COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MINISTERS' DEPUTIES | CM Documents | CM(2017)50-add1final | 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)

a. Explanatory Memorandum to Recommendation CM/Rec(2017)5 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.

Background

1. The present Recommendation on standards for e-voting and explanatory memorandum are the updated version of the "Recommendation Rec(2004)11 of the Committee of Ministers to member States on legal, operational and technical standards for e-voting" and its explanatory memorandum which were adopted on 30 September 2004. In 2010 two complementary documents were approved: the "Guidelines for developing processes that confirm compliance with prescribed requirements and standards in the region (Certification of e-voting systems)" and the "Guidelines on transparency of e-enabled elections".

2. The Recommendation Rec(2004)11 and the accompanying Guidelines have served as legal benchmarks to countries and institutions in the region when introducing, operating and evaluating e-voting systems. Following the conclusions of the 2012 and 2014 biannual review meetings of Rec(2004)11 and of an experts' meeting held in Vienna in December 2013, the Committee of Ministers decided on 1 April 2015, under Article 17 of the Statute of the Council of Europe and in accordance with Resolution CM/Res(2011)24 on intergovernmental committees and subordinate bodies, to set up an "Ad hoc committee of experts on legal, operational and technical standards for e-voting" (CAHVE).

3. CAHVE's mandate was to prepare a new Recommendation updating Rec(2004)11 and its explanatory memorandum in the light of recent technical and legal developments related to e-enabled elections in the Council of Europe member States. The update should consist in enhancing and further developing the existing Recommendation Rec(2004)11. Work should focus on redressing the identified flaws of the Recommendation, taking advantage of recent experiences with e-voting in the region and addressing the implications of emerging technical concepts and solutions. The updating process should be guided by a needs assessment, taking particular account of the views of member States and of non-governmental stakeholders. Based on its mandate CAHVE produced the following documents: Recommendation Rec(2017)XX on standards for e-voting revising and replacing Recommendation Rec(2004)11 on legal, operational and technical standards and the present explanatory memorandum. In addition to its mandate, CAHVE has prepared "Guidelines on the implementation of the provisions of Recommendation Rec(2017)XX on standards for e-voting".

4. The present Recommendation contains standards on e-voting which reflect and apply the principles of democratic elections and referendums to e-voting. Standards aim at guaranteeing the respect of the principles when using e-voting, thus building trust and confidence in domestic e-voting schemes.

5. Principles of democratic elections and referendums stem from existing Council of Europe and other international instruments in the field of elections. Standards express objectives that e-voting shall fulfil to conform to the principles of democratic elections and referendums. The standards are common to the Council of Europe region.

6. The competence of the member States of the Council of Europe in electoral matters and regarding referendums is not affected by this Recommendation. The Recommendation covers the use of e-voting in political elections and referendums. Political elections and referendums are held at different levels. In some countries no referendums are held. The standards apply in the same way whether e-voting is used in political elections or in political referendums.

7. The reasons for introducing or considering the introduction of e-voting differ from country to country and depend on the specific domestic context. It has become clear that an e-voting system can only be introduced if voters have trust and confidence in their electoral system and in election administration. The present Recommendation does not require member States to introduce e-voting. It observes that an increasing number of countries do currently make some use of e-voting or envisage to do so in the near future. The Recommendation introduces standards which aim at harmonizing the implementation of the principles of democratic elections and referendums when e-voting is used in member States.

8. In the present Recommendation, the term e-voting refers to the use of electronic means for voting and counting purposes, in controlled and uncontrolled environments. It covers e-voting machines in polling stations, the use of optical scanners to register and/or count paper ballots as well as remote e-voting. Unless specific mention, standards apply to all forms of e-voting. Standards which are specific only to one or to some forms do mention this. Detailed implementation provisions, often specific to one form of e-voting, are included in the "Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting".

9. Electoral systems may include both non-remote and remote forms of voting. Remote voting can be conducted in both controlled (e.g. voting at embassies or consulates, voting at post offices or municipal offices) and uncontrolled (i.e. unsupervised by officials) environments (e.g. voting from home via postal mail or voting from a private computer via the internet). Each member State has its own established practice concerning the types of voting channels available to voters.[1] For the purpose of this Recommendation remote e-voting means the use of electronic means to cast the vote outside the premises where voting takes place in general.

10. The Recommendation addresses relevant aspects of e-voting relating to the different stages of elections and referendums, namely the pre-voting stage, the casting of the vote, and the post-voting stage, as well as to the roles and responsibilities of different stakeholders. The standards included here are applicable to the use of e-voting as defined in this Recommendation. Annex systems, which relate to e-voting but are not, technically speaking, part of it, such as voter registration systems for instance, require specific regulations. The present standards for e-voting may inspire such regulations. Member States contemplating the introduction of e-voting may also consider the Council of Europe e-voting Handbook “Key steps in the implementation of e-enabled elections” (2010), which provides assistance and guidance with this respect.

11. Detailed guidelines for the implementation of the objectives (expressed in the standards) are to be found in the new "Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting" that accompanies the present Recommendation. The new Guidelines include an updated version of the provisions of this level from the old Recommendation Rec(2004)11 and from the two Guidelines associated to it, namely the "Guidelines for developing processes that confirm compliance with prescribed requirements and standards in the region (Certification of e-voting systems)" and the "Guidelines on transparency of e-enabled elections". The new Guidelines replace both previous Guidelines.

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

12. The present version of the Guidelines needs to be completed through further work to address all forms and all aspects of e-voting covered by CM/Rec(2017)5 on standards for e-voting. Furthermore, due to ongoing developments in the legal and technical fields, the provisions included in the Guidelines need to be updated on a regular basis whereas the Recommendation is intended to provide a stable framework. The update of the Guidelines shall be considered and decided by member States at the periodic review meetings on the implementation of the present Recommendation.

