voting options, other than that required by law.

The e-voting interface should not contain more information about the choices than the official (usually paper) ballots. Elements such as pop-up screens that promote a specific candidate or position, or audio elements that are associated with a particular candidate or point of view, and any other information which does not appear on the paper ballot (equality of voting channels) should not appear on the e-voting interface. This does not prevent the display of official information on voting options.

b. If information about voting options is accessible from the e-voting site, it shall be presented in an equitable manner.

Information about voting options should be presented in an equitable manner in all voting channels.

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.

a. If a voter is allowed to cast an electronic vote multiple times, appropriate measures should be taken to ensure that only one vote is counted.

b. If a voter is allowed to cast a vote by more than one voting channel, appropriate measures should be taken to ensure that only one vote is counted.

Guidelines 9a and 9b: Wherever multiple voting is allowed this should also be reflected in e-voting. For instance, certain voting systems allow voters to submit an advance vote, or several advance votes, and change their minds later. Only the last vote is inserted into the ballot box and thus is the vote cast. This is the case in Andorra, Denmark and Sweden.

The multiple voting option (multiple e-votes or multiple votes via more than one voting channel) may be introduced with e-voting, as a countermeasure to voter coercion, which remains possible when voting takes place outside a controlled environment (remote voting). This is the case in Estonia.

The determination of which vote should be counted is to be made at national level. In an e-voting context, a country may decide that the paper vote has priority. Elsewhere only the last vote cast will be counted. A third country may decide that the first validly issued vote is the one that counts. To be in line with the principles of democratic elections, the e-voting system (or the simultaneous use of paper-ballot and e-voting methods) shall ensure equal suffrage. National legislation decides which of the multiple votes is counted. The "one person, one vote" principle must respected.

The decision on which vote is counted depends on the national policy towards remote voting. Countries that have a stricter policy towards remote voting will tend to give priority to the paper ballot if this is the vote issued at the polling station (controlled environment). Countries that are more open to remote voting may decide that the first validly issued vote is the one that counts, and in this case an e-vote from an uncontrolled environment may supersede a later-issued paper vote. Decisions on how to deal with voter coercion in the case of remote voting in general are to be taken by the national legislature. They should not be left to the e-voting administration alone, as they are a matter of remote voting policy in general, and not only of e-voting implementation.

c. In all other cases appropriate measures should be taken to prevent a voter from casting more than one vote.

In countries where multiple voting is not allowed, multiple votes are considered as an attempt to cast more votes than a particular voter is permitted. This risk might arise, for instance, if the voter tries to cast multiple votes him or herself or if another person tries to use the voter's identity in order to vote, in the voter's name, after he or she has voted.

In the context of voting with paper ballots, this risk is managed through organisational measures. For instance, in the United Kingdom, if a person enters a polling station to vote and finds that somebody else has already voted in his or her name, that person is entitled to cast a special vote with a tendered ballot. This ballot is not placed in the ballot box but is sealed in an envelope, 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. Appropriate measures need to be provided in the context of e-voting. Secure identification is important. Keeping the link between the voter's identification codes and his or her sealed ballot for a defined period may be one of the measures taken.

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 could lead to voting taking place at different times include:

- *when casting a vote in a polling station is the fall-back option for voters who are within the national territory in the event that the electronic voting channel breaks down, the closing time for the electronic voting channel has to be set before the closing time of the polling station;*

- *when the system is designed and operated in such a way that voters can choose between voting channels, but the channels used do not have access to a common register where the names of electors who have voted can be seen, the periods of time when these channels are available should generally not overlap.*

In all cases, counting should only start after the closure of all voting channels.

d. In all cases, the voter should be clearly informed about the voting possibilities that are offered and about the rules for the counting of votes.

It is particularly important to inform the voter his or her voting possibilities, including the possibility to issue more than one e-vote or to vote more than once through different voting channels successively, where multiple voting is allowed.

In all cases the voter should be informed about the vote counting rules in force, in particular about which vote will finally be counted.

III. Guidelines for the implementation of free suffrage recommendations

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

a. In the case of remote e-voting, the voter should 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.

