

Gesellschaft für Informatik (GI)

publishes this series in order to make available to a broad public recent findings in informatics (i.e. computer science and information systems), to document conferences that are organized in cooperation with GI and to publish the annual GI Award dissertation.

Broken down into the fields of

- Seminar
- Proceedings
- Dissertations
- Thematics

current topics are dealt with from the fields of research and development, teaching and further training in theory and practice. The Editorial Committee uses an intensive review process in order to ensure the high level of the contributions.

The volumes are published in German or English

Information: <http://www.gi-ev.de/service/publikationen/lni/>

ISSN 1617-5468

ISBN 978-3-88579-225-3

The 2008 Conference on Electronic Voting took place in Castel Hofen near Bregenz at the wonderful Lake Constance from 6th to 9th August.

This volume contains 17 papers selected for the presentation at the conference out of more than 30 submissions. To assure a scientific quality, the selection was based on a strict and anonymous double-blind review process.



Robert Krimmer, Rüdiger Grimm (Eds.): Electronic Voting 2008

# GI-Edition

## Lecture Notes in Informatics

**Robert Krimmer, Rüdiger Grimm (Eds.)**

### 3<sup>rd</sup> international Conference on **Electronic Voting 2008**

**Co-organized by Council of Europe,  
Gesellschaft für Informatik and E-Voting.CC**

**August 6<sup>th</sup>- 9<sup>th</sup>, 2008**

**In Castle Hofen, Bregenz, Austria**

# The Certification of E-Voting Mechanisms. Fighting against Opacity

Jordi Barrat i Esteve

Dpt. Estudis Jurídics de l'Estat / R+D (SEJ2007-64886)

University of Alacant

Cta. Sant Vicent del Raspeig s/n

E-03690 Sant Vicent del Raspeig

[jordi.barrat@ua.es](mailto:jordi.barrat@ua.es)

**Abstract:** Many countries are using certification procedures to guarantee the full compliance of e-voting mechanisms with democratic standards, but the data generated by these analysis is normally handled almost secretly. Given that transparency is a key principle to guarantee citizen's confidence in the electoral process, this opacity would only be acceptable after a correct balance of the concurrent interests. The paper provides specific data on the certification mechanisms of some countries and assesses the feasibility of a disclosure of the certification reports.

## 1 Introduction

Electronic voting raises several concerns, like, for instance, whether it can provide the same degree of electoral transparency and citizen control that already exists in our current elections. It is not clear how it can guarantee a meaningful recount similar to the traditional one based on paper ballots given that one of the main problems of any electronic voting solution is that an average citizen cannot easily understand how it is working. The current electoral structure allows everybody, even a person without specific skills, to check the accuracy of the process, but unfortunately the electronic voting platforms, at least if they have no paper trail, will never achieve the same degree of external supervision. Its implementation, therefore, should be to strengthen by supplementary control measures, so that, although different from the traditional ones, it would emulate the current framework so that the citizenry could have enough confidence in these new electoral devices.

Although there are different solutions to this problem (e.g. open source e-voting platforms), one of these new mechanisms could be a certification process. They already exists with the traditional paper voting systems, but they become much more important if applied to electronic voting platforms. The electoral authorities would only agree to voting machines that, according to several technical analyses, comply with detailed conditions previously set up. This process would be quite similar to the certification of industrial products, but here there are some specific features because we are not trying to check only whether a device is technically correct. We are also trying to compensate for the lack of citizen control that exists where voting procedures accept computer components. Moreover, ordinary industrial products generate external evidences of their performance, but electronic voting solutions cannot provide these external data because they must also guarantee the secrecy of the vote.

There are several items to be analysed in a certification procedure. The first one could be to decide who will actually carry out the technical analysis that any certification process entails (i). We should opt between public or private bodies and we could also analyse which criteria have been used for each appointment and the detailed conditions and terms to conduct this task. We could also wonder which components of the voting machines will be checked (ii). Once again, the landscape is very different depending on the country. We could find very detailed lists of requirements to be checked by the certification institutions, but also very ambiguous and generic documents. A third focus point could be the legal rules about the disclosure of the reports issued by the certification bodies and the availability of the overall file, that is, the technical documentation of the voting machine (e.g. source code) (iii). Following the patterns of the ordinary industrial certification processes, these policies use to be very opaque.