Recommendations

13. Democracy is inconceivable without elections and referendums held in accordance with certain principles that lend them their democratic status. These principles represent a specific aspect of the "European constitutional heritage" also known as the "European electoral heritage". In 2002, the European Commission for Democracy through Law (Venice Commission) adopted the Code of Good Practice in Electoral Matters[2] which, albeit non-binding, is the reference document of the Council of Europe in the field, and defines the "European Electoral Heritage" through two aspects: the hard core constitutional principles of electoral law and certain basic conditions necessary for their application. The Code identifies the following principles: universal, equal, free, secret and direct suffrage and periodically held elections. The basic conditions are: rule of law, respect for fundamental rights, stability of electoral law and effective procedural guarantees.[3] All voting channels used in elections and referendums, including e-voting, must be designed and implemented in conformity with these principles and conditions.

14. In line with the 2002 Code of Good Practice in Electoral Matters, the meaning of the principles and conditions can be summarised as follows:

- *Universal suffrage:* all human beings have the right to vote and to stand for election subject to certain conditions, such as age or nationality;
- *Equal suffrage:* each voter has the same number of votes, each vote has the same weight and equality of opportunity has to be ensured;
- *Free suffrage:* the voter has the right to form and to express his/her opinion in a free manner, without any coercion or undue influence;
- *Secret suffrage:* the voter has the right to vote secretly as an individual, and the state has the duty to protect that right;
- *Direct suffrage:* the ballots cast by the voters directly determine the person(s) elected;
- *Frequency of elections:* elections must be held at regular intervals;
- *Respect for fundamental rights:* democratic elections require respect for human rights, such as freedom of expression, freedom of circulation, freedom of assembly, freedom of association;
- *Regulatory levels and stability of electoral law:* rules of electoral law must have at least the rank of a statute; rules on technical matters and detail may be included in regulations of the executive. The fundamental elements of electoral law should not be open to amendment less than one year before an election, or should be written in the constitution or at a level higher than ordinary law;
- *Procedural guarantees:* these include procedural safeguards aiming at ensuring the organisation of elections by an impartial body, the observation of elections by national and international observers, an effective system of appeal among others;
- *Electoral system:* within the respect of the above-mentioned principles, any electoral system may be chosen.

15. The standards included in the Appendix I to this Recommendation set objectives that e-voting shall fulfil to comply with the principles and conditions of the "European electoral heritage". However, not all the mentioned principles and conditions call for special attention and the setting of e-voting specific objectives. This is the case for instance with "periodically held elections" which does not require special attention when designing or implementing e-voting, if it's not for the obvious requirement that voting

---

[2] Code of good practice in electoral matters (CDL-AD(2002)023rev), endorsed by Parliamentary Assembly resolution 1320(2003) and CLRAE Resolution 148 (2003), subject of a Declaration by the Committee of Ministers (114th session, 13 May 2004).

[3] - Point 7 of the Document of the Copenhagen Meeting of the Conference on the Human Dimension of the OSCE of 29 June 1990 clearly speaks of free, universal, equal and secret suffrage - point 6 of direct suffrage, albeit in a qualified form
- Article 25(b) of the International Covenant on Civil and Political Rights expressly provides for all these principles except direct suffrage, although the latter is implied (Article 21 of the Universal Declaration of Human Rights).
- Article 3 of the Additional Protocol to the European Convention on Human Rights explicitly provides for the right to periodic elections by free and secret suffrage; the other principles have also been recognized in human rights case law (Universality: ECHR No. 9267 or81, judgment in Mathieu-Mohin and Clerfayt vs. Belgium, 2 March 1997, Series A vol. 113, p. 23; judgment in Gitonas and others vs. Greece, 1 July 1997, No. 18747 or91, 19376 or92; 19379 or92, 28208 or95 and 27755 or95, Collected Judgments and Decisions, 1997-IV, p. 1233; re. Equality: Aforementioned judgment in Mathieu-Mohin and Clerfayt, p. 23.) The right to direct elections has been admitted by the Strasbourg Court implicitly (ECHR No. 24833 or94, judgment in Matthews vs. The United Kingdom, 18 February 1999, Collected Judgments and Decisions 1999-I, para. 64.)

channels, including e-voting, should be ready to allow periodical elections to be held. The standards in this Recommendation address only those matters that were considered of specific relevance to e-voting.

Point I: recommendations *i* to *vi*

Recommendation i and ii*: Respect of the principles and risk policy*

16. E-voting, as any other voting method, must respect the principles for democratic elections and referendums. The rapid changes in its underlying technology present a challenge to such conformity as they introduce new opportunities and threats in an on-going manner. These must be managed appropriately. At the end, it is essential that the principles are not undermined by the introduction of electronically backed solutions in vote casting and/or counting procedures or by their evolution.

17. Accordingly, e-voting systems must be designed and operated in order to ensure constantly that the principles are respected. Member States should dedicate special attention to the risks inherent to the e-voting method chosen. E-voting specific risks need to be monitored permanently and appropriate countermeasures introduced whenever necessary. Given the rapid pace of change in the field of new technologies, member States are advised to introduce a risk management policy framework.

18. There may be exceptions to the principles; restrictions to the conditions for implementing the principles may apply. Furthermore, in an e-voting context, it may be necessary to have a stricter application of one principle and a looser application of another. These decisions are taken by the competent national authority (the Parliament, the supreme judge, the electoral management body or a governmental agency) and depend on the country's specific context. It is important that such decisions are taken in conformity with basic requirements such as being taken by the competent authority, having a basis in law, being of general interest, respecting proportionality, among others. The overall aim of democratic elections and referendums must be respected.

19. The principles for democratic elections to which the Recommendation refers are those of the European Electoral Heritage included in the Code of Good Practice in Electoral Matters of Venice Commission. They represent minimum requirements and apply throughout the region. A country may introduce additional principles or have a stricter interpretation of the principles included here. In such a case the e-voting will have to comply with principles and standards which are stricter than those of the present Recommendation.

