

GI, the Gesellschaft für Informatik, 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 "Seminars", "Proceedings", "Monographs" and "Dissertation Award", 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/>

The 2006 conference on Electronic Voting took place in Castle Hofen near Bregenz at the wonderful Lake Constance from 2nd to 4th of August. This volume contains the twenty papers selected for the presentation at the conference out of more than forty submissions. To assure scientific quality, the selection was based on a strict and anonymous review process. The papers cover the following subjects: e-voting experiences, social, legal, political, democratic and security issues of e-voting, as well as solutions on how to (re)design election workflows, and finally how to implement and observe electronic voting systems.



Robert Krimmer (Ed.): Electronic Voting 2006

P-86

GI-Edition

Lecture Notes in Informatics

Robert Krimmer (Ed.)

Electronic Voting 2006

2nd International Workshop
Co-organized by Council of Europe,
ESF TED, IFIP WG 8.5 and E-Voting.CC

August, 2nd – 4th, 2006
in Castle Hofen, Bregenz, Austria

Proceedings



A Methodology for Auditing e-Voting Processes and Systems used at the Elections for the Portuguese Parliament

João Falcão e Cunha, Mário Jorge Leitão, João Pascoal Faria,
Miguel Pimenta Monteiro, Maria Antónia Carravilla
Faculdade de Engenharia da Universidade do Porto
Rua Dr. Roberto Frias
4200-465 Porto, Portugal
{jfcunha | mleitao | jpf | apm | mac}@fe.up.pt

Abstract: In the 2005 Portuguese Parliament General Elections there were non-valid experiments of e-voting at five voting places and also through the Internet. *Faculdade de Engenharia da Universidade do Porto* audited such experiments. Relevant *security, transparency, usability* and *accessibility* evaluation criteria and sub-criteria were defined, and an auditing procedure based on AHP was established. This paper shortly presents the methodology used, the four e-voting systems and the main results of the overall experiment. The systems could be used successfully and were extremely popular with voters. However, more information to the citizens and to the officials involved in the e-voting process would be required for a valid election. The systems also need to be improved, for instance, to make sure that the number of votes electronically cast is the same as the number of voters that were validated and actually registered to vote at any particular site on the Election Day.

1 Introduction

1.1 Context

During the previous elections for the European Parliament, in 2004-06-13, and for the general elections for the Portuguese Parliament, in 2005-02-20, the government and the parliament agreed to carry out a set of experiments on electronic voting.

For the European Parliament elections there were 9 boroughs involved, geographically and socially dispersed, some in large towns with highly educated voters, and some in small villages with pensioners having little contact with technology. From a total 52 000 electors who cast a valid vote, 9 359 voted electronically (18%) [FE04].

For the elections for the Portuguese Parliament the selected boroughs corresponded to the 5 sites where the President of the Republic and the leaders of the political parties represented at the parliament voted. As Portuguese citizens registered to vote abroad could do it by postal vote (remote vote allowed), it was also decided to set up an Internet voting system. In all cases e-voting was voluntary and not valid, and who cast their vote traditionally was invited to also vote electronically. From a total of 26 515 electors who cast a valid paper vote, 8 824 also voted electronically (33%). From a total of 148 159 electors outside Portugal who were registered to vote by mail, 36 391 voted by mail (25%) and 4 367 voted through the Internet (12% of mailed votes) [Pi05]. After voting, each citizen was personally interviewed by an independent organization in order to collect an opinion about the experience (see below). In the Internet case, the voter could fill in a questionnaire for the same purpose.

Several public and private organizations were involved, but UMIC www.unic.pt, a special government unit with the overall mission of promoting innovation, was in charge of coordinating the project. CNE www.cne.pt and STAPE www.stape.pt, the public entities that oversee and manage general elections in Portugal were also deeply involved. CNPD www.cnpd.pt, a parliament controlled but autonomous unit that oversees the use of information and databases with personal information was also asked to audit and certify procedures. INDRA, MULTICERT, NOVABASE and UNISYS provided the e-voting systems (EVS) for the experiment. MULTICERT, under the guidance of UMIC and CNPD also had the overall responsibility of putting together a digital electoral register for all voters involved in the experiment, and to deploy such system during Election Day at all sites.