In the context of remote e-voting, possible scenarios to be considered are that fraudulent servers may be introduced, for example imitating an official server by tampering with the domain name system (DNS), using a similar domain name to that of the official server, or corruption of the server code (for example, via malware), among others. Voters receive information on how to check the certificate of the official e-voting site. Electronic signatures applied to the ballot by the electoral authority allow for verification of the ballot. This, however, shall not violate the confidentiality of the vote.

b. The e-voting system should not permit any manipulative influence to be exercised over the voter during the voting. In particular, the electronic ballot by which an electronic vote is cast should be free from any unofficial information.

Similar to provision 5a, this guideline requires that the voter be presented only with official voting information and that any manipulative influence from unauthorised parties be excluded.

c. The e-voting system should introduce all possible measures to avoid any manipulative influence to be exercised over the vote once it has been cast, and it will include measures to allow verification that no such influence was exercised.

The concept of free suffrage also protects the vote from any manipulative influence after it has been cast. Any manipulative influence on or unauthorised intervention in the vote must be avoided. Of course, if authorised, multiple voting is not affected by this provision and the voter should be allowed to vote multiple times.

The provision aims at preventing any unauthorised changes to the vote, once it has been cast. It protects from attacks coming from outside the system and from internal threats. Individual and universal verifiability (see standards 15 and 17) are checks that aim at detecting any such unauthorised intervention.

d. Where considered necessary, the e-voting system should offer mechanisms (for example, multiple voting) to protect voters from coercion to cast a vote in a specific way.

Multiple voting is considered to be a mechanism that protects the voter from coercers by allowing him or her to re-vote.

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

a. Voters should be able to alter their choice at any point in the remote e-voting process before casting their vote, or to break off the procedure.

This provision foresees the possibility of breaking off the procedure before the vote is cast, that is, before it enters the electronic ballot box. Once the vote is registered this will no longer be possible. The interface must therefore be programmed to attract voters' attention to this point, for instance by asking them to confirm their intentions before issuing the vote. It would be useful also to remind voters that this operation will validate and finalise the vote in cases where multiple voting is not allowed.

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.

a. When using e-voting machines in polling stations, member States should consider the use of paper ballots as a second medium to store the vote for verification purposes.

Also known as the voter-verified paper audit trail (VVPAT), this method aims at ensuring free suffrage where the vote takes place on e-voting machines in controlled environments. If the e-solution applied in polling stations is a ballot scanner, a second medium is not necessary as the ballot in this case is by definition paper.

Other solutions for providing a second medium include, for instance, parts of the ballot sheet that can be torn away (for example, Chaum's scantegrity model) for individual verifiability. They may be very similar to VVPAT or take another form. They should be made of paper, which is both unalterable and human legible/verifiable.

The validity of this second medium is to be assessed by national regulations that will also decide what to do in case of discrepancies between electronic results and those produced by the second medium.

b. A mandatory count of votes in the second medium in a statistically meaningful number of randomly selected polling stations should be carried out in particular for e-voting machines and optical scanners.

Criteria such as the percentage of votes or the number of polling stations where the count takes place, their designation, etc. should be decided at national level. They should make sure that the overall aim of ensuring free elections is attained.

IV. Guidelines for the implementation of voting secrecy recommendations

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.

a. Voter register data should be clearly separated from voting components.

This provision applies more specifically when biometric techniques to identify the voter are used in polling stations in addition to using e-voting machines or scanners for voting. Separating the two components ensures vote secrecy.

Where votes and anonymised voter information are kept together, end-to-end encryption must protect this information.

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.

a. Authentication should use cryptographic mechanisms.

This provision requires state-of-the-art technical solutions to protect authentication data.

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

a. Where paper proof of the electronic vote is provided to the voter in a controlled environment, the voter should not be allowed to show it to any other person, or take this proof outside of the polling station.

The e-voting should not provide proof of the content of the vote to the voter. Where this is programmed at some point in the voting procedure, as may be the case when voting on e-voting machines in polling stations, organisational measures should be in place to prevent any use of this proof to breach the secrecy of the vote. The aim is to protect voting secrecy and prevent the practice of vote selling. Of course this does not prevent the voter, in absolute terms, from disclosing the content of his or her vote, for instance by taking a picture of it. It is up to the national criminal or administrative laws, which also apply to e-voting, to sanction such breaches of voting secrecy.

b. No residual information related to the voter's decision should be displayed after the vote has been cast.

