VOTESCRIPT: telematic voting system designed to enable final count verification

Ana Gómez Oliva[1], Emilia Pérez Belleboni[1],
Sergio Sánchez García[1], Justo Carracedo Gallardo[1],
Jesús Moreno Blázquez[1], José David Carracedo Verde[2]

[1]Dpto. de Ingeniería y Arquitecturas Telemáticas de la Universidad Politécnica de Madrid
Ctra. Valencia km. 7. 28031 Madrid. Spain
T. +34 91 336 78 18
{agomez, belleboni, ssanche, carracedo, jmoreno}@diatel.upm.es

[2]Observatorio para la Democracia Digital y los Derechos de la Ciudadanía en Internet
Campus de Somosaguas. 28223 Madrid. España
jdcarracedo@yahoo.es

Abstract

In this paper we present a global description of a telematic voting system based on advanced cryptography and on the use of smart cards (VOTESCRIPT system) whose most outstanding characteristic is the ability to verify that the tally carried out by the system is correct, meaning that the results published by the system correspond with votes cast. The VOTESCRIPT system provides an individual verification mechanism allowing each Voter to confirm whether his vote has been correctly counted. The innovation with respect to other solutions lies in the fact that the verification process is private so that Voters have no way of proving what they voted in the presence of a non-authorized third party. Vote buying and selling or any other kind of extortion are prevented. The existence of the Intervention Systems allows the whole electoral process to be controlled by groups of citizens or authorized candidatures. In addition to this the system can simply make an audit not only of the final results, but also of the whole process. Global verification provides the Scrutineers with robust cryptographic evidence which enables unequivocal proof if the system has operated in a fraudulent way.

1. VERIFICATION: THE KEY POINT OF THE TELEMATIC VOTING SYSTEM

Currently, many Governments and Administrations of different countries are promoting the development of pilot schemes on telematic voting. We understand a telematic voting system as one in which votes are computer generated and then sent to a remote Polling Station by means of telematic networks.

A telematic voting system must not only be able to offer the same security guarantees as those provided by a traditional voting system (such as: protecting Voter anonymity, avoiding vote casting by non-authorized Voters or multiple voting, while ensuring a correct vote count), but also to guarantee suitable protection of votes cast while in transit through the network. In this sense the system must prevent votes from being recognized, modified or excluded. Nevertheless, few schemes published till now cover these new requirements inherent to telematic voting, such as the need for powerful verification tools which help guarantee and prove that the results are correct even in the event of possible collusion between the system agents. Nor do these systems provide for Scrutineers[1] who undertake traditional supervision of the correct progress of the entire voting process.

In Spain, the Electoral Processes Department of the Ministry of Interior together with the Spanish Royal Mint undertook a project whose purpose was to study the viability of implementing an electronic voting system as an alternative to the present postal vote for Spanish residents abroad.

This research group, linked from its origins to the above mentioned project, developed a theoretical model for the voting system. The Royal Mint implemented its own subset of our project, tested in El Hoyo de Pinares (Spain, Ávila) in March of 2003.

In order to develop the theoretical model we have worked in two different and complementary areas: the security of the entire voting system and the exclusion of any cultural barriers and suspicions which might hamper its acceptance by citizens. While the corresponding engineering tasks were being performed, the psychological, politological and legal analysis necessary to determine the system’s viability was also carried out [6].

In this paper we present an improved version of the developed system implemented by the Royal Mint and tested in El Hoyo de Pinares, reinforcing the verification aspect as the key point in achieving wholehearted approval by society.

2. COMMUNICATION SCENARIO

The VOTESCRIPT system[2] supports telematic votes in an environment in which Voters cast their votes from any point provided for this purpose and these votes are collected in a remote ballot box. VOTESCRIPT aims to telematically reproduce the decentralized control guarantees of the conventional system, based on the existence of different polling stations, each equipped with a group of persons responsible for their functioning.