Due to length restrictions, this paper will only provide an overview of the third point. The analysis includes a preliminary theoretical approach in conjunction with detailed references of some real cases of binding electronic voting systems, namely in Belgium, Estonia, Netherlands (Internet voting not included) and France (Internet voting not included). However, a full understanding of the problem would also require taking into account the approaches developed in other countries like, for instance, the United States, Venezuela or Brazil.

## **2 The Certification Reports: How to Handle Sensitive Data**

The credibility of a system such as electronic voting is supported by a combination of measures designed to increase its openness. The certification is one of these measures, but its actual effects will largely depend on the disclosure of its final findings and it is worth noting that, except for some slight nuances, in all the cases which have been observed, the decision taken was to restrict to the maximum the access to the documentation produced by the technical analysis.

Thus, we should not place too many expectations on the efficacy of the certification measures, at least strictly from the citizen's point of view. There is no doubt that such measures are thought to carry out a correct supervision, but, if such an obscurity is kept, they will by no means be able to emulate the openness and popular control guaranteed by the traditional voting systems. We shall analyse below the situation observed in several countries, paying special attention to the arguments put forward in order to deny access to the aforementioned documentation and also to certain situations where the possibility to achieve a wider spread seems to be making its way.

The French case is particularly interesting, since the public authorities had to take a position regarding a request by which a citizen expressly demanded the disclosure of the certification reports related to the three authorized voting companies. On February, 3rd 2006 the French Ministry of the Interior refused to grant such a claim following the criteria provided by the CADA –*Commission d'Accès aux Documents Administratifs*—. The CADA is an advisory body whose mission consists precisely on deciding, in the light of the regulations on the access to public information, which documents can be actually disclosed and, on the basis of different criteria, which must be handled in a different way. This Commission recommended not to disclose the requested documentation, arguing that it could be detrimental to "le secret industriel et commercial ... [et] compromettre le bon déroulement des élections" (the commercial and industrial secrecy ... [and] endanger the correct electoral management).<sup>42</sup>

Two reasons are given. The first one (i) emphasizes the rights of the private companies which take part in the process, pointing out that the disclosure of the documentation could be detrimental to their interests, specifically to their commercial and industrial secret. Please note that we are referring to the two companies involved and not only to the one that undertakes the development of the computer applications. This fact implies that both would be at risk, on the one hand, the control over the voting technological solution, and, on the other hand, the internal certification methodology used by the company responsible for drafting the report.

From my point of view, an ideal solution must take into account these legitimate interests, but it must also avoid considering them to be the only important interests in this field. As it has been pointed out before, electronic voting does not have the same features as other areas where the certification reports are normally secret. The reports related to many industrial products are subject to these opaque rules, but the electronic voting has a peculiarity that consists in the fact that it is impossible to verify whether the system really works properly. For instance, it will be relatively easy to prove that an authorized train does not meet the analysed parameters, since external evidences will appear. If an authorized train fails to reach the speed that it should theoretically achieve according to a previous technical document, it is obvious that someone has failed—either the railway company or the certification authorities.

---

<sup>42</sup> Document available at: [www.ordinateurs-de-vote.org/IMG/jpg/cada.jpg](http://www.ordinateurs-de-vote.org/IMG/jpg/cada.jpg) [September 7th 2007].