The term "residual information" refers to information that remains accessible at various locations (in the personal computer's memory, the browser cache, the video memory, swap files, temporary files, etc.) after the vote has been cast and which may reveal the voter's decision.

The provision advises the system developers or service providers to design the e-voting system in such a way that residual information is deleted after the vote has been cast. Technically there may be limited means to ensure this in a remote voting environment. Nevertheless, every measure possible should be taken to delete such residual information when the vote has been cast. However, individual verifiability can be implemented provided adequate safeguards exist to prevent coercion or vote-buying.

c. In the case of remote e-voting, the voter should be informed of possible risks to voting secrecy and recommended means to reduce them ahead of voting.

d. In the case of remote e-voting, the voter should be informed on how to delete, where it is possible, traces of the vote from the device used to cast the vote.

Guidelines 23c and 23d: In the case of remote e-voting, voters should be clearly informed of the risk of breach of secrecy of the vote and on measures and good practices to adopt to counter this risk, for instance by using firewalls, cleaning traces, etc. The system itself should delete automatically as many such traces as possible.

E-voting from a remote, uncontrolled environment implies shared responsibilities between the voter and the e-voting system/election administration body. It is part of the voter's responsibility to adopt the recommended measures (referred to in this provision). It is the duty of the electoral authority to clearly inform the voter on at least three points: the principle of shared responsibilities; the different measures to be adopted by the voter to reduce risk (running an anti-virus software, firewall, deleting traces of the vote, etc.); and remaining risks and verifiability techniques.

Such information should reach the voter well ahead of the voting period. Based on this, the voter can decide whether or not to use remote e-voting.

Warning messages may appear at the beginning of the e-voting procedure; a message on recommended steps that the voter should follow after voting (deleting traces, for instance) may need to be transmitted to the voter at the end of the e-voting procedure. However, such messages are only reminders and do not replace the initial complete information that the voter should receive ahead of the e-voting period.

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.

a. Voter information should be separated from the voter's decision at a pre-defined stage of the counting process.

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

The term "voter information" refers to anonymised information on the voter, such as the identification codes used in remote e-voting. Whereas the link between such information and the sealed vote must be maintained for a certain time under appropriate protection, to allow, in particular, the possibility of multiple voting while respecting the "one person, one vote" principle, the link should be destroyed before the counting takes place.

The encryption of votes will generally be necessary to secure the anonymity of voting. In many cases the vote is encrypted before starting the transmission via computer networks. It 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.

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.

c. Member States should take the necessary steps to ensure that the confidentiality of any information obtained by any person while carrying out auditing functions is guaranteed.

In addition to protecting the information gathered by the audit system against unauthorised access, legal and organisational measures should be taken to check the persons that have authorised access to the audit system. Such measures could, for instance, be included in the accreditation process.

V. Guidelines for the implementation of regulatory and organisational recommendations

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

a. A formal feasibility study should be undertaken and published before the selection and implementation of any e-voting technology. It should include reasons for the adoption of this system, risk analysis, an assessment of the legal framework, the planning of pilots and the evaluation thereof, as well as a cost–benefit analysis.

b. Any implementation of e-voting pilots should start well ahead of elections and include essential preparations such as the adoption of detailed regulations, if necessary, for the pilots and system testing.

c. The final version of the e-voting system should be tested before it is used in regular, binding elections.

d. Pilots should be conducted on the basis of clear and comprehensive criteria to evaluate the effectiveness and integrity of the e-voting system, including the transmission of results.

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

a. The legal framework should include procedures for the implementation of e-voting from set-up and operation to counting.

Detailed provisions will most probably appear in lower-level regulations and instructions. This should be provided for in higher-level laws which should also clarify the responsibilities for adopting such detailed regulations.

b. The legal framework should include rules for determination of the validity of an electronic vote.

c. The legal framework should include rules dealing with problems, failures and discrepancies resulting from the use of verification tools.

When member States use a second medium to store the vote and a mandatory count is carried out, discrepancies between the results of votes cast may arise. In such cases the rules should make clear which type of vote (electronic or the alternative medium) takes precedence. An argument for the electronic vote is that voters have cast their vote in this manner. A case for the second medium would be that this vote could have been verified by the voter themselves, particularly if the medium under consideration includes a paper trail.