2.1. AUTOMATIC AGENTS AND SYSTEMS

A group of automatic systems using only previously published programmes takes part in the communication scenario considered in VOTESCRIPT, with a consequent possibility of evaluation and audit performed by all the entities involved in the voting process. This group of systems is shown in Figure 1. They are as follows:

[1] Scrutineer: an official examiner or counter of the votes in VOTESCRIPT system acting on behalf of the citizens or candidatures

[2] This system has been developed within VOTESCRIPT projects (Secured Electronic Voting based on Advanced Cryptography) sponsored by National Council for Science and Technology of Spain (TIC2000-1630, TIC2002-4223 and TIC2003-2141)

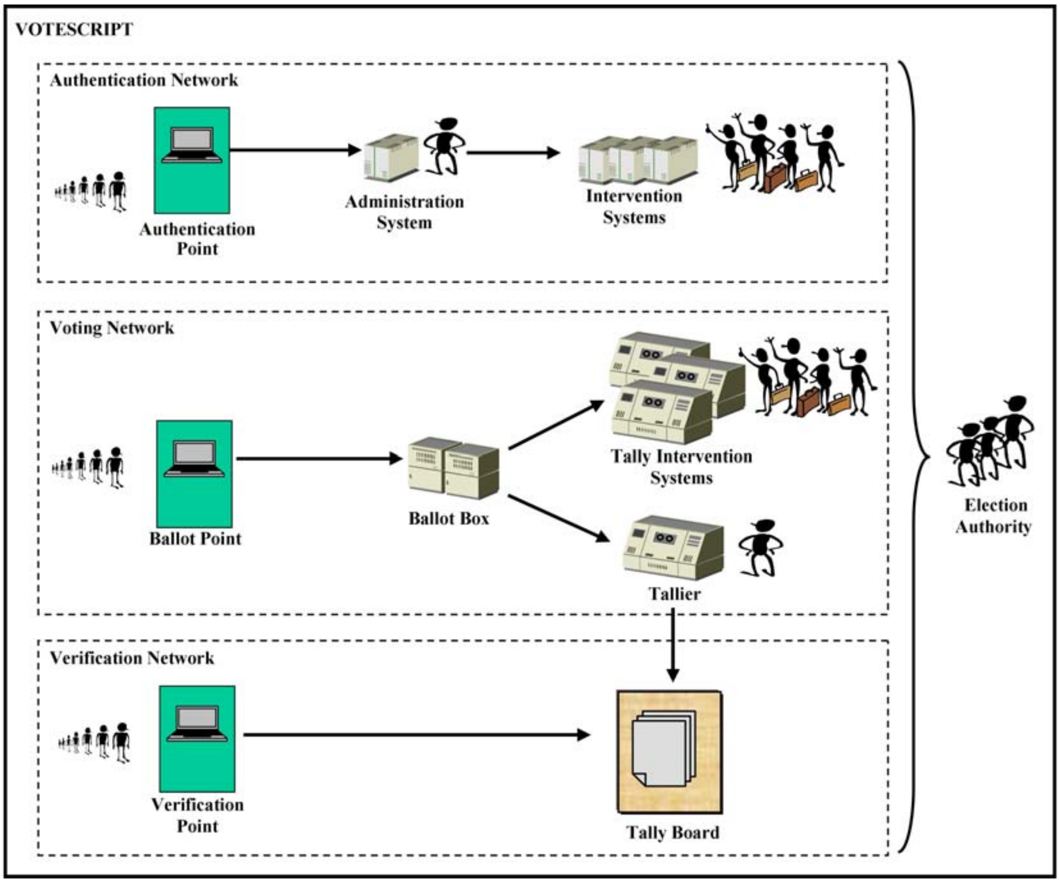

Figure 1. Architecture of the VOTESCRIPT system

- Authentication Points (APs). These are computers equipped with a card reader but with no cryptographic capacity. Here the Voter begins the voting process. In VOTESCRIPT the Voter may choose any of the available APs to authenticate identity.
- Ballot Points (BPs). In the same way as the APs these are computers equipped with a card reader but with no cryptographic capacity. Here the Voter finds all the resources necessary to help him cast the vote. The BPs are installed in cabins which isolate the Voter from external interference. In VOTESCRIPT the Voter may cast his vote at any of the available BPs.
- An Administration System (may be considered official), in charge of the Voter authentication process.
- Different Intervention Systems (ISs). These are computers managed by each of the citizen's group or candidatures authorized to supervise voting, whose objective is to complement the Administrator's tasks. The fact that the ISs are controlled by different candidatures that support opposed interests guarantees that collusion between these agents within the system will not occur.
- A Ballot Box (BB) collects the electronic votes cast by the Voters and returns the voting receipts. BB is not able to decrypt the vote.
- A Tallier (may be considered official) counts the votes. Its private key is shared secret, held only by the Administrator and the Scrutineers and it is revealed only when votes reception is complete.