The experiments were very successful from the point of view of the voting citizens [OS05]. According to the exit interviews, 99.2% of the citizens that voted electronically enjoyed the experience and 98.1% said they would vote electronically in future elections; 80.5% trust the security of the EVS; 84.5% of the voters that had a paper trail option in the EVS used, consider important that the vote had been printed in paper and automatically inserted into a box; 86.3% consider that if such systems allow people to vote from other places then more people would vote. For people voting through the Internet the results were similar: 99.2% enjoyed the experience and 98.3% said they would vote in this way in future elections; 57.8% trusts the security of the EVS, 7.9% thinks it is not secure, and 34.3% do not know or do not answer the question. Regarding the security of Internet voting, only 1.7% thought it is totally secure against attacks from hackers, while 54.3% do not know or do not answer [UM05].

In order to guarantee the transparency of the process, Universities were invited to make proposals for auditing the process. In the case of the elections for the European Parliament five Universities were involved. Given the fact that it was difficult to manage so many auditors, UMIC agreed that for the Portuguese Parliament's elections there would be a call for tenders regarding the auditing process. *Faculdade de Engenharia da Universidade do Porto* (FEUP) was selected as the main auditor, on the basis of the quality of proposed work, experience and qualifications of the auditing team, price and schedule of work.

1.2 The voting experiments

Five e-voting sites were set-up requiring voters to go to the voting place. One of these sites had six e-voting places allowing the citizens to vote outside their traditionally appointed paper voting place. An Internet system was also deployed to allow e-voting from Portuguese voters registered as residing abroad.

Figure 1 describes the general set-up for the experiments during the Portuguese Parliament's elections.

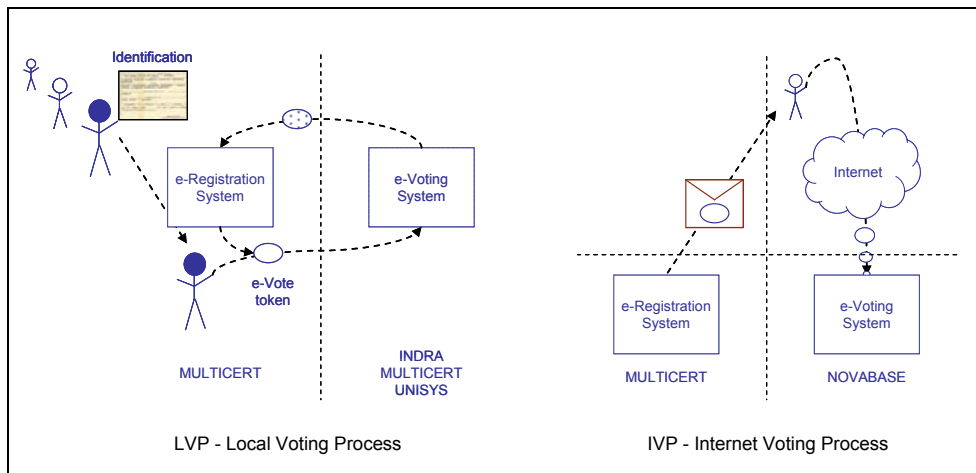


Figure 1: LVP: a citizen with a proper identification gets a token at e-Registration and then can vote. INDRA had one token for each voter, but in the other systems the token is reused after a new permission is granted. Number of voters and votes are counted both at e-Registration and at the e-Voting system. IVP: a citizen that is registered to vote gets an envelope by mail with a token (username and password). He may then log into the e-voting system.

2 The Auditing Methodology

The objective of the auditing methodology was to produce a thorough report on each EVS and to apply scores for each one on the criterion defined by UMIC: Security, Usability, Transparency and Accessibility.

Due to the characteristics of the process, there were 14 auditors involved. This is a large number, and there is a strong need to obtain scores for the EVS that consistently reflect the views of the group as a whole, and not just 14 different views. In order to simplify the assessment, the 4 criteria were decomposed into several sub-criteria. The Analytical Hierarchy Process (AHP) ([Sa80], [Sa87]), which is based on the comparison of the importance of each pair of sub-criteria, was the tool used to obtain weights of each sub-criterion under each criterion, aggregating the views of all the auditors.

2.1 Team composition

The auditing team members' had deep technical and management expertise. They had doctorates in Computer Science, Telecommunications, Security and Information Systems. There was 1 overall coordinator, 4 auditing teams with 3 or 4 elements each (as there were 4 different EVS), and 1 team with 2 elements, both with doctorates in Operations Research, that acted as facilitators during the whole process.

2.2 Phases of the process

The methodology followed by FEUP had three phases, corresponding to the periods before, during and after the Election Day.