Unfortunately, this method cannot be used in the electronic voting field. In view of the fact that the vote is secret, and unless we decide to implement a paper receipt, there is no external evidence beyond the computer audit that allows us to assert that the results obtained by means of the electronic system faithfully reflect the voter's will. As a matter of fact, the scandals arising from some electronic voting applications, such as the those caused in Sarasota (Florida) or in Schaerbeek (Belgium), are based on absolutely illogical results, as, for instance, the recording of an unusually high rate of abstentionism in a given election<sup>43</sup> or a vote distribution that is incompatible with the electoral formula.<sup>44</sup> These extreme cases may in fact be inspected, and such has been the case, but nothing can be done in other less dramatic cases that would happen, for instance, if the electoral fraud consisted only in shifting the direction of a vote in each constituency.

Thus, the legal framework, which supports the certification of the electronic voting, must rest on this basis and not, as usually happens, on the false premise that the general guidelines for the certification of other products are also applicable in this field.

The ideal solution would obviously consist in enforcing the public and general disclosure of these reports, but before reaching such a stage, it is advisable to examine the possibility of finding an intermediate solution which may not only satisfy the companies involved, but which could also be especially beneficial for the openness required by any electoral system.

---

<sup>43</sup> In 2006, Christine Jennings lost her seat as a representative by a very few votes, but in Sarasota County something strange happened and more than 10% of the voters, even though they had attended the polling station and had voted in many of the simultaneous calls for elections that usually take place in the United States, surprisingly decided to abstain from the election for the House of Representatives, which is one of the most important calls. Moreover, if we compare this percentage with that obtained in the neighbouring region, we will easily prove that the citizens who behaved in a similar way in such a region were many fewer on a relative footing. Further information at: Division of Elections / Florida Department of State - <http://election.dos.state.fl.us/CongressDistrict13.shtml> [September 15th 2007].

<sup>44</sup> To be specific, a candidate obtained a number of preferential votes that exceeded the votes received by the list of candidates in which he was included. There was a difference of 4096 votes. The Collège des Experts, together with the company involved and the Ministry of the Interior itself, pointed out that the most probable reason "pouvait être attribuée à une inversion spontanée d'une position binaire dans la mémoire vive du PC ... Un écart de 4096 peut être occasioné par une inversion de la 13ème position binaire du compteur" (could have been a spontaneous inversion of a binary position within the live PC memory ... A difference of 4096 [votes] could be generated by an inversion of the 13rd binary position of a counting device) [Co03, p.19]. The existence of a physical endorsement for each vote in the form of magnetic cards made it possible to repeat the counting and, in view of the fact that this technical incident did not happen again, they opted to accept the second results as valid. However, this does not make what happened less serious and it raises the question of what the solution would have been in the event that there had been no magnetic cards.

We may consider first whether the very premise on which we rely is certain, that is, whether the belief that disclosing these reports will unavoidably entail an irreparable harm for the industrial and commercial property rights of the companies involved. As a matter of fact, stating that this belief is certain, at least in such a convincing and general way, is far from reflecting the reality. There are several factors that must be taken into account and that may make this statement more flexible in certain respects. One of these factors consists in requiring certain previous certification parameters, which must be detailed and comprehensive and must even include the method to be used for the verification. This is what happens in France, where the electronic voting systems must accredit that a total of 114 conditions of different kinds are met. One of the sections included in the certification reports will obviously consist in a detailed review of these requirements and the integration of the corresponding comments regarding the fact of whether or not the voting prototype has passed the tests.

If the circumstances are as described, the risk of revealing important trade and business secrets seems to be quite remote, and thus, allowing at least a partial disclosure of the certification reports would be reasonable. We should bear in mind that sometimes the comments will not just consist in an affirmative or a negative remark, but they will provide some additional information and these are the details which will precisely help strengthen the electoral openness and the trust of the citizens. The incident that occurred in France regarding the internal clock of NEPAD's machines is a perfect example of what has been stated.<sup>45</sup>

---

<sup>45</sup> As a result of a lawsuit brought in Vaucresson, the Ministry of the Interior disclosed part of the report that Bureau Veritas had drafted for NEDAP [available at: [www.ordinateurs-de-vote.org/IMG/pdf/nedap\\_20070412\\_veritas.pdf](http://www.ordinateurs-de-vote.org/IMG/pdf/nedap_20070412_veritas.pdf) (September 7th 2007)]. The issues at stake were, on the one hand, the hypothetical contradictions between the devices manufactured by NEDAP, which had been purchased at that time in Vaucresson, and on the other hand, some of the conditions which were required by the technical regulations on which a report had to be delivered by the certification authorities, to be specific by Bureau Veritas.