- Different Tally Intervention Systems to supervise the task carried out by the official Tallier.
- Verification Points allowing the Voter to confirm that his vote has been correctly counted.
- A Tally Board where the results are kept and shown for a short period of time. Its private key is a shared secret, held by the Administrator and the Scrutineers and revealed just before individual verification starts.
- Smart cards allowing owner identification and decoding of confidential information addressed to it, plus signature of all information requiring proof of origin and the integrity guarantees. In particular, every Voter possesses a voting smart card Java Card (VC) [11] which includes cryptographic algorithms specially designed for VOTESCRIPT and also executes a part of the Voter's application in order to increase the global security of the system.

2.2. PERSONS PARTICIPATING IN THE PROCESS

As mentioned in the previous paragraph, the system contemplates the existence of a group of persons directly present in the voting, counting and verification processes. All these persons must possess some kind of smart card which would help them to interact with the VOTESCRIPT agents.

- Voters.
- An Administrator of the Administration System.
- Scrutineers responsible for each one of the Intervention Systems.
- Election Authority (EA), consisting of a group of persons whose responsibilities are general control of the system and resolving possible complaints.

2.3. SMART CARDS: KEYS AND IDENTIFIERS

As a previous step to voting, every Voter will have received the Voter's Card and the Voter's identifier which is known to all the members taking part in voting control.

The Administration System, the Intervention Systems, the Ballot Box, the Tallier together with the Tally Intervention System, the Tally Board and the Election Authority each have their own key pair (a public and a private key). All their public keys, by means of their correspondent certificates are known to all telematic agents and to all the persons participating in the voting system using their smart card.

The smart card enables, on one hand, the Voter's and agent's private keys to be kept safely in order to guarantee their identity, and on the other hand, permits safe storage of the pieces of information generated throughout the voting process.

In the voting process, the Voter's applications are in charge of dialoguing with the Voter to authenticate him and to ask for his voting option as well as to carry out secure dialogue among the different system agents. This process is undertaken by means of appropriate cryptographic operations inside the card. From a practical point of view, this solution is not feasible using a conventional smart card, but it can be obtained using the new generation of smart cards: Java Cards. In fact, these cards, besides pooling all the security requirements of the conventional smart cards, also allow storage and later execution of different user applications, developed in Java language. This means that it is a suitable location for the Voter's application due to the new features of Java Card combined with the tamper-proof characteristics of any type of smart card.

3. GLOBAL BEHAVIOUR OF THE SYSTEM

3.1. OUTLINED PROCEDURE OF VOTE DELIVERY

During a limited period, the citizens will fulfil the steps we describe in the following paragraphs. Meanwhile the Administration System and the Intervention Systems are ready to issue authorizations for the legitimate Voters who will request them and the Ballot Box is ready to receive the votes and return the receipts. (See Figure 1)

Relation between the Voter and the Authentication Point

1) Once at the Authentication Point, the Voter introduces his Voter's Card (VC) into the card reader. The Authentication Point checks the validity of the card by means of a generic identifier possessed by all cards participating in voting. Therefore, any attempt to introduce a different kind of card into the card reader will be rejected. The Voter authenticates himself on his card by means of a biometric identification mechanism.[3]
2) The Voter's Card contains the key pair (the public and the private key) of Voters. Additionally, within the VC an asymmetric voting key pair is generated (k_{dV}, k_{eV}), which is stored in such a way that not even the Voter himself may read it. The card itself also generates the blinding factors [14] to blind the previously generated k_{dV} key (using the correspondent blinding factor) for the Administration System and for each one of the Intervention Systems, creating a k_{dV} key blinded for each one of the destiny entities of the message. The card signs a piece of information which consists of a Voter's identifier and all the previously blinded keys, after which it encrypts all this data with the public key of the Administration System for ensuring confidentiality.
3) Using the information referred to in the previous step, the Authentication Point generates an APDU (Application Protocol Data Unit) and sends it to the Administration System.
4) The Administration System reads and decrypts the data inside the APDU and then sends all the information to all the Intervention Systems. Every Intervention System, in the same way as the Administration System, will have to confirm that the received Voter's identifier is correct[4]. That is to say, it confirms that the identifier is included in the list of valid identifiers, that the signature of the Voter making the request is valid and that no blinded key

[3] In the framework of our proposal the smart card is the one to store the biometric data using the Authentication Point as a simple intermediary. This kind of data does not travel through the network and is neither stored in a BP, making impossible a creation of "biometric" lists.