Before the Election Day the team met several times in order to make decisions on the criteria and sub-criteria, on the assignment of the auditing team members to the e-voting systems (EVS) and voting periods, and on the set of questions and requests for information to send to each company.

At the Election Day, in order to make possible a comparative classification of systems for the same criteria and sub-criteria, each auditor visited at least two different EVS. There was always an auditor at each voting site, observing the opening moment, the voting process and the final closure, including the vote counting and the communication of results to the counting centre. There was also an auditor at the counting centre.

After the Election Day the auditing team had also at least one meeting with each company, in order to ask further questions that did arise during the audit. With all the information on-hand the auditing team had a long final meeting, facilitated by the Operations Research team, to discuss the scores given for each EVS on each sub-criterion. Taking into account all information, a report on each EVS was produced and sent to UMIC and then to each company.

The procedure for auditing the Internet EVS was adapted from this one as there was not an Election Day but an election period of several weeks. Such votes could only be counted after the postal votes were counted, two weeks after the actual Election Day.

2.3 The evaluation criteria and sub-criteria

The evaluation criteria (Security, Usability, Transparency and Accessibility) were defined a priori by UMIC. During several meetings that took place before the Election Day, the auditing team agreed on the sub-criteria under each one of the evaluation criteria (see Figure 2), based on [Ne93], [BH04], [Ca04], [Me00], [Mo01] and [Pi04]. These meetings were very important for the auditors to discuss and get a consensus on the meaning of each sub-criterion. As, during the Election Day, the teams could not meet and discuss the evaluation criteria it was necessary to promote a discussion on the criteria and sub-criteria with all the auditors, in order to obtain homogeneous evaluations.

SECURITY (S)	100,0%
S1 Audit-ability	10,3%
S2 Operator authentication	4,4%
S3 Certify-ability	9,0%
S4 Reliability	9,8%
S5 Detect-ability	4,6%
S6 Availability of system	5,4%
S7 Immunity to attack	8,1%
S8 Integrity of votes	14,4%
S9 Invulnerability	9,3%
S10 Traceability	3,8%
S11 Recoverability	5,3%
S12 Fault tolerance	4,6%
S13 Isolation	2,6%
S14 Security of communications	8,3%

TRANSPARENCY (T)	100,0%
T1 Anonymity	11,3%
T2 Atomicity	7,0%
T3 Authenticity	11,5%
T4 Trust	6,2%
T5 Technical documentation	2,2%
T6 Integrity of personal	2,8%
T7 Integrity of system	6,0%
T8 Non-coercion-ability	10,5%
T9 Precision of system	7,6%
T10 Privacy	7,6%
T11 Singularity (non reuse)	10,7%
T12 Transparency of process	3,5%
T13 Transparency of system	3,9%
T14 Verifiability	6,5%
T15 Separation of roles	2,9%

USABILITY (U)	100,0%
U1 Easiness of use	38,4%
U2 Speed of use	10,1%
U3 Clarity of language in interface	23,4%
U4 Localisation of interface	11,1%
U5 Emotional satisfaction	17,0%

ACCESSIBILITY (A)	100,0%
A1 Convenience	14,4%
A2 Right to vote	47,0%
A3 Documentation for the elector	7,6%
A4 Flexibility	11,9%
A5 Mobility	19,1%

Figure 2: Criteria and sub-criteria for auditing, with relative weights [FE05].

As an example, the sub-criterion “Availability of the System” was described as “During the voting period, the EVS must always be available for all the actors, particularly the voters, in order for the process to run normally”. Again as an example, a score of 1 would be given to an EVS that could work during the whole election day, if nothing wrong happened, a 3 if the system would for instance include a battery, that would allow it to work for at least 30 minutes without external power supply, and a 5 if the system would work, based also on batteries, during the whole election day. Such concrete guidelines are not always possible to define, but are desirable for consistent evaluations.

During those meetings it was also necessary to obtain the weight of the sub-criteria under each criterion. The tool used to obtain these weights is called Analytical Hierarchy Process (AHP) and is based on the comparison of each pair of sub-criteria by their relative importance. Every team-member had to fill-up a matrix (see Figure 2) comparing each pair of sub-criteria under each criterion. A 1 means the sub-criteria are equally important, a 9 means, for instance, that “Right to vote” is extremely more important than “Flexibility”. The pairwise comparison matrix for each criterion was obtained by calculating the average of the answers of the team members. The AHP methodology was then applied to each criteria matrix leading to a balance of the sub-criteria under each one of the 4 criteria.

