GI, the Gesellschaft für Informatik, publishes this series in order

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/

Robert Krimmer (Ed.): Electronic Voting 2006

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.

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

Contributions to traditional electronic voting systems in order to reinforce citizen confidence

Ana Gómez Oliva, Sergio Sánchez García, Emilia Pérez Belleboni

Dpto. de Ingeniería y Arquitecturas Telemáticas (DIATEL)
Universidad Politécnica de Madrid. Ctra. Valencia km. 7. 28031 Madrid. Spain
{agomez | sergio | belleboni}@diatel.upm.es

Abstract: This document provides a general description of the telematic voting scenario designed by the author's research group. This scenario reinforces verification procedures as key elements to achieve full acceptance of the system on the part of voters. To frame this work, a general overview of electronic voting is given and the conditions entailed by these systems are specified.

1 Problems inherent to telematic voting

Since the first experiments in the 1960's with computerized voting until today, in which electronic ballot boxes or Internet voting are being tested, the mass media highlighted a number of experiences around the world under the general concept of *electronic voting*. However, these experiments have involved diverse types of voting systems, where the security guarantees required in authentication processes, voting and tallying are provided in quite diverse forms. In [CGP02] the authors propose a classification of voting systems into several levels of complexity. We can therefore identify two main groups that are relevant to our work: i) Systems that substitute one of the physical components of traditional voting procedures with some type of electronic process (i.e. Direct-Recording Electronic), and ii) those that use telematic networks to link voters to a remote polling station. For the last several years, nearly all governmental action designed to automate voting processes involve policies that fall within the first group, where the electronic ballot box, with or without a ballot, is the most commonly used device in all cases. The experiences of countries like Brazil [Re04] and India [In06] are noteworthy in this regard, particularly the latter, with its hundreds of millions of votes cast confirming the validity of this method.

In the second group, i.e. voting through telematic networks, which we have decided to call **telematic voting**, there have been few experiences with the status of official validity, although numerous proposals or voting schemes have emerged, defining the agents, procedures and security protocols necessary in order to carry out the voting process. In most of these schemes (of which [CC96] [OMA99] and [Ri99] are samples), determination of the security requirements to be met by voting systems has reproduced the guarantees provided by traditional voting processes, as these efforts have focused mainly on ensuring voter anonymity, preventing votes by voters that are either unauthorized or that have already voted and achieving an accurate vote tally. Moreover, since the voter is casting a vote through telematic networks, these voting schemes include cryptographic procedures that prevent votes from being altered or examined during their transmission to the ballot box.

1.1 Common solutions to basic problems

We shall now discuss in detail the problems faced by the designers of any system of telematic voting and the solutions most commonly adopted:

(1) Properly identify voters when casting votes; that is, there should be no usurpation of identity, for here no person can attest to voters' identity as is done at present in traditional voting with members of a polling station. The method for solving this problem is based, in every case, on the existence of a prior offline procedure involving distribution to voters of specific voting credentials that identify the bearer. These credentials today are found in many forms, from the simplest like a secret key to the most sophisticated, like a digital certificate.

(2) Guarantee the anonymity of voters, so that the credential used to validate a vote – and the voter's identity – cannot be associated with the vote cast itself. The most common solution to this problem is to divide the vote casting process into two phases: vote authentication and the voting process itself, so that distinct, unrelated entities will handle these two processes. Typically, the first entity verifies the credentials of the voter and grants permission to vote, while the second recognizes this permission and accepts the vote of the voter. Precautions must be taken to prevent any collusion between the two entities that might allow for establishing a relationship between the voter and the vote.

(3) Prevent voters from voting more than once. The solution to this problem is provided verifying the voter's credential, by simply marking a given credential as already used, with this status checked prior to giving permission to vote.

1.2 Threats posed by the use of computer networks and systems

In addition to the foregoing requirements to be fulfilled by any voting system, telematic voting systems must face specific threats: first, the fact of using communications networks to interconnect voting system devices, (voting sites, remote polling stations, etc) and second, the use of computer systems to cast votes or undertake counting procedures. Either of these conditions makes the following attacks possible:

(1) Attacks on the confidentiality of information and its integrity, making it feasible for an attacker to modify or eliminate votes legitimately cast or to discern their content.

