DIRECTORATE GENERAL OF DEMOCRACY AND POLITICAL AFFAIRS

DIRECTORATE OF DEMOCRATIC INSTITUTIONS

PROJECT "GOOD GOVERNANCE IN THE INFORMATION SOCIETY"

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

GGIS (2010) 3 fin. E

Strasbourg, 16 February 2011

Certification of e-voting systems

Guidelines for developing processes that confirm compliance with prescribed requirements and standards

prepared by the Secretariat

Introduction

In 2004, the Committee of Ministers of the Council of Europe adopted Recommendation (2004)11 on legal, operational and technical standards for e-voting. Following this, Council of Europe member states agreed to hold biennial meetings in order to keep under review their policies and experience of e-voting since the adoption of the Recommendation. The first such meeting took place in Strasbourg in November 2006, the second one in Madrid, Spain, in October 2008, and the third one in Strasbourg in November 2010.

At the 2008 Biennial Review meeting the Secretariat was invited to investigate issues that could be examined in order to strengthen the implementation of the Recommendation. In particular, it was suggested that certain aspects of the Recommendation such as the certification of e-voting systems and the transparency of e-enabled elections required further consideration.

With this in mind, review work has been undertaken on the certification of e-voting systems and the present guidelines have been elaborated in the light of the findings and conclusions of the workshops on certification of e-voting systems held on 26 to 27 November 2009, 31 May to 1 June 2010 and 27 to 28 September 2010 at the Council of Europe in Strasbourg. They were considered and endorsed at the 3rd biennial intergovernmental meeting to review developments in the field of e-voting and the application of CM Recommendation (2004)11, held in Strasbourg on 16-17 November 2010. The present final version of the Guidelines takes into account the comments made at that meeting.

These guidelines provide a practical tool to facilitate the implementation of the 2004 Recommendation, in particular paragraphs 111 and 112 which recommend member states to introduce certification processes that allow for any IT component to be tested and certified as being in conformity with the technical requirements described.

In this document certification means a process of confirmation that an e-voting system is in compliance with prescribed requirements and standards and that it at least includes 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.

The added value of certification is not only to establish if an e-voting system is in compliance with prescribed requirements and standards, it is also an important tool in the establishment of trust. Certification can also be helpful in the context of public procurement.

The guidelines are developed for use in political elections and referendums at all tiers of governance. They are not intended to prescribe or to impose on any country a particular way of certification, but rather to provide member states with a tool to assess the requirements for a comprehensive certification process. The goal of this document is to support member states to improve their current processes, to exchange best practises and to gradually move towards a common framework.

Certification can be applied in different ways. Solutions chosen by a member state may include certification of a single e-voting system for nation-wide use, it can opt to certify multiple systems, provisionally certify an e-voting system, or only test one or several parts, i.e. component testing. Member states may choose those measures described in the present guidelines that correspond with their particular voting system, bearing in mind the need to ensure that the voting procedures respond to possible threats and risks while being in line with international commitments.

The Guidelines address relevant aspects relating to all stages of elections and referendums, i.e. 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. Not every government will use electronic means in all aspects of elections; hence these guidelines are applicable to those stages in which member states decided to use electronic means.

The guidelines laid out in this document are each followed by explanatory paragraphs. A glossary of relevant terms is provided in Appendix I and relevant extracts from Recommendation (2004)11 can be found in Appendix II. In order to visualise the certification process, a comprehensive theoretical model describing a possible formal certification process has been added in Appendix III.

Regulation and oversight

1. **Member states are responsible for the functioning of all e-voting systems used for statutory elections and referendums within their territory**

   There are numerous stakeholders that play a role and bear some degree of responsibility in developing, testing, certifying, deploying, applying, observing and auditing e-voting systems. Ultimately, however, from an electoral point of view, it is only the government that bears the overall responsibility for the e-voting system, including the certification thereof.

2. **Member states should establish the aims of certification and develop requirements for proper certification procedures and certification methods**

   When considering certification of non-remote or remote e-voting systems, the first step is to clearly clarify 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 about the conduct of the elections.