Accessibility	A1 Convenience	A2 Right to vote	A3 Documentation for the elector	A4 Flexibility	A5 Mobility
A1 Convenience	1	1/7	6	9	1/6
A2 Right to vote	7	1	9	9	8
A3 Documentation for the elector	1/6	1/9	1	1/6	1/8
A4 Flexibility	1/9	1/9	6	1	1/7
A5 Mobility	6	1/8	8	7	1

Figure 3: Matrix for the pairwise comparison of the sub-criteria of the Accessibility criterion.

After the Election Day, the auditing teams met to evaluate each EVS on each sub-criterion. This evaluation was given simultaneously to all the EVS after a general discussion and an agreement of the auditors involved. The score of each EVS under each criterion was obtained by calculating the internal product of scores with the weights of the sub-criteria under each one of the 4 criteria. The final result is shown in Figure 4.

	UNISYS	INDRA	MULTICERT	NOVABASE
Security	4,2	4,1	2,6	3,6
Transparency	4,2	4,3	3,2	3,0
Usability	4,2	3,9	2,7	3,8
Accessibility	3,7	3,3	3,5	3,6

Figure 4: Final evaluation under the 4 criteria of the 4 EVS (scale 1-5).

3 The e-Voting Systems and Associated Processes

The e-voting experiments involved hardware and software from 4 enterprises: MULTICERT, UNISYS/ESS, INDRA and NOVABASE. As mentioned in the introduction, MULTICERT developed the elector registration system used in all experiments and NOVABASE developed the Internet voting system. There were two kinds of presentational voting systems: The *local voting* systems required that voters would go to their traditional voting place. This was the only location where they could cast their electronic vote. In the *local voting with mobility* system the voter could choose one from several places where to vote, all located in the same borough. All systems are shortly presented in the next sections. For further details see [FE05].

3.1 INDRA – Local Voting

The system proposed by INDRA is named Point&Vote. It consists of special purpose equipment based on a standard PC platform equipped with a touch screen with side view protection, a smart card reader and an internal printer for reports. The unit is portable and must be placed on top of a table. Two alternative versions were available, one with headphones and mouse for physically impaired voters, and another with a printer, where votes could be seen for a few seconds by the voter, but could not be removed from the collecting basket. This version was intended for evaluation of the need of a paper trail.

In order to vote using the INDRA system, each citizen receives a smartcard. This token is required to enable the use of the actual voting machine where votes are cast (and counted at the end of the Election Day). After being used the smartcard is returned to the e-registration and is not used again at the current election.

At the end of the voting period, each Point&Vote machine is closed with the operator (supervisor) smartcard and password, thus disabling any further voting action. Results from each machine can now be locally printed and transmitted subsequently over the internal modem via a secure communications link to a computer of the Central Election Authority.

3.2 UNISYS/ESS – Local Voting

The system proposed by Unisys and manufactured by Election Systems and Software (ESS) was the iVotronic. It can be generally characterised as a touch screen voting unit, portable and easily configurable (height and orientation), with good privacy protection. These features, plus an optional audio interface, allow good support to visually impaired and wheelchair locomoting voters.

The PEB (Personal Electronic Ballot) is the token that gives access to one vote in the iVotronic machine, prevents overvoting, and notifies the voter in the case of an incomplete operation (such as removing the PEB from the iVotronic unit before pressing the physical VOTE button). It's a sealed unit communicating within a very short range through a proprietary infrared technology and protocol that was designed to prevent communication with standard IrDA transceivers. After each use the PEB must be regenerated in a specific machine with the proper infrared interface.

Some special operations can be performed using a different supervisor PEB requiring explicit password validation. If validated, operations such as opening a voting session (zeroing the counters), closing the voting session, or casting or eliminating incomplete votes (when the voter didn't press the VOTE button), are allowed and logged. During the voting session results are accumulated internally and redundantly recorded (in 3 different flash memory units). All operations, including the supervisor actions, are also timed and logged.

At the end of the session the voting units must be closed and its accumulated results transferred and added to the supervisor PEB memory, allowing several units to be combined in a single one. This PEB is then read in another machine, which also can combine several results. This machine can now print the results (totals and partials) and transmit them to a computer of the Central Election Authority using a modem and a phone line.