(2) To counteract such attacks on telematic networks, the most advanced voting systems use cryptographic procedures that usually involve the application of ciphering algorithms of public keys and blind signatures to ensure the confidentiality and integrity of data, as well as to provide proof of the effective source of the same.

(3) These threats are compounded by the real possibility that the communications infrastructure could undergo a denial of service attack on voting day and thereby deny voters their legitimate right to vote. This problem is quite difficult to solve if voting is cast from home over the Internet, owing to the open, universal character of the net. Therefore, the usual countermeasures against this threat are based on constraining the scope of exercise of voting rights: voting from only specific places with the use of private virtual networks.

1.3 Telematic voting and alteration of results

Another danger faced by any voting system, whether traditional or not, is the possible alteration of the voting results from within the system itself. That is, when the results published do not truly reflect the votes cast (i.e., an election is rigged). In traditional voting, this risk is offset by the physical existence on paper of votes cast and the use of supervisors that monitor both the voting and tallying processes. However, in telematic voting, this risk is often underestimated, in spite of the fact that studies of the problem [Me01] indicate that one of the factors preventing social acceptance of these systems is the perception by citizens that it is quite easy to modify electronically stored data.

One of the solutions proposed to deal with this problem involves issuance of a receipt that would allow voters to be sure that the vote has been cast as desired. However, the existence of a receipt showing the vote poses the risk of its use as an element of coercion or sale of votes. Thus, alternative solutions have been discussed [Ch04], which in our view are not fully satisfactory, as they offer only an acceptable probability that votes have been included correctly in the tally.

Nevertheless, few voting schemes address the problems inherent in voting through telematic networks that require powerful verification tools to ensure the accuracy of results against possible collusion between system agents, while adding control elements for monitoring the proper execution of the entire voting process.

1.4 Solution proposed

This article proposes a system of telematic voting (called VOTESCRIPT), that reinforces verification processes as a crucial element to achieve full acceptance of the system by voters. Its most noteworthy features are the following:

a) Voting from specific sites (polling stations, kiosks) to avert both denial of service attacks and coercion of voters.

b) Use of a Java Card to store voting software and data related to the voting process. Inclusion of a receipt stored on the card, which is properly protected to prevent its use for coercion or vote selling.

c) Involvement of vote monitors to supervise and attest to the proper functioning of the voting process. The proposed system arises from the experience of this research group in contributing to the development of a theoretical model used by the Spanish Royal Mint to create its own voting system, for which field tests of the prototype were conducted in Ávila (Spain) in 03/2003. Smart cards technology available at that moment did not allow the prototype to fulfil all the specifications included in the theoretical model. Currently, a complete prototype of VOTESCRIPT has been developed making use of Java Cards.

2 Architecture

The VOTESCRIPT system is based on the use of blind signature algorithms as proposed by Chaum [Ch83] and a smart Java Card that would store the voter keys, the vote delivery applet and the voting receipt, among other things. It relies on the voting designs proposed by Fujioka [FOO93] and Cranor [CC96], while substantially improving upon them, as explained below.

2.1 Agents and persons

The communication scenario of VOTESCRIPT involves a set of automatic systems as follows:

(1) Authentication Points (APs). Computers equipped with card readers – but without cryptographic capacities – in which the voter engages in the authentication process.

(2) Ballot Points (BPs). Like the APs, these are computers equipped with card readers, though without cryptographic abilities, in which voters cast votes. A voter can cast a vote in any of the existing BPs.

(3) An Administration System (AS) that could be considered official, which authenticates voters.

(4) Several Intervention Systems (ISs). These are appointed by each of the groupings of electors or the candidacies authorized to supervise voting, with the mission of supplementing the work of the Administration System.

(5) A Ballot Box (BB) that collects votes cast and returns voting receipts.

(6) A Tallier (T), which could be considered official, for tallying votes following the end of the vote reception period. The key is a secret shared between the Administration and the Intervention Systems, and is obtained at the end of the vote reception period.

(7) Several Tally Intervention Systems to supervise the task previously performed by the official Tallier.

(8) Verification Points (VPs) to enable voters to see that their vote has been included and properly accounted for.