   Although a detailed list of requirements might seem at first glance to be a good option towards guaranteeing a correct certification analysis, such a tight legal framework might generate paradoxical effects. While auditors would be subject to a high level of supervision, the vendors might customise their products to the limited goal of simply fulfilling the prescribed requirements of a given electoral administration. If this is the case, the vendors may 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.

Clarifying the aims, the software, operating system, hardware and process requirements, as well as 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 system, hardware and processes.

Socio-political 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. Comprehensive and nuanced knowledge of the expectations of society and politicians, the effects of new voting channels on electoral behaviour and on political actors is required.

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

3. Member states should ascertain that all technical requirements fully reflect the relevant legal and democratic principles

In this context, two examples may be noted: The Common Criteria approach is based on a dialogue between users and vendors. The KORA (*Konkretisierung rechtlicher Anforderungen* or “concretisation of legal requirements”) approach[1] aims to improve and facilitate communication between legal and technical points of view. However, the law should not be changed solely to meet the requirements of a system designer.

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

Member states should develop and publish procedures in which it is defined who has access to which information and when. Specific attention needs to be given to the needs of domestic and international observers as well as 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. The non-disclosure of

[1] For more information, please refer to: http://www.uni-koblenz-landau.de/koblenz/fb4/institute/iwvi/aggrimm/projekte/modiwa (German only)

the certification report or part of it and of all relevant documents should only be considered in exceptional circumstances.

Special attention needs to 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. Non-Disclosure Agreements (NDA), 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. In this context, we can mention the "college of experts" in Belgium which is responsible for overseeing the entire electoral process for the competent legislative assembly.

5. Accredited election observers should have access to all steps of the certification process

In the past 20 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. So as 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 should be granted access to all relevant information during the entire duration of the certification process in order to accomplish their duty.

In 2005, the "Declaration of Principles for International Election Observation and Code of Conduct for International Election Observers"[2] established a common ground for election observation, which has been endorsed by all relevant international organisations in the field. These principles include the disclosure of the applied methodology.

[2] http://www.venice.coe.int/site/dynamics/N_Opinion_ef.asp?L=E&OID=325

Selection of certification bodies

6. **Member states should devise a clear framework for the institutional responsibilities, criteria and procedures for ascertaining the competence and independence of certification bodies**

   Any body that is being 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 regarding 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 the vendors and foster the electors' trust in the procedures. The number of certification bodies should not be limited; any body which 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 to hav the selection procedure carried out by professional auditors who hold international certificates. An example is CISA (Certified Information System Auditors), 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.

7. **The mandate of the certification body must 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 in regular intervals, and these tenders need to be public. It needs to be clear whether the decision to commission a system certification to a specific selected certification body may be taken by the vendor or whether this decision lies with the competent electoral authority.

Certification

8. **The bodies selected for certification processes are required to perform their task in accordance with prescribed and published rules and requirements**

   The certification procedures should be governed by clear rules and guidelines, including liability considerations, which should be published well in advance of an election. This form of quality control is needed in the process. Again, this will facilitate the task of the vendors and foster electors' trust.

Certification can include software, operating systems, hardware, processes and personnel, including usability, accessibility, data such as ballot papers and voting results, the interfaces between the e-voting system and other software, and document review. Steps to be included in the certification process should be the pre-electoral phase, voting, tallying, suitability of the legal framework for the application of e-voting, etc.

Specific responsibilities of certification bodies include the collection of sufficient objective evidence upon which to base the decision whether to award a certificate or not and a commitment to select competent and suitably trained auditors.

A particular challenge to certification occurs with remote electronic voting over the internet: The client software and hardware used during voting via the internet may remain outside of the certification boundaries. All stakeholders should be made aware of the potential risks of using client computers outside a controlled electoral environment and of possible remedies to redress this situation.

9. Member states may consider the use of standardised protocols, in particular in formal certification processes

While the previous guideline addresses certification in the broadest sense, this guideline deals specifically with formal certification.

Looking beyond some already known standards and recommendation, for example the relevant Constitution, the Code of Good Practice in Electoral Matters and the Code of Good Practice on Referendums by the Council of Europe's Venice Commission and the Committee of Ministers' Recommendation (2004) 11 on legal, operational and technical standards for e-voting, it is also important to decide which protocols should be used. Examples include: ISO 9001, ISO 9000-3, IT Grundschutz[3] (regarding operational environment protection and including ISO 27001), k-resilience value for inside threats[4], Content Management System and Common Criteria (ISO 15408).