3.3 MULTICERT – Local Voting with Mobility

Differently from the previous systems, the MULTICERT voting system allowed citizens to vote electronically in a place different from their traditional one, within the same borough. In the future, the goal of the system is to allow citizens to vote in any other borough.

This was achieved by a distributed e-registration system, based on a central database that stored information about what electors had already voted, and was remotely accessed by client applications located in each place.

Another distinguishing feature of this system was the existence of an electronic ballot box system (EBBS) that actually stored the electronic ballots, separated from the electronic voting units where the electronic ballots were filled in. Small i-button devices were used to carry authorizations (similar to empty ballots) from the EBBS to the electronic voting units, and carry back filled in ballots to the EBBS.

Besides a touch screen, each electronic voting unit had a small printer to print and store paper ballots corresponding to the electronic ballots, with the purpose of enabling non-electronic ballot recounting and improving the confidence on the process. The elector could check by visual inspection that the printed ballot corresponded to his electronic ballot.

Special operations could be done in the EBBS using supervisor i-buttons, namely start a voting session (zeroing the counters), close the voting session, and subsequently view on screen, print and export the results. The results were not transmitted electronically.

3.4 NOVABASE – Internet

The Internet voting system was aimed at all the citizens registered to vote outside of Portugal using postal vote. Two separate mailings were sent to voters abroad: the one containing the valid ballots and another one with the information and keys to allow the vote using the Internet system. The Internet voting process (i-voting), had the following steps:

1. Using a database of electors the system generates individual credentials for each one, a unique code of a username and a password.
2. The electors' information is registered together with the credential in the Active Directory of the central system.
3. The credentials are posted to the electors abroad by mail. The message does not include the elector number, to prevent other people to vote.
4. Pairs of encryption keys are generated. The public key is send to Novabase to be stored in the Database. The private key is divided into 7 parts, one for each political party represented. Votes can only be read with these 7 keys.
5. The vote process is open, allowing browsers to access the server. In the experiment this server was located at the headquarters of Novabase.
6. The elector receives the credentials. He/She can use any computer with a browser, able to accept some JavaScript and cookies, to access the web page www.votoelectronico.pt. He/She has to introduce the elector number and the credential. If all is correct, he/she can then proceed to vote.
7. The confirmed vote is registered in a database table, using two key encryption. The public key is used to encrypt. During the same transaction it is stored that the citizen has voted in the credentials table and in the Active Directory. Afterwards the elector is informed that the vote has been confirmed.
8. At closure of the election the information in the Active Directory is printed and sent to CNE. The Active Directory is erased in the presence of CNPD. A copy of the database is stored and sealed in a CD with a MD5 seal, kept by UMIC.

9. Counting of the votes is done with a special application. As the votes are encrypted it is required to bring together the 7 keys to produce the final result.

The system uses traditional client server architecture. From a logical point of view there is one Web site and clients over the Internet. The Web site is in fact divided in two parts: an http information site and an https secure one, with the forms and vote registration.

4 Conclusions

It is widely accepted that there is very high satisfaction and trust with the current paper based electoral process in Portugal. Most of the citizens cannot evaluate the security or transparency of the computing and communication systems to be eventually used in elections. Certification and audits are therefore required to provide a wide socially recognised guarantee of security and transparency for the new systems and processes.

The audit identified many advantages and problems of the several EVS. One of the problems observed has to do with the inconsistencies in the final number of counted electronic votes. In each voting site there were a number of total electronic votes N_v (counted by the EVS) and a total number of citizens C_v that were given tokens to vote (counted by the e-Registration system). The three situations below occurred. This could be a problem of the EVS, of the procedures people used, or both:

- $N_v > C_v$. At least one citizen voted twice. It could have happened that one citizen was given more than one chance to vote (e.g.; claimed token was faulty).
- $N_v < C_v$. At least one citizen did not vote. It could have happened that one citizen actually did not vote at the EVS (not a problem, if voluntary).
- $N_v = C_v$. All was fine, or pairs of the above happened at the same EVS.

All systems, except the Internet one, suffered from this problem. This can be a major problem facing the adoption of e-voting, and illustrates the need for improved systems and improved voting processes. Improved systems can make the voting process more secure and transparent, as well as more usable and accessible. Improved information to the citizens and to the officials running the election, are key requirements for maintaining trust and satisfaction with the democratic election processes.

The audit method presented did not produce a final ranking of systems. This would require that relative importance would be given to the 4 criteria. Acceptable minimum levels of performance on each criteria (or subcriteria) could have been defined. For instance, one may argue that EVS security level must be over a certain level in order to be acceptable to be used. Both of these decisions, on relative importance of criteria and minimum performance levels, must also involve political involvement.