(9) A Tally Board that will hold the results published for a short period of time. The key is a secret shared between the administrator and the intervention systems, and is obtained when the individual verification process is performed.

(10) Voters. Each voter has a smart voting card, a Java Card that contains not only cryptographic algorithms specially designed for VOTESCRIPT, but which also executes part of the voter software.

(11) The Election Authority (EA). Consists of a group of persons responsible for general oversight of the system and charged with addressing any complaints.

2.2 Description of protocol

During the voting period, citizens that wish to vote will go through the steps described below, which constitute the VOTESCRIPT protocol (Figure 1).

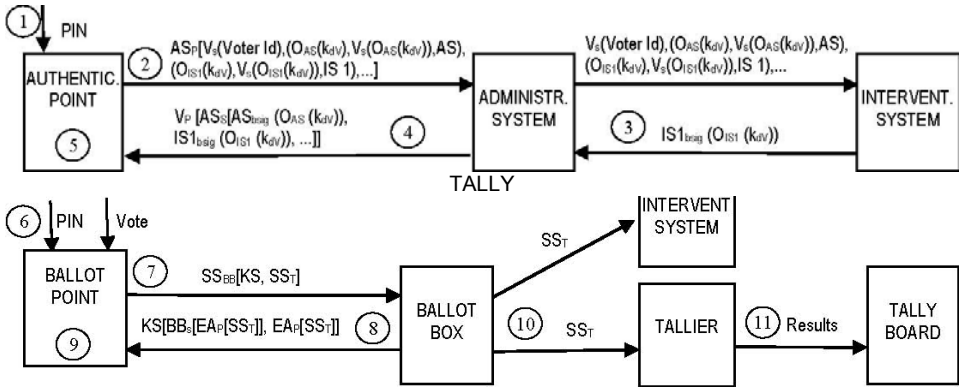

Figure 1: Voting protocol

Voter-Authentication Point Relationship

1 At the Authentication Point, the Voter inserts the Voter Card and is authenticated with a PIN or a biometric mechanism of identification.

2 The Voter Card, which contains two Voter keys – a public and private one – generates a pair of asymmetrical keys for voting (k_{dV}, k_{cV}) and a series of opacity factors. The key k_{dV} is opaque for the Administration System and for each of the Intervention System. The card signs the *voter ID* and all the opaque keys and ciphers the result with the public key of the Administration System. The Authentication Point sends this information to the Administration System.

$AS_P\ [V_s\ (Voter\ Id),\ (O_{AS}\ (k_{dV}),\ V_s\ (O_{AS}\ (k_{dV})),\ AS),\ (O_{IS1}\ (k_{dV}),\ V_s\ (O_{IS1}\ (k_{dV})),\ IS\ 1),\ ...]$

3 The Administration System reads and deciphers the data received and sends all the data to all the Intervention Systems. Each of the Intervention Systems, in the same way as the Administration System, checks that the Id is on the list of valid Ids, that the signature of the Voter making the request is correct and that the card has not undergone authentication previously. If not, the reception is rejected. If everything is in order, the Administration System and each Intervention System blindly signs the relevant opaque k_{dV} key.

4 The entirety of the opaque keys are signed by the Administration System with its private key and ciphered with the voter's public key, and then sent to the Authentication Point.

VP [ASS[ASbsig (OAS (kdV)), IS1bsig (OIS1 (kdV)), ...]]

5 The Authentication Point sends to the Voter Card the data received from the Administration System, so that the smart card receives the k_{dV} signed by the Administration System and by the Intervention Systems. It then verifies that the signatures are correct, and if they are, it stores them, so that they will constitute the vote delivery authorization for the voter during the voting process.

Voter - Ballot Point Relationship

6 At the Ballot Point, the Voter inserts the Card and is authenticated by means of a PIN or a biometric identification mechanism.

7 The Ballot Point asks the Voter to vote. In the Voter Card, the vote chosen is ciphered with k_{cV} and a piece of information is created with the ciphered vote, the k_{dV} and k_{dV} keys signed by the Administration System and the Intervention Systems. Then this piece of information is "stored" in a *T Secure Envelope* between the smart card and the Tallier. A *symmetrical* key (KS) is generated, joined to the T Secure Envelope and stored in a new *Secure Envelope BB*, which is sent to the Ballot Box.