Recommendation iii: Guidance by the Recommendation in reviewing domestic legislation, interconnection between Appendix I and the Guidelines

20. Respect for the principles is ensured in different ways and with different means depending on the voting channel and underlying technology. The standards included in Appendix I to the Recommendation translate the principles into concrete objectives. Guidance on how to implement the objectives is offered in the Guidelines. It is foreseen that the Guidelines will be completed and updated in the future on a regular basis so that they keep pace with practical experiences and the development of new technologies.

21. There exists a close relationship between the new Recommendation and the new Guidelines. Appendix I to the Recommendation contains high-level, hard core standards which express objectives that an e-voting system shall fulfil to respect the principles for democratic elections. Standards should be stable over time. Detailed provisions on how to implement the objectives (standards) are included in the Guidelines. They are based on experiences and developments in member States and on suggestions from academic research.

22. The Recommendation recommends member States, when introducing e-voting, to be guided in their relevant domestic legislation in the light of its provisions. Careful thought needs to be given to aspects of law other than those relating simply to the electronic equipment needed and its use. The extent of the review advisable will depend upon the existing laws of the member State in question. Examples include provisions specific to voting methods, criminal legislation relating to elections matters, data protection legislation or legislation on election observation.

23. Member States are recommended to take into consideration other modifications in legislation that may become necessary as a result of the introduction of e-voting.

Recommendations iv and v: Review of implementation and updating policy on the basis of shared experiences in the field

24. E-voting is a new and rapidly developing area. Standards and implementation guidelines need to keep abreast of legal and technical developments. In recognition of this, it is recommended that each member State keeps its own developments on e-voting under review, reports to the Council of Europe the results of such reviews and participates in the updating work of the Recommendation and of the Guidelines (see Point II). The Council will review the implementation of the Recommendation at least every two years after its adoption and the member States will share overall experiences in this field.

Recommendation vi: Translation and dissemination

25. The Recommendation and its accompanying Guidelines should be translated and disseminated by each member State in local language in order to inform the 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 adequately.

Point II: Update of the Guidelines

26. The Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting are a living document and should be up-dated regularly if legal, operational or technical developments make it necessary. The abovementioned review (para 24) would provide for an opportunity to assess such need.

Point III: Repealing of Rec(2004)11

27. The new CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting and the Guidelines on the implementation of the provisions of Recommendation CMRec(2017)5 shall repeal and replace the existing Recommendation Rec(2004)11 of the Committee of Ministers to member States on legal, operational and technical standards for e-voting and the "Guidelines for developing processes that confirm compliance with prescribed requirements and standards in the region (Certification of e-voting systems)" as well as the "Guidelines on transparency of e-enabled elections". This will avoid that any confusion subsist as to what principles, standards or Guidelines are henceforth applicable to e-voting in Council of Europe member States.

Standards

28. The Appendix I to the Recommendation contains a set of standards on e-voting which express objectives that e-voting must fulfil to conform to the principles of democratic elections and referendums. They represent minimum standards, which, if followed in an e-voting system, would facilitate compliance with the principles of democratic elections and referendums. However, compliance with these standards alone does not guarantee the democratic quality of the e-election or e-referendum. National legislation may contain additional requirements. The e-election or e-referendum has to be judged as a whole and in detail, in the specific context. But compliance with the standards is an important element in enhancing the democratic quality of the e-voting system.

Interpretative Definitions

29. Appendix II at the end of the document contains definitions of terms used throughout the Recommendation, its Appendix I and the present Explanatory Memorandum. The definitions should also be consulted when the Recommendation or parts of it are translated into other languages.

APPENDIX I: E-VOTING STANDARDS

UNIVERSAL SUFFRAGE

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

30. In order to respect universal suffrage, member States need to ensure that the voter interface of the e-voting system is understandable and useable by as many voters as possible. Ergonomics need to be considered when designing an e-voting interface to take account of the interaction between the interface and the voter. The aim is that the voter can use the system easily and is able to execute the instructions, including the security-related ones.

31. Consideration must be given to different user-related constraints linked to age, language, lifestyle, etc. Instructions provided to voters shall be clear, easy to understand and to follow by as many voters as possible.

Standard No. 2. "The e-voting systems shall be designed... "

32. Not all persons with disabilities may be able to use e-voting. The design of the e-voting system should, however, aim to maximise the potential of accessibility that this voting channel provides for them. In conjunction with other voting channels available, e-voting aims at enabling as many persons with disabilities and special needs as possible to vote independently.

33. At the implementation level, the responsible authority decides how to accommodate the needs of people with disabilities and special needs. For example, individuals with a visual impairment or with dyslexia may need screen reading devices, sharply contrasting text and backgrounds, as well as the possibility of adjusting the text size in their Web browsers or on voting machines. Users with communication impairments may prefer graphically presented information. Those with co-ordination impairments may prefer using a keyboard rather than a mouse. Voting interfaces need to be adapted to the needs of mobility impaired users.

34. User-friendly solutions for the disabled may be less resistant to e-voting security threats. This is the reason why it's up to the responsible authority to decide to develop and use them as far as practicable, meaning as far as an acceptable balance between usability and security is found.

Standard No. 3 "Unless channels of remote e-voting are universally accessible..."

35. Adding additional channels, namely e-voting, to traditional forms of voting may render elections and referendums more accessible and thus strengthen the principle of universality. However, offering the remote e-voting channel exclusively restricts accessibility, given the fact that the channel, namely internet, is not universally accessible for the time being. This provision aims at protecting the voter so that he or she is offered a means of voting which is effectively available to him or to her.

Standard No. 4 "Before casting a vote using a remote e-voting…"

36. When introducing totally new voting methods, especially remote e-voting, voters' attention shall be specifically drawn to the fact that this is an official channel used in a real election or referendum. The aim is to avoid that voters mistakenly imagine that they are taking part in a fake election or referendum or any other test. The same communication effort should be made when using a demonstration or test version, to avoid that voters get the impression that they have already voted. Furthermore, an election or referendum should be clearly distinguished from opinion polls and vice-versa.