Therefore in case of any discrepancy, the case should be examined thoroughly and any decision on the result of the vote count should depend on the result of the investigation. Member States are asked to establish rules which should address which vote is used in the official counts, if and when a recount is considered necessary, when and how the mandatory count takes place, under which circumstances all second votes are counted, and when a re-election should be held.

d. The legal framework should include procedures for the process of data destruction, in particular to align processing, storing and destruction of the data (and equipment) of voting technology with the personal data protection legislation.

The storage medium that contains the votes (hard drive, memory sticks, etc.) should be destroyed.

e. The legal framework should include provisions for domestic and international observers.

Member States should include the role of domestic and international observers in the e-voting process and should regulate this in line with international commitments and good practice. The type of access to e-voting that observers will have will depend on national provisions. These should reflect international commitments, such as those of the Office for Democratic Institutions and Human Rights of the Organization for Security and Co-operation in Europe (OSCE/ODIHR). Observers should include representatives of political parties and the general public.

f. Legislation should provide for clear timetables concerning all stages of the e-election.

An e-election can differ from an 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 and the way the e-voting actually takes place. These differences should be clearly 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 a well-founded decision on which voting channel to use. Careful consideration should be given to how much time the voter needs for this decision.

g. The period in which an electronic vote can be cast should not begin before the notification of an election or a referendum.

Communicating the period of time for voting is especially important when the e-voting time period differs from other voting channels. This difference arises particularly in the case of remote e-voting in which a different period of time for voting using the electronic voting channels may be necessary, due to the specific nature of those channels.

h. Remote e-voting may start and/or end at an earlier time than the opening of any polling station.

i. The period in which an electronic vote can be cast should not continue after the end of the voting period.

Guidelines 28h and 28i: 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.

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, if a voter's personal computer is not working due to a power failure), a voter who is living 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 were to continue after polling stations close, the voter would not have this possibility.

j. The depositing of electronic votes into the electronic ballot box should be allowed for a sufficient period of time after the end of the e-voting period to allow for any delays in the passing of messages over the remote e-voting channel.

k. After the end of the e-voting period, no voter should be allowed to gain access to the e-voting system.

Guidelines 28j and 28k: These provisions deal with internet voting sessions that start shortly before the e-voting channel closes. The ballot box should stay open to be able to collect these votes. The duration will be equivalent to the normal duration of an e-voting session to allow those voters who access the system a few seconds before it closes to finish the e-voting process normally.

Another case, again in internet voting scenarios, relates to a higher demand on the services which might occur in the short period just before the poll closes. This may lead to delays before the vote enters the electronic ballot box. Votes that have been sent in time should not be discarded as a result of such delays. The processing of the votes must not be shut down immediately after the closing of the e-voting service. However, starting an e-voting session after the system has closed should not be possible.

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.

a. Procurement processes for e-voting should be carried out in a transparent manner.

b. Provisions should be made to ensure against possible conflicts of interest of private stakeholders involved in the process.

c. A strict separation of duties shall be maintained and documented.

d. Member States should take appropriate measures to avoid circumstances where the election is unduly dependent on vendors.

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

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

b. The counting of votes should be reproducible. There should be a possibility to obtain sound evidence that the counting procedure has been performed satisfactorily including through an independent recount.

The objective here is that there should be a possibility to obtain sound evidence that the counting procedure has been performed correctly. An independent recount is one way to do this, if it is done with a different system from a different source. However, this can be achieved by other means, for example, using cryptographic proof (universal verifiability).

c. Other features that may influence the accuracy of the results of the e-voting system should be verifiable.

Depending on the system used, there may be elements other than a recount that contribute to the accuracy of the result. The confirmation that all votes cast have been counted is an example.

In addition to verification tools, the percentage of votes cast by e-voting and the comparison of the results of e-voting with the results of voting by other channels shall be considered to establish the plausibility of the e-voting results and to validate their accuracy.

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

The information kept in the electronic ballot box must be protected as long as is necessary to allow for possible recounts or legal challenges or other legal requirements in the member State in question.

VI. Guidelines for the implementation of transparency and observation recommendations

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

a. The competent electoral authorities should publish an official list of the software used in an e-election. At the very least it should indicate the software used, the version, date of installation and a brief description.