SEBB[KS, SET]

8 The Ballot Box, after eliminating the *Secure Envelope BB* protecting the information received, obtains the *KS* and the *T Secure Envelope*. The Ballot Box stores the *T Secure Envelopes* received until the voting period is over. Based on the data protected with *T Secure Envelope*, it returns a receipt to the Ballot Point that preserves the anonymity of the voter. To generate the receipt, it performs the following operations: a) it ciphers *T Secure Envelope* with the public key of the Election Authority b) it signs it with its private key, and c) ciphers the receipt with the symmetrical key it received from the Ballot Point.

KS[BBs[EAP[SET]], EAP[SET]]

9 In the Voting Booth, information received is delivered to the Voter Card, which obtains the receipt, and it verifies the signature by the Ballot Box. The vote receipt is stored in the Voter Card and only the Electoral Authority can gain access to the data of the receipt in case of a complaint after the end of the voting process.

Opening the Ballot Box and tallying the votes

10 Opening the Ballot Box requires the physical presence of the Administrator and a sufficient number of scrutineers, who will insert their smart cards in the readers and authenticate themselves, either biometrically or with a PIN. The Ballot Box randomizes everything it receives and sends it to the Tallier and the Tally Intervention Systems, while also providing persons with management and supervision responsibilities over the electoral system a list of the data that has been sent. At that moment, all the information received by the Ballot Box during its operations is deleted. The restricted disclosure of the records transferred by the Ballot Box will help verify that the Tallier and the Tallier Intervention Systems are receiving the same information, so as to enable identification any element causing a malfunction in the event an alteration of the vote is detected.

11 The vote tally is then undertaken. Prior to reading the results, the System Administrator and the Scrutineers once again use their smart cards – with a shared secret procedure – to jointly provide the Tallier and the Tally Intervention System their private keys (which are stored and hided until that moment) needed to begin operations. After receiving all the information from the Ballot Box, the Tallier opens the T Secure Envelopes, performs the vote tally and sends to the Tally Board the information, composed of a kdV key and the kdV key signed by the Administration System and the Intervention Systems, along with the deciphered vote. The Tally Board announces the results of the vote to persons with management and supervisory responsibilities over the electoral system.

2.3 Voter Card

Along with the procedures designed to enable audits of software and the results, one of the pillars undergirding the strength of the proposed voting system is the possession of a smart card on the part of each voter. To meet the essential requirements of a voting system the smart card includes self-protection mechanisms against any attempt at reading or writing by equipment that is not standardized for the voting system.

The fact that all citizens make use of a smart card that enables them to sign information to offer proof of origin and decipher confidential information is not sufficient to provide the guarantees required by a voting system. A smart card is needed with cryptographic capacities that have been specially designed for this project, enabling performance of sensitive cryptographic processes, in addition to the usual tasks of identifying its holder. If performed outside the card, these processes would leave a trail of operations in machines that could be subject to subsequent analyses, with the intention of breaking the basic principle of secret voting.

The voter's smart card will internally generate keys for subsequent use. Among these are two pairs of asymmetrical keys: i) one composed of a secret key used to sign or decipher, and another of the public key, which is duly certified and disclosed by the responsible authority, to guarantee the identity of the holder. ii) The other pair is similarly useful to the prior one, but guaranteeing, this time, the anonymity of the holder. Cryptographic mechanisms ensure that the card bearer is a legitimate voter, that two voters will not have the same pair of keys, or that a single voter will not have more than a pair of keys for this use. The cryptographic procedures used will also ensure that no internal or external agent or collusion between them will be capable of disclosing the identity of the voter. This key will be used to legitimate the vote, which will come ciphered from the card so that it can be deciphered only by the Tallier in the tally phase.

Cryptographic processes to be executed inside the card also require the existence of a session key and opacity factors, knowledge of which by third parties would compromise the security of the system to the same extent as if the secret keys were disclosed. Thus, the smart card is the valid secure format, for it will generate keys and factors and, when necessary, share the keys with other agents; it will come from the card with all the confidentiality guarantees offered by cryptographic mechanisms, namely ciphering with the public key of the receiver.