[4] The fact that the Administration System checks the validity of the request at the same time as the Intervention Systems permits to keep a log of such an incident (in the same way as in a conventional voting by means of a ballot in Spain).

associated to the mentioned identifier has been previously received. Otherwise, the request is rejected[5].

5) Once confirmed that the received Voter's identifier is valid, every Intervention System will sign its correspondent blinded k_{dV} key and will return the result to the Administration System. The Administration System does the same with its corresponding blinded k_{dV} key and attaches it to the blinded keys signed by the ISs, creating in this way a *signed keys set* which will be transformed into an "authorization" once they are decrypted and unblinded by the Voter's Card.
6) This *signed keys set* is signed by the Administration System and encrypted with the Voter's public key, after that it is sent (by means of an APDU) to the Authentication Point. In this way the VC will be the only one capable of reading the *signed keys set* (data confidentiality). It also has the guarantee that the Administration System was the one to return it the *signed keys set*.
7) The data contained in the APDU, which has been received from the Administration System, is delivered to the Voter's Card by the Authentication Point. The VC decrypts the information using first the Voter's private key and then checks the Administration System signature. Once the blinded *signed keys set* are read (step 5), the VC excludes the blinded factor, obtaining the k_{dV} signed by the Administration System together with the k_{dV} signed by each Intervention System. Next it checks that Administration and Intervention System signatures on the keys are correct. If this is the case, interaction between the Voter and the Authentication Point has finished and the Voter's Card keeps the signatures of its k_{dV} which will next be used as the authorization during the voting process. There is only one legitimate Voter able to possess it and this Voter may only possess a single authorization.

Relation between the Voter and the Ballot Point

8) There are resources which will help the Voter to issue his vote and to send it to the Ballot Box at the Ballot Point (BP). The Voter, in the same way as he did at the AP, authenticates himself on the Card.
9) The BP asks for the Voter's vote by means of a dialogue in which the text and images simplify the Voter's choice. The vote to be delivered is encrypted within the Voter's Card with k_{eV} (*vote encrypting key*).This implies that the vote can only be decrypted by using k_{dV} key (*vote decrypting key*), which is the previous one's pair. In this way the vote and the "authorization" signed by Intervention and Administration Systems are inseparably interlinked.

   The VC creates a piece of information containing the encrypted vote, the k_{dV} key and the authorization. Next this piece of information is "put" inside the *Secure Envelope T* (a *Secure Envelope T* is confidential to the Tallier)[6]. After that a symmetric key is generated within the Voter Card which joins the *Secure Envelope T* and both are "put" inside a new *Secure Envelope BB* which only a Ballot Box can open. Next the Card delivers the *Secure Envelope BB* to the Ballot Point in order to be sent immediately to the Ballot Box. This double secure envelope, together with the procedures needed to put the Tallier into

[5] In this paper we do not take in consideration the behaviour of the system in case of incidents or possible communication problems.

[6] The mechanism used for this *Secure Envelope* is similar to the one usually called *Secure Channel* which offers major security protections than the conventional *digital envelope.*

operation, guarantees that it is impossible for any entity or group of entities to find out the partial results while there are still Voters waiting to cast their vote.

10) At the Ballot Point an APDU with the *Secure Envelope BB* is generated and it is sent to the Ballot Box so confidentiality is guaranteed.
11) After excluding the *Secure Envelope BB* which protects the information received, the Ballot Box gets the symmetric key and the piece of information contained in the *Secure Envelope T*. The Ballot Box retains these *Secure Envelopes T* until the voting period is finished. In order to generate the voting receipt, the Ballot Box carries out the following operations:
    a) Signs the *Secure Envelope T* (received in the previous step).
    b) Encrypts this piece of information with the Election Authority's (EA) public key. This encrypted information will be the voting receipt.
    c) Signs the voting receipt.
    d) Encrypts the voting receipt signed in the previous step with the symmetric key received from the Voter Card.