Constant developments in information and communication technologies require frequent updates of hardware and software and regular adaptations to central systems and voting facilities used in a controlled environment (for example, voting machines). For e-voting to remain transparent, 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 the legal provisions in force, citizens.

b. Public access to the components of the e-voting system and information thereon, in particular documentation, source code and non-disclosure agreements, should be disclosed to the stakeholders and the public at large, well in advance of the election period.

When an electronic device/system yields binding results, the technical details that determine what and how to calculate can easily become just as important as an electoral law that defines polling stations' counting rules. To ensure public confidence through transparency, the voting software source code, the configuration as well as the list of all hardware and software components of the e-voting system should be part of the audit trail. Protocols of audited processes such as the installation and set-up procedure, the verification that the certified source code is the one used during the election, and the tallying process of the electronic ballot sheets should also be part of the audit trail. This should help member States to provide relevant documentation to voters and third parties, including national and international observers and the media.

The expression "well in advance" implies that clear time frames are set in national regulations for such disclosure and that the planned deadlines allow stakeholders to exercise their rights, react to such disclosures, and request changes. The electoral management body should have the time and possibility to react to such feedback, including by updating the system. Publishing such information twelve months before the vote may respect the "well in advance" criteria. Shorter time frames for last-minute changes might be necessary. However the main elements should be disclosed well in advance and not just shortly before the election.

c. Deployment of electronic voting technologies should include the development of comprehensive, detailed, step-by-step guidelines including a procedural manual.

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.

a. Support and guidance material on voting procedures should be made available to voters.

Support and guidance material on voting procedures should be in place regardless of the specific channel used. For each electronic voting channel used, such information should be available at least on the same electronic voting channel. In other words, a website with help information and e-mail facilities, at the minimum, should be in place when internet is the e-voting channel and a telephone hotline should be in place when voting by telephone is possible.

b. In the case of remote e-voting, voter information material should also be available through a different, widely available communication channel.

Information on remote e-voting should be available also on a fall-back, different, widely available communication channel for situations when the remote e-voting channel is out of order. For example, a telephone hotline might be such an alternative communication channel for internet voting.

c. Voters should be provided with an opportunity to practise before, and separately from, the moment of casting an electronic vote. In such a case, participants should have their attention drawn explicitly to the fact that they are not participating in a real election or referendum.

Traditional voting methods are well tried and tested in member States and voters are familiar with the general rules that govern them. The introduction of e-voting challenges the voter. Such systems and the way they operate are less easy to understand. To maintain voter understanding and confidence, steps should be taken to present the system to voters. This effort may need to continue over time.

To promote understanding and confidence in any (new) e-voting system, opportunities to practise using it should be provided before and separately from the moment of casting an electronic vote (for example, through demo systems or test elections). Special attention should be paid to categories of voters liable to have greater difficulties (for example, the elderly) and their specific needs.

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

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

b. Domestic and international observers should have access to all relevant documentation on e-voting processes.

Access to documentation, including minutes, certification, testing and audit reports, and detailed documentation explaining the operation of the system, is essential for domestic and international observers. Such observers include representatives of political parties and the general public. They should be invited to relevant meetings. Where possible, member States, the vendor or the certification body should provide information to all stakeholders, for example by posting relevant documents on the internet well in advance of the election period.

Member States should develop procedures to define who has access to what and when. Such procedures should also be developed for domestic and international observers as well as for the media. Procedures for other stakeholders such as citizens, political parties and NGOs also need to be established. Open access should be the central theme in these procedures.

Member States should make these requirements clear to potential vendors who should also understand that stakeholders, and specifically domestic and international observers, require access to certain documentation during the tender process. Non-disclosure agreements, which prevent observers from publishing assessments and the facts on which assessments are based would deprive all stakeholders – most importantly observers – of important information.

c. Member States should make the relevant documentation available to observers, as far as practicable, in a language commonly used in international relations.

Relevant information required by domestic and international observers to carry out their work satisfactorily should be available in the official language, or languages, of the country concerned. Such information should, as far as possible, also be made available in one of the official languages of the Council of Europe (English and French). In particular, international observers require access to documentation in one of these languages.

d. Member States should provide training programmes for domestic and international observer groups.