Ciphering with a public key generally offers confidentiality guarantees; however, in voting processes, the number of messages to be ciphered is limited and sheer force may be sufficient to disclose the message. Thus, the card also includes the mechanism of random chains, which must also be generated inside the card, since it is indispensable that the chain be unknown to prevent successful violation of the secret vote.

For the purposes of use following publication of the results, the Ballot Box will give the voter a receipt for the vote. This receipt is designed so as not to expose the voter to the risks of coercion, since it is ciphered with the public key of the Electoral Authority. In this project, the citizen's smart card will securely store the receipt, having first verified its authenticity and storing it in a form that it can be read only by the Electoral Authority.

3 Individual verification and global verification

This project envisages two types of verification of results, which as a whole will act as a deterrent to temptations to commit fraud by the persons responsible for the operations of the different systems, since not only will the malfunction be detected, but also the system in which the malfunction has occurred will be identified unequivocally.

There are two types of verification: global and individual. Global verification of results is undertaken by candidates' representatives or by groupings of electors authorized to perform monitoring of the process. Individual verification is effected by the voter him or herself, with protection against possible coercion by means of properly designed procedures. As already described, the work of the Administrator during the voting process is supervised by the Intervention Systems in such a way that any anomalous issuance or denial of authorizations would be detected.

After the period provided for voters to deliver their votes to the Tallier, the content of the Tallier will be delivered to the Ballot Box and a copy of the data will be received in the Tally Intervention Systems, thus dissuading the Tallier from the intention of eliminating, adding or modifying votes. It would still be possible for the Ballot Box to destroy votes prior to delivering them to the Tallier and the Tally Intervention Systems. This circumstance – apart from raising less interest, since the destruction would be carried out against ciphered pieces of information, the true meaning of which is unknown – would be detected with individual verification procedures by means of the vote receipt signed by the Tallier and stored in the voter's smart card.

3.1 Global verification

Each Scrutineer will have a machine – Tally Intervention System – which will load a copy of the information that the Ballot Box delivers to the Tallier. This machine shall be audited in advance by experts trusted by system managers to achieve complete confidence that it can only perform a vote tally. Any divergence between the votes obtained by the Tally Intervention System and those obtained by the Tallier and published in the Tally Board would be a sign of an anomaly. Thus, neither the Tallier nor the Tally Board can alter – i.e., add, eliminate or modify – votes, nor will they are able to accept the validity of votes that have not been properly authorized. Both for lists of records received by the Tallier and for lists of information delivered to each candidacy, a validity period shall be in effect, so that once the specified time has elapsed and the election is considered valid, the lists must be destroyed in an audited procedure.

3.2 Individual verification

Once voting has concluded and the results have been published, each Voter can independently check that his or her vote has been properly accounted for. This verification is performed by a voter at their own initiative, with resources available to ensure their anonymity and protection from coercion. The Voter need only go to a Verification Point – in an individual manner – use the Voter Card and ask to be shown the vote associated to the information published by the Tallier and the information stored on the card. At this site, the same measures must be taken to ensure that the voter is protected against external surveillance as were taken when casting a vote at the Ballot Point. If the voter does not accept the vote shown at the Ballot Point, the person may appeal to the collegial body called the Electoral Authority, which is responsible for overseeing the proper functioning of the system, and which addresses all complaints lodged by voters. When a complaint is made by a voter regarding treatment of their vote, the Electoral Authority can obtain the vote receipt stored in the smart card of the voter and will use all cryptographic proofs available in the system to investigate the validity of the complaint. The Electoral Authority will obtain solid cryptographic proofs to determine where the anomaly lies and what agent is responsible for it.

4 Innovations of VOTESCRIPT system

This section highlights the main innovations provided by the VOTESCRIPT system, with a comparison of the solutions it proposes with those contained in the main voting schemes used as a reference in this field.

(1) The VOTESCRIPT system provides an individual verification system that enables each voter to check, in specific places and during a determinate period of time, whether their vote has been properly included and accounted for. The innovation as regards other solutions lies in the fact that the process is private, as the voter can at no time show to unauthorized third parties the content of the vote, thus preventing the buying and selling of votes or extortion.