While each of these protocols in itself can play a role in the certification process, a combination of them could prove to be more useful. For example, the scope of ISO 27001 only addresses procedural and organisational issues, and not the core of the system, that is to say, the software and similar components. ISO 27001 could therefore be combined with the Common Criteria methodology.

Although ISO certification can be very useful, it needs to be noted that ISO certification is limited in time. Consequences could be that the entire ISO certification

[3] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

[4] For more information on k-resilience and Common Criteria , please refer to www.coe.int/t/dgap/democracy/Source/EVoting/E-voting%202009/E-voting%20workshop/Volkamer_presentation.pdf

process will need to be repeated with each election, which could be a very costly procedure. Also this long procedure could be inconsistent with early elections which could specifically raise the problem of prohibitively high costs of the procedure.

10. Member states may consider to authorise certification bodies to find suitable ways of perusing and re-using existing material from certification processes performed previously

Member states could opt to re-use certificates or certification reports which have been issued by other bodies or by other countries. The re-use of this information can contribute to saving costs, time and resources, thereby making the certification process more efficient and effective. The re-use of information should satisfy at least the same standards of transparency as the original process.

Even if member states decide not to re-use certificates or certification reports, they may consider facilitating the exchange of experiences of certification processes with other countries.

11. The conclusions reached in a certification report should be entirely verifiable with the information contained in that report

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

12. Member states should determine the apportioning of costs entailed in the certification process, bearing in mind the need for its integrity, independence and quality

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 costs, including formal certification, be borne by the vendors, which could lead to a greater involvement by the latter. The costs could also be the responsibility of the member states 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 needs to be made public.

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

Bodies which are responsible for performing the certification should have access to information and data which is necessary and sufficient to perform their duties as to reach the conclusion about 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 have taken place only shortly before the elections proper. 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 budget is, once an initial certification process has been carried out and the e-voting component has been certified, for future certification only to certify the modified modules and the sequence of the modules. This can only be done if a difference is being made between major changes (modifications) and minor changes (minimis changes) to the e-voting system.

14. In case of formal certification, the certificate issued should clearly identify the subject of certification and should include safeguards to prevent its unnoticed modification

The certificate itself should make the certification process and the outcome transparent and reproducible for third parties especially if they 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 ;
- 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.

Appendix I

Glossary of terms
used in the Guidelines on the certification of e-voting systems

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

- 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.

- 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 at least includes 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 and to issue a certificate upon completion.

- Certification report: a document which explains what a certificate has certified and how it is certified.

- Component testing: a method by which individual units of the system code are tested to determine if they are fit for use.

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

- E-voting system: the hardware, software and processes which use electronic means to make a choice between options in an election or referendum.

- Formal certification: type of certification that is official and conducted only before the election day and leads to the issuance of a certificate.

- Guideline: any document that aims to streamline particular processes according to a set routine. By definition, following a guideline is 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.

- Requirement: a singular documented need of what a particular product or service should be or perform.

- Stakeholder: a person, group, organisation, or system who impacts on, or can be affected by, a government’s or organisation’s actions. These include citizens, election officials, political parties, governments, domestic and international observers, media, academics, (I)NGOs, anti-e-voting organisations and specific e-voting certification bodies.

- Standard: 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 subject works as expected.

- Transparency: the concept of determining how and why information is conveyed through various means.

Appendix II

Text of Recommendation 2004 (11) on Legal, operational and technical standards on e-voting

F. Certification

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

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

Text of explanatory memorandum of Recommendation 2004 (11) on Legal, operational and technical standards on e-voting