E-voting systems are not easily understandable for non-e-voting-experts. In order to improve stakeholders' understanding of the system in use, training is necessary, in particular for domestic, but also for international observers. It should provide basic and easy tools for use in observation work, including ways to check seals, read a voting machine print out and read an audit file.

e. Domestic and international observers and the media should be able to observe the testing of the software and hardware.

Stakeholders, including accredited observer groups, should not only have access to documents, but should also be able to observe the verification of the e-voting devices and system. The observation of such tests and/or audits should not interfere with the election process. Therefore, such monitoring should only take place under guidance of those responsible for the organisation of elections. As already mentioned, such observers should include representatives of political parties and the general public. Furthermore, the people observing the tests and/or audits should attend a training session in advance. The process should be open enough to allow observers to have full insight into the operation of the system.

f. Election observers should have access to all steps of the evaluation and certification process.

In the past twenty years, election observation has proven to be a successful method to ensure transparency and access to elections. With the emergence of electronic voting, the established methodologies for election observation need to be updated. To enable observers to observe the certification of electronic voting systems, the duration of election observation missions needs to be

extended. It is crucial that none of the procedures necessary for certification of e-voting take place behind closed doors as this would raise suspicion.

Observers, including representatives of political parties and the general public, should be granted access to all relevant information during the entire duration of the certification process in order to carry out their duty. Observers, for their part, need to disclose the methodology they are going to apply.

VII. Guidelines for the implementation of accountability recommendations

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.

a. Member States should establish the aims of certification and the certification methods.

When considering certification of on-site or remote e-voting systems, the first step is to clearly define the aims of and requirements for the certification procedure. When drafting these requirements, it is important to verify that they are in line with domestic legislation and international standards, including any appeals or complaint procedures relating to the conduct of elections. Although a detailed list of requirements might initially seem to be a good way to guarantee a proper certification analysis, a strict legal framework might generate paradoxical effects. For example, auditors would be subject to a high level of supervision, but vendors could customise their products to the limited goal of simply fulfilling the prescribed requirements of a given electoral administration. In these circumstances, vendors might not optimise the product and the electoral administration would be obliged by its own legal rules to accept a sub-optimal product. The use of a contract where the award criterion is quality and not price should help to avoid this trap.

Defining the aims, requirements in terms of software, operating system, hardware and e-voting process, and the scope and methods will contribute to the effectiveness of the certification process, the usability of the certification regime and the overall transparency of e-voting systems.

Certification of e-voting systems is not limited to the initial certification; it also includes procedures for de-certification and re-certification of software, operating systems, hardware and processes.

Sociopolitical factors may condition citizens' confidence and pose a major challenge. As such factors may also have a bearing on certification processes; member States should promote scientific research in this field, including an international exchange of relevant information.

A framework should be established that ensures all parties are aware of and have a good understanding of the system. Work should be done in accordance with established methodologies such as confirmation testing, component testing, performance testing and functional testing.

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.

a. Member States should determine the apportioning of costs entailed in the certification process. They should define the responsibility, including financial, of the certification body for the quality of their work.

Anybody authorised to participate in the certification of an e-voting system, including certifiers, evaluators and auditors, must be independent and qualified. The criteria, modalities and competent

institutions involved in the selection of certification bodies should therefore be explicitly laid down in national legislation. Member States are responsible for drafting the rules and guidelines for the selection process.

These procedures need to be known and made public well in advance of the election day. This will facilitate the task of vendors and foster electors' trust in procedures. The number of certification bodies should not be limited; anybody who is independent and qualified should be eligible to perform the certification. Preference should be given to the use of a European public tender or consultation with a set of potential certifiers for the determination of qualified certifiers.

Member States should consider having the selection procedure carried out by internationally certified professional auditors. For example, CISA (Certified Information System Auditors), is a standard of achievement for those who audit, control, monitor and assess an organisation's information technology and business systems. Attention should be paid to the costs of such procedures. Another important factor is that the use of international certificates should not become an obstacle for member States to use a specific e-voting system or even make it impossible for countries to use a specific valid e-voting system.

Member States should make explicit from the outset which bodies are responsible for the costs of the certification procedure. They may decide that the entire cost, including formal certification, is to be borne by the vendors, which could lead to a greater involvement by the latter. Costs could also be the responsibility of the member State in question, and a third option is to share the costs. The costs of certification should under no circumstances compromise the independence, integrity and quality of the certification process. Whichever option is chosen, the member State should have sufficient funding available and the decision should be made public.

b. Evaluation and certification bodies should have full access to all relevant information and should be allotted sufficient time to carry out the certification process ahead of the election.