Thus, for instance, the 6th requirement establishes that the members of the polling station must be able to "régler l'horloge interne de la machine à voter" (adjust the internal clock of the e-voting machine) and to the same effect the 46th requirement states that such adjustment must rely on "les données heure-minute-seconde" (the data hour-minute-second). The aim of both conditions is to get devices able to "dater les divers événements et comptes-rendus mémorisés au cours d'un scrutin" (fix the temporal data of the different actions and memos saved during the election) (46th requirement) and, subsequently, the final printings produced by the voting machine must include "les heures d'ouverture et de clôture du scrutin" (opening and closing hours of the election) (19th requirement). Another important issue was the locking mechanism of the voting system, since the 7th requirement envisages "un double dispositif d'authentification électronique" (a double electronic authentication device).

To begin with, from my point of view, it is difficult to assert that the pages that were sent to court compromise the trade secrets of NEPAD or *Bureau Veritas*. In both cases the pages only contained some three-column tables where, together with a tag regarding each requirement demanded by the legal regulations, *Bureau Veritas* had included a comment to the effect of whether or not the prototype complied with each legal condition. Should there be any doubt about the interpretation of the legal regulations or about the total or partial compliance with them, as in the clock's case, the certification authority shall reflect the results obtained and describe as minor or major discrepancies the differences that have been found. All-in-all, we are dealing with documents which neither uncover a computer's architecture nor explain in detail the internal methodology of *Bureau Veritas*, but still they can be extremely helpful for the citizens to get an exact idea of how an electronic voting system works.

For instance, in the internal clock's case, the most important fact is not so much whether or not the machine has an absolute or a relative timer, an argument which was, by the way, rejected by the *Conseil d'État*<sup>46</sup> as well as by the *Conseil Constitutionnel*.<sup>47</sup> The important fact is that now reading the report lets us know that the machine did not really comply with all the legal requirements and that the certification company as well as the Ministry itself had to resort to the cunning argument that the discrepancies were minor in order to be able to validate them.<sup>48</sup>

---

<sup>46</sup> As a result of an appeal lodged in Versailles, the Conseil d'Etat solved this question as follows: "Considérant ... que le règlement technique fixant les conditions d'agrément des machines à voter impose seulement que les machines soit dotées d'une horloge interne que le bureau de vote puisse régler lors de son initialisation et qui permette le chronométrage des événements du scrutin, mais n'exige pas que ce réglage et ce chronométrage soient opérés directement en fonction de l'heure légale; que par suite il est manifeste que le système d'horodatage 'relatif' retenu par les concepteurs de ces machines ne méconnaît pas les conditions d'agrément des machines à voter" (Taking into account ... that the technical document is only requiring an internal clock for each voting machine that could be adjusted by the polling staff during the opening and that allows the chronological counting of the actions generated during the election, but it does not require a counting linked to the official hour; it is thus obvious that the relative counting foreseen by the computer scientists fully complies with the conditions for the acceptance of the voting machines) (Ordonnance no. 305184 from May 2nd 2007).

<sup>47</sup> The Conseil Constitutionnel literally accepted the judgement given by the Conseil d'Etat and, on the basis of the same objection, dismissed an appeal lodged in Aulnay-sous-Bois as a result of the parliamentary elections held in June [Decision 2007-3449 from July 26th 2007]. May I draw your attention to the fact that the argument related to the existence of a mechanical key does not seem to have been used either in the litigation before the Conseil d'Etat or in the one before the Conseil Constitutionnel.