EQUAL SUFFRAGE

Standard No. 5 "All official voting information shall be presented..."

37. All official voting information, in particular voting options, shall be presented in an equal way on the different channels. This implies equality of content. Measures should be introduced that prevent both the omission of information that should appear on the electronic ballot and the introduction of any additional information which does not appear on the official ballot, as foreseen by the law.

38. This also implies that there shall be equality with respect to the way information is displayed. However complete equality of display may be difficult or impossible to achieve as different supports (for instance mobile phone, digital TV, e-voting machines or PC) display the information in different ways on their screens. In such a case, it should be recognized that this is not a purely technical matter and should not be left to technical personnel alone to decide. The electoral management body should provide guidance on this matter.

Standard No. 6 "Where electronic and non-electronic voting channels are used..."

39. E-votes are first decrypted and counted. Then the results are aggregated with those obtained from paper votes and the final result is calculated. To do so an aggregation method, probably software, is needed. It must fulfil the same security and reliability objectives as the e-voting software.

40. When the number of e-votes or of paper votes is particularly small there is the risk that vote secrecy may be violated if the results of those few votes are disclosed. The aggregation method should contain the necessary technical and procedural safeguards to ensure consolidation of results of the different voting channels before results are disclosed, thus ensuring secrecy. In addition, procedural rules, related namely to personnel intervening in the counting process, should take into account such cases.

Standard No. 7 "Unique identification of voters..."

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

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

Standard No. 8 "The e-voting system shall only grant a user access..."

43. In cases where anonymous voting tokens prove that a voter is eligible to vote, identification of the voter may not be required at this point as it has already taken place at an earlier stage, namely when the specific token is assigned to a specific voter.

Standard No. 9 "The e-voting system shall ensure that only the appropriate number of votes..."

44. All votes cast by either electronic or non-electronic voting channels are counted. It should be ensured that only eligible voters' votes are included in the election result. The principle "one person one vote" shall be respected and only the appropriate number of votes, as foreseen in legislation, is included per voter.

FREE SUFFRAGE

Standard No. 10 "The voter's intention shall not be affected..."

45. The voting system must not influence the eligible voter's intention. The personal exercise of the right to vote is a fundamental principle. As it is vulnerable particularly in the context of remote e-voting, special attention is drawn to this fact. This standard does not prohibit remote e-voting, however adequate provisions should be introduced at the regulatory and implementation levels to ensure that personal and free suffrage is respected. The same is true for non-remote e-voting.

46. In a remote e-voting context, aspects to be considered are the possible faking of an official server by tampering with the domain name system (DNS), the use of a similar domain name to that of the official e-voting server, man-in-the-middle attacks, or malware in the voter's system that replaces the original ballot or submits counterfeit ballots.

47. Depending on national legislation and policies and in order to ensure accessibility, the principle of universality may be given priority over the principle of personal suffrage and therefore, for example, proxy voting may be allowed. The same conditions apply also to the e-voting channel. However, here again, the rules and conditions for allowing proxy voting shall be respected.

48. Electronic signatures, verifiability codes or other techniques applied to the ballot may allow verifying that the vote has not been tempered with. The use of such techniques shall, however, respect the confidentiality of the vote. At the same time, it should be clearly regulated how to proceed in case the verification shows that the vote has been tampered with.

Standard No. 11 "It shall be ensured that the e-voting system presents an authentic ballot..."

49. In addition to the techniques foreseen under standards 5 and 10, standard 11 requires procedural steps to be introduced to make sure that all information entered in the e-voting and presented to the voter through the e-voting interface is authentic, namely identical to the one provided by the competent authority.

Standard No. 12 "The way in which voters are guided through..."

50. During the voting process, it is important that decisions cannot be taken by inadvertently pressing a button or a link but truly reflect the will of the voter. In particular where e-voting takes place from an uncontrolled environment, the voter should be reminded at the beginning of the process that he or she is participating in a real vote. Throughout the process, both in controlled and uncontrolled forms of e-voting, the voter should be left with enough time to think and react so that he or she is not obliged to vote without reflecting on the choices he or she enters. The design of the interface, messages to the voter and any other relevant aspect should be programmed so as to allow the voter to express his or her true will. At the end of the voting process the voter's choices are summarized and the voter is asked to confirm that the summary reflects his or her true will. Only after this, the vote is sent to the voting server or entered in the electronic ballot box. The detailed implementation of this provision may however vary depending on the specificities of the e-voting system used.

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

51. With paper-based voting systems voters are enabled to participate in the election and yet not to express a preference for the proposed choices. The standard provides that this possibility has to be maintained with e-voting.

52. This standard does not influence the legal validity and effects of a blank vote or of an intentional invalid vote. These issues are regulated at the national level. Countries decide for instance if such votes are accepted, how (if) they are counted or what is their legal effect on the result. It is a matter for each member State to decide whether such options must be allowed with e-voting as well. Where the "blank vote" option is already foreseen on the paper ballot, it is sufficient if this option is also present on the e-vote ballot. This standard simply forbids a system where a voter is obliged to select one choice (other than blank) in order to complete the voting process. As such, it intends to provide the same guarantees than paper-based systems, where a voter does have the choice not to choose any proposed candidate for instance.

Standard No. 14 "The e-voting system shall advise the voter..."

53. As explained in the previous paragraphs, this Recommendation does not prevent member States from introducing other voting options such as the possibility intentionally to cast an invalid vote. Furthermore, intentionally valid votes may, under specific circumstances, be invalidated namely due to technical complications without the voter necessarily being aware of this fact. The present standard does not require that the invalid voting possibility is introduced as a voting option. It only requires that, whenever an invalid vote is received by the e-voting system, for whatever reason, the voter that issued that vote shall be informed accordingly. The aim is to avoid unintentional invalid e-votes. It applies in all cases, whether the e-voting system allows or disallows invalid votes. Of course, it only applies to votes cast electronically.