(2) The existence of Intervention System is one of the main innovations of this system, since it enables monitoring of the entire electoral process by groupings of citizens or by duly authorized candidacies. Global verification made available to scrutineers provides solid cryptographic proofs that make it possible to demonstrate unequivocally whether the system has operated fraudulently or not.

(3) The cryptographic cards designed for the project guarantee the identity of the voter, and also perform all functions of ciphering and deciphering, generate of session keys and authentication of signatures in the card itself, with the aim of blocking access to critical information by malicious users. The voter card is a Java Card that contains vote-casting software, while it stores certain information associated to the vote¬casting process, the receipt, with a view to enabling subsequent verification.

(4) There is a collegial body called the Electoral Authority, which is charged with the tasks of overseeing the proper functioning of the system and addressing any complaints made by voters. In the event of a complaint by a voter about the treatment given their vote, the Electoral Authority shall discover and compare all the cryptographic proofs in the system in order to check the validity of the tally.

(5) The system also ensures that the content of a vote cannot be disclosed in the future. Cryptographic presentation of the vote through cryptographic algorithms means that these systems cannot gain knowledge of the vote's content, but it does not ensure that the advancement of cryptoanalysis will not enable it to be known in the future.

5 Conclusions

Today, experiences in telematic voting abound, and these initiatives always highlight the benefit for voters of being able to cast a vote from any computer connected to the Internet. However, the euphoria seen in these experiments makes both organizers and voters overlook the fact that these systems are unable to demonstrate that the results published have not been tampered with prior to their release.

The system presented herein is fully verifiable, as the system's strength lies in its provision of cryptographically solid and secure pieces of information that can be used as proof before third parties in case of litigation or rejection of the results of the process. In the VOTESCRIPT system, as in other recent proposals for telematic voting, the smart card serves as a security token that allows for the protected storing of private keys that enable the voter to undertake authentication in the system and cast a vote in reliable manner. Nevertheless, the smart card plays a much more important role in VOTESCRIPT than these other systems.

The system presented constitutes a valid solution to traditional problems of voting systems, and it can counteract the understandable wariness of voters towards telematic voting processes. E-voting systems that aspire to replace traditional voting systems must include the positive aspects of these traditional arrangements, while offering new functionalities such as those presented here in order to deserve the trust of the citizenry.

References

[CC96] Cranor, Lorrie F.; Cytron, Ronald K.:. Design and Implementation of a Practical Security-Conscious Electronic Polling System, WUCS-96-02, Informatic Department of the University of Washington, St. Louis, USA, 1996.

[CGP02] Carracedo, J.; Gómez, A.; Moreno, J.; Pérez, E.; Carracedo, J.D.: Votación electrónica basada en criptografía avanzada (Proyecto VOTESCRIPT). II Congreso Iberoamericano de Telemática. CITA'2002. Mérida, Venezuela. 2002.

[Ch04] Chaum, D.: Secret-Ballot Receipts and Transparent Integrity. IEEE Security & Privacy. Vol 2 N1. January-February 2004; pp 38-47.

[Ch83] Chaum, D.: Blind signatures for untraceable payments. Advances in Cryptology, Crypto '82, Springer-Verlag, Berlin. 1983; pp. 199-203.

[In06] Indian Voting. http://www.ensl.cs.gwu.edu/voting/India, last accessed February 2006.

[Me01] Mercuri, R.: Testimony presented to the U.S. House of Representatives Committee on Science. http://www.house.gov/science/full/may22/mercuri.htm. 2001.

[OMA99] Ohkubo, M; Miura, F.: Abe, M.; Fujioka, A.; Okamoto, T.: An Improvement on a Practical Secret Voting Scheme. Lecture Notes in Computer Science 1729, Springer-Verlag, Berlin, 1999; pp. 225-234.

[Re04] Rezende P.: Electronic Voting Systems. Is Brazil ahead of its time?. Cryptobytes, Vol 7, N. 2, RSA Security Laboratories, USA. Fall 2004; pp. 2-8. http://www.rsasecurity.com/rsalabs/cryptobytes/CryptoBytes_Fall2004.pdf, last accessed February 2006.

[Ri99] Riera i Jorba, A.: Design of Implementable Solutions for Large Scale Implementable Voting Schemes. PhD thesis, Universitat Antónoma de Barcelona, 1999.