An improved audit method could include a comparison of EVS with the traditional paper voting system, on the same criteria. Weak and strong points of each type of system could be compared under the same sub-criteria, if making sense.

Acknowledgments

The authors would like to acknowledge the work and contributions of Gabriel David, J. Correia Lopes, A. Carvalho Brito, J. Magalhães Cruz, Sérgio R. Cunha, R. Moreira Vidal, Henriqueta Nóvoa, J. Vila Verde, Miguel Gonçalves, L. Miguel Silva, and J. Fernando Oliveira. The auditing process benefited from contributions from Diogo Vasconcelos, Sara Piteira and João Vasconcelos, from UMIC, and from Fernando Silva, from CNPD. The authors would like to state their appreciation for the very professional attitudes of officials from CNE and STAPE, and from the representatives of all the enterprises that were directly involved in the experiments.

References

- [BH04] B. Bederson, P. Herrnson: «Expert Review Plan of Voting Machines», Research Report, HCI Lab & Centre for American Politics and Citizenship, U. Maryland, USA, 2004.
- [Bu04] T. M. Buchsbaum: «E-Voting: International Developments and Lessons Learnt», in [PK04], p. 31-41.
- [Ca04] Jean Camp, Allan Friedman, Warigia Bowman (ed.): «Electronic Voting Best Practices - A Summary», Voting, Vote Capture & Vote Counting Symposium, Kennedy School of Government, Harvard University, 2004-06, 23 p.
- [FE04] (in Portuguese) J. Falcão e Cunha (ed.): «Relatório Final de Auditoria – Eleições para o Parlamento Europeu de 2004-06-13» (Final audit report of the Portuguese electronic elections experiment for the European Parliament); 2004-08-04, FEUP, Portugal, 28 p.
- [FE05] (in Portuguese) J. Falcão e Cunha (ed.): «Relatório Final de Auditoria – Eleições Legislativas de 2005-02-20» (Final audit report of the electronic elections experiment for the Portuguese Parliament); 2005-04-21, FEUP, Portugal, 78 p.
- [Me00] Rebecca Mercuri «Generic Security Assessment Questions» (www.notablesoftware.com).
- [Mo01] (in Portuguese) A. Monteiro, N. Soares, R. M. Oliveira, P. Antunes: «Sistemas Electrónicos de Votação» (Research Report supervised by P. Antunes, DI-FCUL TR-01-9), 2001, Dep. Informática, FCUL, Campo Grande, 1700 Lisboa, Portugal.
- [Ne93] Peter G. Neumann: «Security Criteria for Electronic Voting», 16th National Computer Security Conf. Baltimore, Maryland, 1993.09.20-23.
- [OS05] (in Portuguese) OSIC – Observatório da Sociedade da Informação e Conhecimento «Voto Electrónico - 2.ª Experiência Piloto de Voto Electrónico Presencial, Resultados Eleições Legislativas de 2005-02-20», 2005-03, 22 p.
- [Pi04] (in Portuguese) R. R. Pinto, F. Simões, P. Antunes: «Estudo dos Requisitos para um Sistema de Votação Electrónica» (Research Report supervised by P. Antunes, DI-FCUL TR-04-2), 2004, Dep. Informática, FCUL, Campo Grande, 1700 Lisboa, Portugal.
- [Pi05] (in Portuguese) S. R. Piteira: «Projecto Voto Electrónico», Voto Electrónico e Defesa da Privacidade Workshop (Electronic Voting and Privacy Protection Workshop), CNPD, Assembleia da República, Lisboa, 2006-12-07, 21 p.
- [PK04] A. Prosser, R. Krimmer (Eds.): «Electronic Voting in Europe – Technology, Law, Politics and Society», Lecture Notes in Informatics, GI-Edition, 2005.04.23, 182 p.
- [Sa80] T. L. Saaty: «The Analytic Hierarchy Process». McGraw-Hill, New York, 1980.
- [Sa87] T. L. Saaty: «The Analytic Hierarchy Process: what it is and how it is used», Mathematical Modelling, 9, 1987.
- [UM05] (in Portuguese) «Voto Electrónico - 1.ª Experiência Piloto de Voto Electrónico Não Presencial, Resultados - Eleições Legislativas de 2005-02-20», UMIC, 2005-03.