54. When advising the voter that his or her vote is invalid, the system should also inform him or her on the consequences of such invalidity (is it considered or not, etc.) as well as the possibility to cast a new vote if the invalidity is unintentional. If a system does not accept invalid votes, the ballot may be refused, or taken and discarded. If the system accepts invalid votes, it will be accepted pending reaction of the voter: if the invalidity is unintentional, the voter may want to cast a new vote; otherwise he or she has issued an intentionally invalid vote and maintains that choice. A lot depends in this case on the national regulation of invalid votes. The advantage of an e-voting system is that it is possible to inform and for the voter to react to such invalidity when it does not reflect his or her true will.

Standard No. 15 "The voter shall be able to verify that..."

55. Standards 15 to 18 introduce verifiability mechanisms which develop the concept of chain of trust in e-enabled elections. Standard 15 refers to verifiability tools which enable the voter to verify that his or her e-vote was cast as intended and recorded as cast, also known as individual verifiability. Individual verifiability tools vary depending on the specific e-voting solution. The voter verifiable paper audit trail produced by an e-voting machine used in a polling station or the return codes used in internet voting are examples of such tools.

56. Standard 16 is about confirmation by the system that the voting procedure was completed successfully. Standard 17 refers to verifiability tools which allow any interested person to verify that votes are counted as recorded (universal verifiability) and standard 18 provides that it is possible to verify that only eligible voters' votes were included in the final result, thus completing the chain of trust.

Standard No. 16 "The voter shall receive confirmation..."

57. The voting procedure is completed successfully when the electronic vote is deposited in the electronic ballot box. In the context of remote e-voting this means that the voting procedure is completed successfully only when the vote has been sent from the voter's voting device (PC, telephone, etc.), over the internet or another network and has reached its destination, i.e. the ballot box server.

58. The system confirms to the voter that his or her vote is deposited in the ballot box and will be counted and that the voting process is completed successfully. From the moment the voter learns this, he or she can safely log out or break the connection. Both messages on the successful casting of the ballot and on the completion of the procedure can be combined into one message, if the two events coincide. It is good practice to accompany these messages with a reminder and instructions to the voter on how to delete traces of the vote if voting was done from an uncontrolled device.

Standard No. 17 " The e-voting system shall provide sound evidence that each authentic vote..."

59. The voting system ensures that each vote is correctly included in the election result. This requires the ability to provide sound evidence to voters and third parties that the results are a true and accurate representation of the authentic votes cast and meet the legal requirements of democratic elections and referendums. "Sound evidence" refers to criteria for such evidence to be broadly accepted. "Authentic votes" refers to previously mentioned standards which make sure that the vote reflects the free will of the voter.

60. Furthermore, it should be possible to audit the evidence to verify its correctness with tools which are external to and independent from the e-voting system. To do so, the e-voting system should provide interfaces with comprehensive observation and auditing possibilities, subject to the needs of secrecy and anonymity of the vote.

61. The percentage of votes cast by e-voting and the comparison of the results of e-voting versus the results of voting by other channels can be considered to establish the plausibility of the correctness of the e-voting results.

Standard No. 18 "The system shall provide sound evidence that only eligible voters'..."

62. Voters and third parties should be able to check that only eligible voters' votes are included in the election result. At the same time counted votes should be anonymous. In the case of internet voting, there exist encryption methods that do not require decoding before votes are counted (homomorphic encryption). Counting can be performed without disclosing the content of encrypted votes.

SECRET SUFFRAGE

Standard No. 19 "E-voting shall be organised in such a way..."

63. This standard sets the general requirement of secrecy of the vote which applies throughout the entire procedure: in the pre-voting stage (e.g. transmitting of PINs, or electronic tokens to voters), during the completion of the ballot paper, the casting and transmission of the ballot and during counting and any recounting of the votes.

64. The necessary measures include of course encryption, but also, for example, that the votes cast are mixed in the electronic ballot box so that the order in which they appear at the counting phase does not allow reconstruction of the order in which they arrived.

Standard No. 20 "The e-voting system shall process and store..."

65. The voting system shall only process and store the personal data without which the system does not operate correctly. This requirement, also called "data minimisation", refers to data necessary for fulfilling legal requirements of the voting process. The electoral management body in charge of organising e-voting identifies such data and should be able to explain what are the underlying legal provisions and considerations that render them necessary. The duration of processing, storing etc. also depends on legal requirements, namely those related to appeals. Data minimisation aims at ensuring data protection and is part of vote secrecy.

Standard No. 21 "The e-voting system and any authorised party..."

66. Domestic legislation may foresee different ways of identification and authentication for different voting channels (indication of the voter's name, showing of an ID-Card, use of codes which are specific to each voter, etc.). The overall aim is to ensure that only people with the right to vote can effectively vote and to prevent multiple votes or other misuse.

67. The standard implies that the system itself and any authorised party do at some point handle authentication information. An example of authorised party is the entity that prints the voting material which contains authentication information. The system and any authorised party should protect this information through technical and organisational means. Anyone else, by definition unauthorised party, should not access or otherwise use this data.

68. Other services, such as information services for the voter prior to entering the voting process, which clearly do not need authentication, are outside the scope of this standard.

Standard No. 22 "Voters' registers stored in or communicated by the e-voting system..."

69. This standard provides that only authorised parties have access specifically to voters' registers.

Standard No. 23 "An e-voting system shall not provide the voter..."

70. The aim of this standard is to prevent the breach of vote secrecy as well as vote selling. However, individual verifiability can be implemented provided adequate safeguards exist to prevent coercion or vote-buying.

71. Provisions that handle cases of breach of vote secrecy or vote selling should be in place. In many countries criminal law provisions deal with such violations. They cover all voting channels used and should apply also when e-voting is used. If necessary they should be updated to take into account e-voting specificities.