F. Certification

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

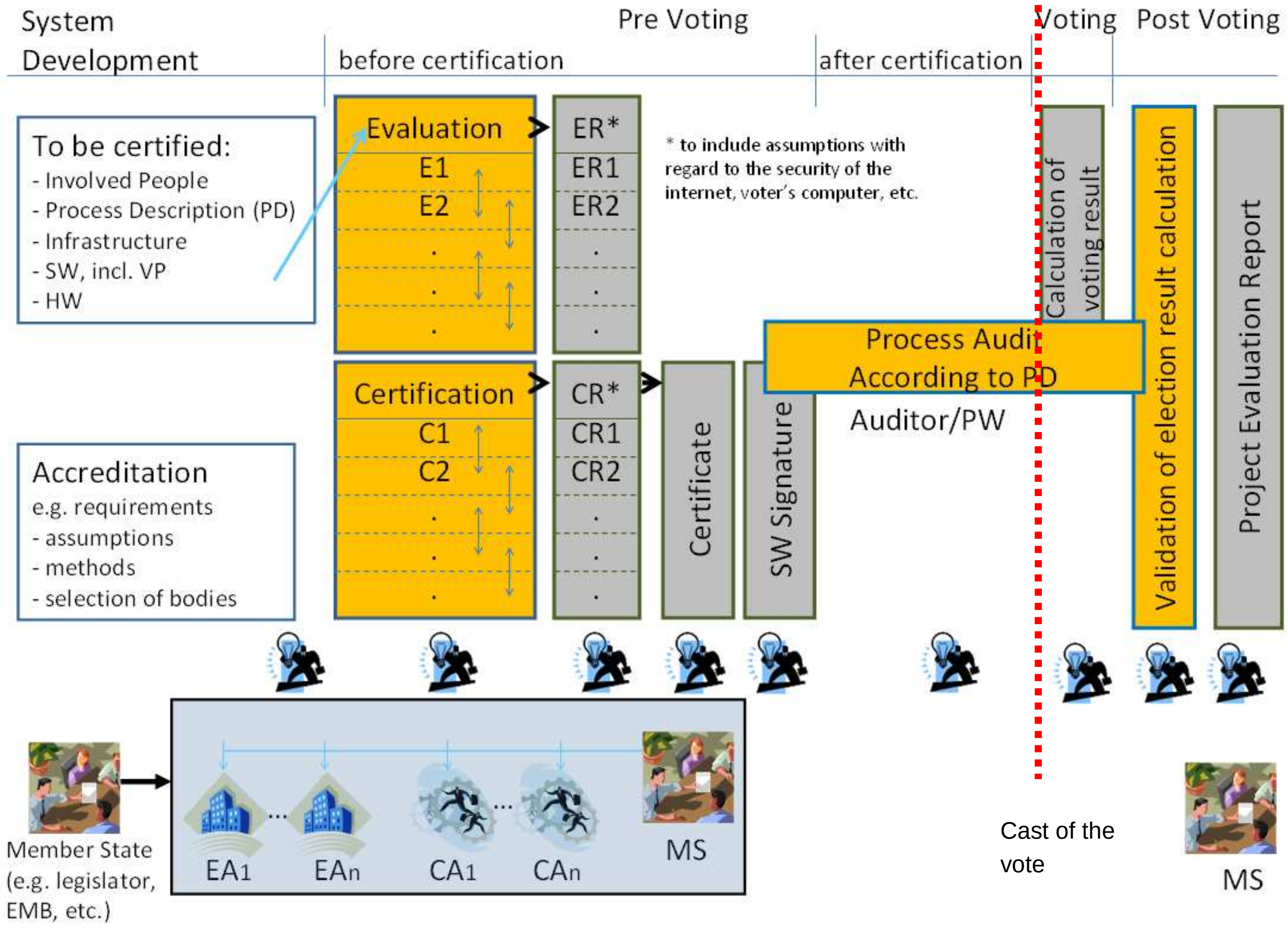
189. Election officials should consider the use of techniques ranging from testing to formal certification in order to ensure, before the election or referendum takes place, that the system does exactly what it is supposed to do.

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

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

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

Appendix III – Theoretical model of possible formal certification process



SW – Software
VP – Voting Protocol
HW – Hardware
D – Developer and Developing Process
EA – Evaluation Authority
EAx – xth Evaluation Authority
CA – Certification Authority
MS – Member State (e.g. legislator, Electoral Management Body, etc.)
E – Evaluation
Ex – xth Evaluation as different types of evaluation are required
ER – Evaluation Report
CR – Certification Report
PD – Process Description
PW – Poll Worker