Certification bodies should have access to information and data which is necessary and sufficient to perform their duties, namely to reach a conclusion regarding the voting system under inspection; they should have sufficient time to review all information and data. Citizens have the right to know what kind of information has not been considered necessary and sufficient to conduct the certification. Moreover, rules regarding the relationship between the vendor and the certifier, such as non-disclosure agreements (NDA) or other similar documents should be made public.

In some cases, such as early elections or the introduction of a new voting system, certification processes may take place only shortly before the elections open. This entails a risk of not having sufficient time to undertake a thorough certification procedure and this could, in turn, jeopardise the credibility of the election. Therefore, the certification procedure needs to be finished ahead of the elections, giving enough time to review the conclusions.

One solution to save time and money is to certify only the modified modules and the sequence of the modules for future certification, once an initial certification process has been carried out and the e-voting component has been certified. This can only be done if a difference is made between major changes (modifications) and minor changes to the e-voting system.

c. The mandate of the evaluation and certification bodies should be reconfirmed regularly at prescribed intervals.

Member States should develop procedures not only for the initial selection procedure, but also for follow-up procedures such as re-examination or re-confirmation of the mandate and withdrawal of the mandate. The mandate given to any certification body to certify an e-voting system should be valid only for a limited time. Tenders need to be made at regular intervals, and these tenders need to be public. It must be made clear whether the decision to entrust system certification to a specific, selected certification body may be taken by the vendor or whether this decision lies with the competent electoral authority.

d. The conclusions reached in a certification report should be self-explanatory with the information contained in that report.

The certification report should be self-explanatory, namely that its conclusions should only be based on the information it contains, enabling a third party to replicate the same research and thereby confirm that the conclusions of the certification report are valid.

e. Member States should set and publish clear rules with regard to the disclosure of the final certification report and of all relevant documents, bearing in mind the importance of transparency.

Member States should devise and publish procedures in which it is defined who has access to what information and when. Specific attention must be given to the needs of domestic and international observers and to those of the media. Also, procedures for other stakeholders, such as citizens, political parties, NGOs and, not least, election officials need to be established. Such procedural rules are essential in order to reinforce citizens' confidence in the security and reliability of e-voting systems and in the oversight role of the electoral authorities. Non-disclosure of all or part of the certification report or of all relevant documents should only be considered in exceptional circumstances.

Special attention must be given to those components of the software that are relevant for the system's security. This could be done by including the testing of security in test plans in order for the reader to understand how security was tested. Labelling of all documents by member States and vendors may also be considered.

Vendors and even certifiers themselves might not agree with publication of some or most of the documentation of the e-voting system, as they wish to protect intellectual property rights. So as to avoid excessive secrecy during certification processes, potential vendors and certifiers should therefore be made aware, during the tender process, that stakeholders need to be granted access to specific documentation. NDAs which prevent observers from publishing assessments and the facts on which assessments are based make it very difficult to conduct a meaningful observation.

Finally, in order to oversee the certification process, or to compensate for any partial and incomplete disclosure of information to the public, member States may establish specific committees with experts, academics and/or politicians. For example, in Belgium, a college of experts is responsible for overseeing the entire electoral process for the competent legislative assembly.

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

a. The audit system should record times, events and actions, including:
- all voting-related information, including the number of eligible voters, the number of votes cast, the number of valid and invalid votes, the counts and recounts, etc.;
- any attacks on the operation of the e-voting system and its communications infrastructure;
- system failures, malfunctions and other threats to the system.

Automated tools and system procedures should enable the data to be analysed and reported on in a fast and accurate manner, thus enabling rapid corrective action. The audit system should provide verifiable reports on:
- *cross-checks of data;*
- *system or network attacks;*
- *intrusion detection and reporting;*
- *data manipulation;*
- *fraud and fraud attempts.*

The audit system should maintain records of any attacks on the operation of the election or referendum system or its communications infrastructure. The system shall include a function 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.

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

b. The e-voting system should maintain reliable synchronised time sources. The accuracy of the time source should 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.