72. Where paper proof of the content of the vote is produced, as this happens in controlled environments where electronic voting machines are used, technical and organisational measures should be in place that prevent the voter from making any use of that proof other than the normal use foreseen during the voting process. The voter cannot for instance use the proof to breach vote secrecy or take it with him or her outside the supervised place.

73. In a remote e-voting system using the internet, the voter should be informed on the necessity to delete traces of the voting transaction from the device used to cast the vote and on how to do so. Such traces could be kept for instance in the personal computer's memory, the browser cache, the video memory, swap files, temporary files, etc.

74. Specific attention should be paid to the way in which the anonymity and secrecy of the vote are implemented when designing an e-voting system. With respect to remote e-voting, there are at least three layers to be considered: the web application, the browser and the utility software on the computer of the voter.

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

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

c. Pieces of software that can record in some way what actions a specific user of a computer has performed have to be accounted for. Three common examples are screen shot utilities, utilities that make films of the sequence of screens and utilities that record the key strokes a user makes. Such software can be present as malware in the user's computer, without the user's knowledge. The e-voting system may not be able to prevent the presence of such malware. The voter should be informed about the possibility of such malware, the potential risks they present, the good practice to be adopted by him or her to minimize the risks and, more generally, about alternative and more secure voting channels that are open to him or her.

Standard No. 24 "The e-voting system shall not allow the disclosure..."

75. This standard aims at preventing the establishing and publication of intermediary results of the e-voting channel. Information about participation levels falls outside the scope of this standard and can be collected and released as foreseen by national regulations.

Standard No. 25 "E-voting shall ensure that the secrecy of previous choices..."

76. This standard requires that the secrecy of previous choices which were entered and then deleted by the voter during the voting process shall receive the same protection as the secrecy of the final vote.

Standard No. 26 "The e-voting process, in particular the counting stage..."

77. This standard provides that it must not be possible to link the vote to the voter who cast it and thus prevents vote secrecy breaching.

78. In non-remote e-voting processes the voter authentication and the vote can be separated physically also when e-voting systems are used. This physical separation can, in principle be controlled by election officials and election observers, assuming that there is deliberate or inadvertent error in the e-voting system (and no malware).

79. In the remote voting process, information linked to the voter (usually a code) and the votes are connected up to a certain stage. In countries that allow multiple voting, this link is necessary to handle multiple votes and their effect (a vote erases another). The separation has to be made electronically at a predefined stage before counting takes place. This requires specific technical solutions.

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

81. An audit system should maintain voter anonymity at all times, except when specifically required otherwise under domestic legal provisions. In all cases the information gathered by the audit system has to be protected against unauthorised access.

REGULATORY AND ORGANISATIONAL REQUIREMENTS

Standard No. 27 "Member States that introduce e-voting..."

82. Electronic voting technologies should be introduced in a gradual, step-by-step manner and tested under realistic conditions prior to Election Day. According to member States' experience, the gradual introduction is necessary given the legal and technical challenges and opportunities that e-voting presents. Some of the main steps are described in the guidelines related to this standard.

83. In particular, other forms of remote voting such as postal (correspondence) voting, should be well established and trusted before introducing remote e-voting. Many operational and user-confidence issues related to remote e-voting are similar to those related to postal voting and can be more easily addressed in the context of postal voting.

Standard No. 28 "Before introducing e-voting, member States..."

84. While this standard may look obvious at first sight, the aim is to call member States' attention to the fact that in addition to regulating the details of e-voting, they may need to change the law or even the constitution to allow for e-voting. Existing legislation is not written with automation in mind and may be ambiguous when applied to e-voting.

85. Another lesson learned from experiences in the region is that e-voting specific regulations need to be detailed to allow any stakeholder concerned to understand e-voting and to conduct his or her own functions in relation to it. Detailed regulations are furthermore important to guarantee that the implementation of technology complies with the principles for democratic elections and referendums.

86. The legal framework should provide for judicial review of e-voting which allows citizens to challenge the actual method used for e-voting, as well as the implementation of the method, thus increasing public confidence and trust in e-voting.

Standard No. 29 "The relevant legislation shall regulate the responsibilities..."

87. There are numerous stakeholders that play a role and bear some degree of responsibility in developing, testing, certifying, deploying, applying, maintaining, observing and auditing e-voting systems. Ultimately, however, it is the government that bears the overall responsibility for the voting and

thus for the e-voting system. It is recommended that the relevant legislation provides for the supervisory role of the electoral management body over e-voting. The role and the responsibilities of the other parties involved should be clarified at the appropriate regulatory or contractual level.

88. One aspect which will help make sure that the electoral management body has effective control over e-voting is for member States not to be over dependent on just a few vendors since this could result in a vendor-lock-in. Indeed, software and hardware of an e-voting system require ongoing maintenance. This is in addition to the procedures required for a specific event, for example the creation of ballot papers. When considering outsourcing, it is essential that those who are responsible for the elections understand what is being outsourced, why it is being outsourced and what methods and processes the vendor intends to undertake. Statutory duties of the body responsible for the conduct of elections must never be outsourced, since this body is in charge of the election.

Standard No. 30 "Any observer shall be able to observe the count of the votes. The electoral management body shall be responsible for the counting process."

89. The aim of this standard is to underline the role of the electoral management body in the counting process, not only as one of the participants but as the organiser and supervisor of the counting. The presence of observers should be provided for. Such observers should include representatives of political parties as well as the general public.

TRANSPARENCY AND OBSERVATION

Standard No. 31 "Member States shall be transparent in all..."

90. An e-voting system can only be introduced if voters have trust and confidence in their electoral system and in election administration. However, trust should not be taken for granted and states need to do their utmost in order to ensure that it is preserved. Fostering transparent practices in member States is a key element for building public trust and confidence. Being transparent about the e-voting system, the processes surrounding it and the reasons for introducing e-voting will contribute to voters' knowledge and understanding, thereby generating trust and public confidence.