<sup>48</sup> Diverse mechanisms are used in order to deal with the literal sense of the technical requirements, although they all have a common origin, which is some discrepancy between the voting system subject to analysis and the legal requirements. Sometimes the strategy consists in acknowledging some minor discrepancies which, therefore, would not compromise a general positive assessment. This is what happens with the mechanical key problem (7th requirement) and, setting aside the classification of the incident as serious or slight, with the implementation of a relative clock (6th requirement).

However, sometimes the certification authority agrees that the corresponding requirement has been met, even though the previous comments logically lead to a different conclusion. Such is the case, for instance, of the 19th requirement which states that the documents generated by the computer contain all the data "exceptées les heures d'ouverture et fermeture, qu'il convient d'ajouter à la main" (unless the opening and closing hours, that should be manually added) (the italics are mine). The surprising fact is that, as it was pointed out before, according to the technical document, these data related to time are precisely the data which must be printed.

This detail could only become known as a result of the publication of the extract sent to court, since it was not included in any of the previous public statements. In this sense, a wider spread of these tables which, as has been said before, do not compromise the commercial interests of the companies, could provide the citizens with a more complete and detailed sight of the certification process, of the possible implications of the discrepancies, and of the criterion used by the certification authorities in order to classify them as minor or major discrepancies. Although most of the citizens actually lack technical knowledge, such data would allow them to have a better-grounded opinion on whether or not the certification process has been properly designed to perform its purpose, that is to say, to verify whether or not the electronic voting system observes the basic principles of any democratic election.

Other parameters to be taken into account consist in identifying which players will actually receive the sensitive data of the e-voting company and under which conditions. If we implement a certification process, the vendor is accepting to provide sensitive data to a third party, that is, the certifying body, and it seems therefore feasible that other stakeholders might have access to the same information or, at least, to the final report generated by these certification activities. Obviously the vendor could require some conditions, like a confidentiality agreement similar to the one already accepted by the certification body, but there should be no obstacle to broaden the recipients of this information to research groups, to professional corporations or to given civil society organizations closely related to these topics. It would not be a full openness, that could barely guarantee a minimum of confidentiality, but we are managing to involve some supplementary stakeholders. We maintain the same confidentiality conditions already implemented, but we enhance the principle of transparency.

If we analyse the praxis in some countries, we will easily discover that the apparently strict confidentiality requirement is actually breached in some cases. *ES&S*, for instance, accepted during the last French presidential elections, a partial disclosure of its *Bureau Veritas* certification report to some customers belonging to local administrations because, in France, these bodies are actually deciding which e-voting supplier, among the three previously authorized, is the best one. These representatives were invited to *ES&S* headquarters where they could read –not copy— the report. If the vendor itself is implementing such protocols, it would hardly be acceptable not to provide the same information with the same conditions to other stakeholders that seem to be at least as important as local authorities. I am referring, for instance, to political parties.

Belgium is an interesting example, although we will also find some paradoxes. While the source code is largely spread, the certification reports, apparently less dangerous information, are handled with great opacity. The source code is delivered to the political parties even before the elections, although they have to respect a confidentiality agreement. Their IT experts could therefore analyse the system and communicate to the Ministry of Interior whatever mistakes they have found. Second, the electoral authorities upload the full source code to the website immediately after the elections.<sup>49</sup>

---

<sup>49</sup> See a technical analysis carried out by aFRONT based on the source code used in 2003 and 2004: [www.afront.be/lib/vote.html](http://www.afront.be/lib/vote.html) (September 15th 2007).

This transparent behaviour hardly matches with the treatment provided to the results of the certification activities. It would be difficult to reject the publication of the certification report on the grounds of risks for the industrial property, because the source code will already be known by the citizenry. Following the aforementioned Fresh arguments, we could also argue that what is actually in danger is the methodology of the certifying institution, but we already know that this parameter could have minor relevance if the criteria are previously set up in a very detailed way. Unfortunately, Belgium does not meet this condition because the criteria are not detailed and therefore the certifying bodies have large powers to assess whether the software complies with them.