There may be different accuracy requirements for different users 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" is used as an indication for marking the data. There are several means available, depending on the situation: secure time stamps might be needed for critical events, whereas 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. Careful consideration should therefore be given as to how and if they should be used in relation to ballots or votes.

c. The conclusions drawn from the audit process should be taken into consideration in future e-elections.

VIII. Guidelines for the implementation of system reliability and security recommendations

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.

a. The availability of e-voting services to all voters during the entire e-voting process must be maintained.

An e-voting system should be protected against malfunction and breakdown. However, the possibility of a breakdown can never be entirely excluded. Procedures and alternative solutions for emergency cases should be foreseen.

b. Voters should be promptly informed through appropriate means in case of interruption, suspension or restart of the electronic voting system.

c. The voting system does not exclude eligible voters from casting their vote.

d. The e-voting system should maintain the availability and integrity of the votes.

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 encryption.

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

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

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, take into account the possibility of denial of service attacks and should document the contingency reserve in system performance that has been designated. Independent penetration tests can reduce the probability of successful deliberate service disruption.

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

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

f. Member States should consider usability throughout the development of security mechanisms.

Guidelines 40e and 40f: This does not suggest that every possible method of protection available must be used. In each case, a choice will have to be made as to the nature and extent of the protection measures to be applied. A proper balance shall be struck between different, equally important factors, for example 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. Similar considerations might apply if a very small additional security benefit is only achievable at an excessively high usability cost.

g. Regular checks should be performed to ensure that e-voting system components operate in accordance with the system's technical specifications and that its services are available.

h. Key e-voting equipment should be located in a secure area and that area shall, throughout the election or referendum period, be guarded against any unauthorised interference or access.

i. During the election or referendum period, a disaster recovery plan should be in place.

Guidelines 40h and 40i: For their security, central systems must be installed in secure, controlled locations. Physical access should be controlled and restricted. An alternative location should also be planned to be able to react after a physical disaster, with the appropriate equipment pre-reserved (disaster recovery planning).

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 established. These will imply procedures, backup arrangements, resource reservation and so on.

j. It should be possible to check the state of protection of the voting equipment at any time. Those responsible for the equipment should use special monitoring procedures to ensure that during the polling period the voting equipment and its use satisfy requirements.

k. Sufficient backup arrangements should be in place and be permanently available to ensure that voting proceeds smoothly. Any backup system should conform to the same standards and requirements as the original system.

l. The staff concerned should be ready to intervene rapidly according to a procedure drawn up by the competent electoral authorities.

i. Those responsible for operating the equipment should draw up a contingency procedure.

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

Guidelines 40j, 40k and 40l: An electronic voting system needs formalised procedures for monitoring its security and reliability and dealing with problems, and adequate resources for troubleshooting the infrastructure.

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

m. Any data retained after the election or referendum period should be stored securely.

All election or referendum data that must 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, optical media such as DVD or microfiche, USB memory key and printout) and they should be stored in different locations.

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.

a. Appointed persons shall have restricted access to e-voting services, depending on their user identity or their user role. User authentication should be effective before any action can be carried out. Separation of duties should be clear and strictly enforced through technical measures.

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

c. Any other critical technical activity should be carried out by teams of at least two people. The composition of the teams should be regularly changed. As far as possible, such activities should be carried out outside election periods. They should be the subject of a report.

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

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

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.

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

a. Formal procedures should be developed for the deployment of software and voting technology configurations. Deadlines for updates should be established. Updates that are distributed should be authenticated (signed).

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

a. The private cryptographic keys be should be generated at a public meeting and should be divided in separate parts and shared by at least two people who are unlikely to collude.

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.

a. The types of incidents are specified in advance by the electoral authorities.

b. In case of an incident, competent electoral authorities should take the necessary steps to mitigate the effects of the incident.

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.

a. Printing of voter identification data such as polling cards should be reviewed to ensure security of sensitive data.

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

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

In an internet voting context, the expression "within prescribed time limits" refers to the time limit where the internet voting channel closes. This can be implemented by using time marks or a confirmation of a trustworthy system. A time mark attached to the vote should not, however, be used to reveal the vote.

APPENDIX

Definitions

In these guidelines 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 at least two 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 third parties;
- 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 affects, 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 the Appendix I to Recommendation CM/Rec(2017)5;
- 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).