91. This standard provides for broad transparency on all aspects of all forms of e-voting. In particular system's transparency, or the possibility to check that it is functioning properly, must be guaranteed. Member States regulate who has access to what and when and under what circumstances.

92. Transparency can furthermore be achieved by being open about the e-voting procedure. In addition to the electronic voting system, member States should also ensure transparency regarding all procedures (before, during and after Election Day/period) related to e-voting. This can be done by publishing illustrations (e.g. photos, videos, etc.) on the official website that explain e-voting to all interested parties. The use of sign language and subtitles should also be included to further reduce barriers when communicating on e-voting.

93. Representatives of people with disabilities should be involved in the process of introducing e-enabled elections so as to see how this could affect the people they represent.

Standard No. 32 "The public, in particular voters, shall be informed..."

94. An e-election can differ from an election or referendum without e-voting, namely 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 communicated to the voter in order to avoid any misunderstanding of the procedures and in order to give the voter all the information necessary on the use of the e-voting channel. Careful consideration should be given to deciding how much time the voter needs for this decision. Consideration should also be given to offering the voter the opportunity to try the suitability of his or her equipment before he or she decides to use a specific electronic voting channel.

Standard No. 33 "The components of the e-voting system shall be disclosed..."

95. Assessment that e-voting systems function correctly and that security is maintained is essential. The means to achieve this is the independent evaluation or certification of the system as a whole or of its components, which requires disclosure of the critical system elements. The assessment can be accomplished for instance by disclosing the system design, by allowing inspection of the detailed documentation, by disclosing the source code, by allowing inspection of component evaluation and certification reports, in-depth penetration testing, etc. The actual level of disclosure of the elements of the system, necessary for achieving appropriate assurance, depends on the peculiarities of the system, its components and the services provided.

Standard No. 34 "Any observer, to the extent permitted by law, shall be enabled..."

96. Although the availability of documents to the public is important, it will not be possible for everybody to understand an e-voting system. In order to have confidence, voters rely on others who are in a position to understand the materials and the processes. It is therefore essential that observers have as much access as possible to relevant documents, meetings, activities etc.

97. There are various international and domestic election observations. Observers should include representatives of candidates and political parties as well as the general public, both domestic and international independent observers. All member States are bound to the commitments of the Document of the Copenhagen Meeting of the Conference on the Human Dimension of the OSCE of 29 June 1990 to "invite observers from any other OSCE participating state and any appropriate private institution and organisation who may wish to do so to observe the course of their national election proceedings [… and …] facilitate similar access for election proceedings held below the national level." Procedures for accepting observers, as well as rights and obligations of observers are defined by the respective country's legislation and should respect the international commitments of the country.

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

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

Standard No. 35 "Open standards shall be used to enable various technical..."

100. In order to be able to use e-voting systems or services from different suppliers, these must be interoperable. Interoperability means that the input and output conform to open standards and especially open standards for e-voting. Such standards need to be updated on a regular basis to take account of legal and technical developments.

101. The main benefits of using open standards are:

- Greater choice of products and suppliers
- Less dependency on a single supplier
- Avoidance of proprietary lock-in
- Stability or reduction in costs
- Easier accommodation of future changes

102. Countries, in particular decentralised ones with a variety of states/members and thus a variety of electoral practices, may decide to adopt such standards at the country level.[4] At the regional level, countries may decide to adopt regional standards.

103. At the international level, OASIS, the International e-Business interoperability consortium, developed standards for election and voter services information using XML. OASIS elaborated the Election Markup Language (EML). EML is a set of data and message definitions described as XML schemas. It was the first international standard for the structured interchange of data among hardware, software, and service providers who engage in any aspect of providing election or voter services. Its function is to ensure open, secure, standardised and interoperable interfaces between the components of election systems. Further information on OASIS work on elections (which ended mid 2015) is available at http://www.oasis-open.org/committees/election

ACCOUNTABILITY

Standard No. 36 "Member States shall develop technical, evaluation..."

104. Election management bodies or the entity designated by them should develop technical requirements for e-voting systems. They should furthermore develop requirements for evaluation techniques ranging from testing to formal certification of e-voting systems. Common Criteria Protection Profiles and Common Criteria CC/ISO 15408 contain such kind of requirements.

105. Both types of requirement aim at ensuring, already before the effective use of the e-voting system in an election or referendum, that the system is designed in conformity with requirements for democratic elections and that it operates correctly, namely does exactly what it is supposed to do.

106. It's up to the election management body or the designated entity to make sure that all mentioned requirements fully reflect the relevant legal principles for democratic elections. This implies that requirements are updated as often as necessary to integrate possible legal developments. For example, the organisational rules of a type of election may change over time: so should also the respective requirements that translate such rules into technical instructions for the system or for its certification.

Standard No. 37 "Before an e-voting system is introduced and at appropriate..."

107. An appropriate control of an e-voting system provides evidence as to the compatibility of the system with technical requirements which, as mentioned in the previous provision, are derived from, and aim at implementing principles for democratic elections. The added value of such a control is not only to establish if an e-voting system is in compliance with the prescribed requirements and standards; it is also an important tool in the establishment of trust on the e-voting system.

108. The election management body must ensure that the e-voting system complies with technical requirements. To do so, it should charge an independent and competent body to evaluate the system. The notion of an independent body covers both independence from the system manufacturer or service provider and independence from political interference.

109. The independent body may be a governmental one, such as an agency in charge of national IT security certification. It may be a private (national or international) organisation such as evaluation laboratories or certification bodies (for instance those that are accredited for the national or international evaluation schemes such as BS7799/ISO17799, Common Criteria, or ITSEC). Whichever the case, such a body should be competent to conduct the certification work, in addition to being independent from the manufacturer/service provider and from political interference. Furthermore, its designation (as a certification body) should be transparent.