This opaque approach may have unwanted consequences since the citizenry could become more and more reluctant to easily accept the fair behaviour of the electoral authorities. It is worth recalling, for instance, the following statement of the *Collège des Experts*: "Il est à noter que l'attitude du SPF Interieur vis à vis les rapports des organismes d'avis est fort peu critique. En effet, peu importe la qualité des tests, un rapport positif est visiblement accueilli avec un grand soulagement" (It is worth noting that the Ministry of Interior's behaviour is not very rigorous regarding the reports issued by the certifying companies. Despite the actual quality of the checks, a positive report is publicly received with a great relief) [Co07, p. 16]. The only way to avoid this perception is to accept a full disclosure of the certification report and the *Collège* actually makes this recommendation later [Co07, p. 28].

The Netherlands also has a nuanced framework that does not match with the simple and quick French solution. The *Brightsight's* report was kept secret during the 2006 elections, but the implementation of the Act regarding a free access to the public information allows the disclosure of significant data about the relationships between the electoral authorities and their computer supplier *Groenendaal* [Wv07]. The certification report is not publicly available yet, however.

Finally, assuming that Estonia does not have a formal certification procedure [DM02, p. 238], its electoral authorities accepted in 2007 several verifications carried out by specialists, but unfortunately "the results of these reviews were not made public" [Os07, p 15]. The private audit, carried out during the electoral period aiming to check whether the operational protocols were correctly followed, is not publicly available either [Os07.p. 15].

There are therefore some interesting paradoxes. While the system seems to be very open, accepting reviews carried out by any interested group, the subsequent decisions are very opaque because the findings of these procedures remain secret. Is it actually useful, from a democratic point of view, to foster such confidentiality agreements? Obviously these reviews are important achievements, mainly if we take into account what is happening in other countries, but their usefulness is not clear since we will not be able to alert the society to the vulnerabilities that we could have found.

It is difficult to find balanced solutions in these cases, but we could try to soften confidentiality agreements so that any person could at least publicly provide a general overview of his/her analysis confirming the system's reliability or pointing out some weaknesses. The first statement will definitively strengthen the citizen's confidence and the second one, even in these generic terms, will likely rouse citizen's concerns and will foster further check ups by the electoral authorities themselves.

Finally, there was a second argument (ii) within the CADA's recommendation. A full disclosure of the certification reports "pourrait compromettre le bon déroulement des élections." Certainly, one common argument against open source is the risk to provide sensitive information to external hackers. Although this is a technical debate and this paper only has a legal approach, it is worth underlining that many computer scientists, even perhaps a large majority, are actually supporting open source solutions as the best ones. Jason Kitkat, for instance, thinks that a disclosure is not neutral and actually increases the system's security: "Cryptographers and security professionals use peer review to provide assurance for the quality of their systems. A security scheme whose source code and design is known yet continues to offer a useful level of protection is a good one" [Ki04, p. 65; same opinion Ru06, p. 125]. There will be other challenges, like the verification that all the devices are actually containing the correct code, but the security and robustness of the product would be enhanced with an open strategy.

### **3 Concluding Remarks**

The certification of industrial components used to be an ordinary procedure thought to guarantee their quality and security within a standardized protocol of supervision mechanisms. However, electronic voting platforms have some specific features, like the need to maintain the transparency of any electoral step and the lack of a paper trail that, if required, could allow us to perform a second tally. Since the certification process should take into account these specific needs, we should profile a special protocol for this single product. Although there are several items to analyse: who is doing the technical analysis (i), which criteria should be used (ii) and who should receive the final reports (iii), this paper is only focused on the third one.

The protection of the industrial property has been so far a common argument to reject a full disclosure of the certification reports. It is a legitimate position, but it should be balanced with other approaches given that we are talking about electoral processes and therefore the citizens' confidence in the system should be a major outcome. A fair business concurrence might also be a sound argument against opacity. Should e-voting systems increase their implementation worldwide? Should new or more balance between transparency and property be sought? Despite the current framework, the paper shows how some minor data coming from given countries actually suggests that the opacity is not well grounded and that it would be easily feasible to include a certain degree of transparency without breaching the industrial property.