110. Certification or any other appropriate control is done before the e-voting system is introduced and at appropriate intervals whenever necessary, namely after important changes in the system. Certification can be applied in different ways. Member States may choose for instance to certify the whole system or

[4] This is the case for instance in Switzerland, where standards have been introduced by eCH, the e-Government standards setting association. Further information on e-voting related standards is available www.ech.ch under *eCH Documents > nach Themenbereich > Politische Aktivitäten*.

only components of it, bearing in mind the need to ensure that the voting system and procedures should be able to respond to possible threats and risks and respect standards for democratic elections and referendums.

Standard No. 38 "The certificate, or any other appropriate document..."

111. Any appropriate document issued should make the evaluation process and the outcome transparent and reproducible for third parties especially those that have access to the system. Based on the certificate it should be possible to verify that the system used for the election is the one that was certified. Therefore the certificate should at least include (or refer to) the following information:

- Issuer;
- Validation period/ date/ conditions (e.g. non-disclosure agreement);
- Description of the purpose of the certificate. Does the certificate declare if the system is accessible, secure, usable, functionally correct, and to what extent;
- Description of the method of the certification process. What standards are used? What methods are used for testing and evaluating a system? How is source code reviewed? How are hardware components checked?;
- Description of the certified system. To ensure reproducibility for third parties this has to include digital fingerprints of software components, detailed specifications of firmware versions, hardware components, etc.;
- Outcome of the certification process;
- Comments about operational requirements or other preconditions;
- A digital fingerprint of the certificate or a similar system.

Standard No. 39 "The e-voting system shall be auditable..."

112. Auditing of the e-voting process, resources or infrastructure is a means to establish trust and confidence in the operation of the ICT system(s) used for e-voting. It requires integrity and authenticity of the audit information and of the deployed auditing systems.

113. Audits aim at detecting possible attacks on systems. Independent and extensive security monitoring, auditing, cross checking and reporting are a critical part of e-voting systems. E-voting systems should therefore have audit facilities for each of the main components (vote, count, etc.) and on different levels of the system: logical, application, technical.

114. Audit facilities on the logical level should report upon the use that is being made of the system. Audit facilities on the application level should give information on the activities that the system supports in order to enable reconstruction of the system's operation. Audit facilities on the technical level should provide information on the activities that the infrastructure that is being used supports. This varies from routine information on, for example, specific load information and system malfunction, to specific information on the signals an intrusion detection system (IDS) gives with regard to possible attacks.

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

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

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

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

119. The audit system should be able to detect voter fraud and provide proof that all counted votes are authentic. All occurrences of attempted voter fraud should be logged; the audit system logs should contain data that provides the ability to cross check credentials giving the right to vote and shall ensure that all counted votes were cast by a voter with a right to do so and that all authentic votes have been counted as such.

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

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

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

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

RELIABILITY AND SECURITY OF THE SYSTEM

Standard No. 40 "The electoral management body shall be responsible..."

124. In addition to being available and usable, the e-voting channel needs to be reliable and secure to comply with the principles for democratic elections. It is the member State who has to guarantee that this is the case. The overall responsibility falls on the electoral management body that supervises e-voting and cannot be delegated for instance to a voting system supplier.

125. Respect for the principles shall be ensured also in the presence of failures or attacks. This implies that the e-voting system shall be secure, i.e. robust as to withstand deliberate attack, and reliable, i.e. able to function on its own, irrespective of shortcomings in the hardware or software.

126. Technical solutions that reflect state of the art, are peer-reviewed and broadly endorsed by the respective scientific community help ensure availability, reliability, usability and security of the e-voting system even in the presence of failure and attacks.

Standard No. 41 "Only persons authorised by the electoral management body..."

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

Standard No. 42 "Before any e-election takes place, the electoral management body..."

128. Before any e-election takes place, the electoral management body shall satisfy itself that the e-voting system used is actually the system that is supposed to be used, that is, that the software is genuine (the same as the one previously checked and authorised for use) and operates correctly.

129. Verification should prevent any e-voting system being installed if the system or any of its components have been tampered with or have been replaced. The electoral management body needs to ensure that the correct system is put into service. Furthermore, the standard requires that the system operates correctly.

Standard No. 43 "A procedure shall be established for regularly..."

130. Constant development in information and communication technologies renders regular updates (particularly) of software necessary. This calls for updates to central systems and voting facilities used in a controlled environment (for example, voting machines). Any important update needs to be certified similar to the initial certification before being brought into operation.

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

Standard No. 44 "If stored or communicated outside controlled environments..."

132. From the moment the vote is cast, no one should be able to change it or relate the vote to the voter who cast it. This is achieved, among other measures, 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 by using encryption. 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.

133. To seal and protect an electronic ballot box, physical and technical measures may be necessary, such as control of access, authorisation structures and firewalls.

Standard No. 45 "Votes and voter information shall be kept sealed..."

134. This clarifies the moment where sealing ends: just before the counting. As mentioned elsewhere (and by analogy with the physical ballot box), before unsealing, votes are mixed.

Standard No. 46 "The electoral management body shall handle..."

135. This standard reminds that adequate, state of the art procedures must be foreseen for the handling of cryptographic material.

Standard No. 47 " Where incidents that could threaten the integrity of the system..."

136. It is important that incidents that threaten the integrity of the system are reported immediately to the competent entity in charge of communication which makes sure that the necessary measures are taken and all interested stakeholders, namely political parties and voters are properly informed.

Standard No. 48 "The authenticity, availability and integrity of the voters' registers..."

137. Data-origin authentication can for example be provided by electronic signatures in fully electronic processes. In semi-electronic processes, data-origin authentication may employ also conventional security measures, such as manual signatures, seals, couriers, etc.

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

Standard No. 49 "The e-voting system shall identify votes..."

139. Irregularities shall be identified so that the necessary measures are taken and stakeholders (voter, electoral management body, etc.) can be informed and are able to react accordingly.