These humble measures could be a good beginning in order to achieve afterwards a new balance between electoral transparency and other opposite interests. Moreover, the Belgian experience should be seriously taken into account, because its structural weakness, the Collège des Experts, provides external control over the e-voting process.

## References

- [AH04] Álvarez, M.; Hall, T.: Point, Click and Vote: The Future of Internet Voting. The Brookings Institution, Washington, 2004.
- [Co03] Collèges des Experts: Rapport concernant les élections du 18 mai 2003. Collège des Experts chargés du contrôle des systèmes de vote automatisés, [Brussels], 2003. [www.poueva.be/IMG/pdf/RapportExperts2003.pdf](http://www.poueva.be/IMG/pdf/RapportExperts2003.pdf) [September 15th 2007]
- [Co07] Collèges des Experts: Rapport concernant les élections du 10 juin 2007. Collège des Experts chargés du contrôle des systèmes de vote automatisés, [Brussels], 2007. [www.poueva.be/IMG/pdf/RAPPORT\\_CONCERNANT\\_LES\\_ELECTIONS\\_DU\\_10\\_JUIN\\_2007.ocr.pdf](http://www.poueva.be/IMG/pdf/RAPPORT_CONCERNANT_LES_ELECTIONS_DU_10_JUIN_2007.ocr.pdf) [September 8th 2007]
- [DM02] Drechsler, W.; Madisse, Ü.: E-Voting in Estonia. In: *Trames. Journal of the Humanities and Social Sciences*. n. 3, 2002; P. 234-244.
- [Fe07] Fernández Rodríguez, J. J.: Voto electrónico. Estudio comparado en una aproximación jurídico-política (Desafíos y posibilidades). Fundap, Querétaro, 2007.
- [Gr03] Gritzalis, D. A. (ed.): *Secure Electronic Voting. Advances in Information Security*. Kluwer, Boston, 2003.
- [KB04] Kersting, N.; Balderstein, H. (eds.): *Electronic Voting and Democracy: a Comparative Analysis*. Palgrave Macmillan, Basingtoke, 2004.
- [Ki04] Kitcat, J.: Source Availability and E-Voting: An Advocate Recants. In: *Communications of the ACM*. n. 47(10), 2004; P. 65-67. <http://doi.acm.org/10.1145/1022594.1022625> [September 4th 2007]
- [Kr06] Krimmer, R. (ed.): *Electronic Voting 2006*. (Col. "Lecture Notes in Informatics – LNI" / P-86), Gesellschaft für Informatik, Bonn, 2006..
- [OS07] Osce: Republic of Estonia. Parliamentary Elections 4 March 2007. OSCE/ODIHR Election Assessment Mission Report. OSCE (The Organization for Security and Co-operation in Europe), Warsaw, 2007. [www.osce.org/item/25385.html](http://www.osce.org/item/25385.html) [September 15th 2007]
- [PK04] Proser, A.; Krimmer, R.: *Electronic Voting in Europe. Technology, Law, Politics and Society*. Gesellschaft für Informatik, Bonn, 2004.
- [Ru06] Rubin, A. D.: *Brave New Ballot. The Battle to Safeguard Democracy in the Age of Electronic Voting*. Morgan Road Books, New York, 2006.
- [TM05] Trechsel, A. H.; Méndez, F. (eds.): *The European Union and E-Voting. Addressing the European Parliament's Internet Voting Challenge*. Routledge, London, 2005.
- [Tu05] Tula, M. I. (coord.): *Voto electrónico. Entre votos y máquinas. Las nuevas tecnologías en los procesos electorales*. Ariel, Buenos Aires, 2005.
- [Wv07] Wvsn: Voting systems company threatens Dutch state. Ed. Wij vertrouwen stemcomputers niet — WVSN, Amsterdam, 2007. [www.wijvertrouwenstemcomputersniet.nl/English/Groenendaal](http://www.wijvertrouwenstemcomputersniet.nl/English/Groenendaal) [September 2nd 2007]