    Once these four operations are completed, the Ballot Box sends the result to the Ballot Point.
12) The Ballot Point delivers the received information to the Voter Card which decrypts the information, obtaining the voting receipt. Next it verifies that the Ballot Box signature is correct (even though it can not find out its content as it is encrypted with the public key of the Election Authority). The voting receipt is stored in the Voter Card and it is available only for the Election Authority (according to the rules established) once the voting process is finished in case of a claim.

    The Voter is informed at the Ballot Point that the process of delivery of his vote has ended. A Voter Card which has completed the previous process and has stored its receipt, will reject a new process of vote delivery, even if the Voter, its owner, tries to do so (the card is tamper-proof) guaranteeing that each Voter may only vote once.

3.2. OPENING BALLOT BOX AND VOTE TALLYING

The Tallier and the Tally Intervention System are the only ones who can open (read) these votes after the Administrator and the Scrutineers have collaborated in the process of generating their secret key (votes are protected inside the *Secure Envelopes T*).

1) To proceed to the opening of the Ballot Box the physical presence of the Administrator and enough Scrutineers is required (depending on the rules established). These persons are to insert their respective smart cards into the Ballot Box' card readers prepared for this purpose and they are to authenticate themselves on them biometrically or by means of a PIN. The opening process consists in modifying the order of appearance of the records by the Ballot Box and in sending them to the Tallier and to the Tally Intervention Systems. At the same time the Ballot Box provides persons responsible for the management and those responsible for supervising the electoral system with a list containing all the information sent (the encrypted votes inside the *Secure Envelopes T*). At this moment all the information that the Ballot Box has been collecting during its work is removed. The removal process will be audited by persons with specific authorization. The data concerning the transferred records is known also by a group of persons in order to provide mechanisms to

check that the Tallier and the Tally Intervention Systems receive the same information and, as explained below in the verification paragraph, to identify the element causing a malfunction in case an alteration of the votes is detected.

2) Next the votes are counted. Before decrypting the votes once again the Administrator and the Scrutineers with their smart cards (by means of a shared secret procedure) together supply the Tallier and the Tally Intervention Systems with their private key (which has been hidden till this moment). This key permits the Tallier and the Tally Intervention Systems to come into operation. The Tallier "opens" the *Secure Envelope T* which contains the vote information described in step 9 above. For each vote it checks that the k_{dV} (used to open an encrypted vote) has been correctly signed by the Administration System and the Intervention Systems, and if so, it decrypts the vote. The results obtained by Tallier and the Tally Intervention Systems must be the same.

   The k_{dV} key signed by the Administration and the Intervention System guarantees that none but a single authorized Voter can deliver a valid vote. The inseparable interlink between the Vote and the Authorization takes place because only the Voter's Card knows the value of the symmetric k_{dV} key, (k_{eV}). The integrity and the confidentiality of the Vote are guaranteed by the Secure Envelope procedures. Although the Voter's Card prevents the Voter from voting more than once, in the event this protection is violated, the Tallier will detect the k_{dV} duplicity and it rectifies this incident.

   Once the tally is completed, the Tallier transfers the information to the Tally Board which will make known the voting results to the persons responsible for management and supervision of the electoral system. These results are gathered in a list and its entries are as follows: a) a clear vote b) the k_{dV} key c) the k_{dV} key signed by the Administration System and d) the k_{dV} key signed by each of the Intervention Systems. This list and the tasks completed by Intervention Systems help to carry out the verification steps described in the following paragraphs.

The final results, made public to citizens, correspond to the votes for each candidature on the Tally Board.

3.3. VERIFICATION OF THE VOTING RESULTS

VOTESCRIPT allows two kinds of verification to be performed: individual verification by the Voter and global verification of the results by the candidatures or authorized citizen groups.

Individual verification, in which every Voter provides evidence stored in his card, will prevent the system (basically the Ballot Box) from the temptation of eliminating votes, since each Voter card contains a vote signed by the Ballot Box which should have been processed at the moment of the tallying. If the vote has been modified or excluded by the Ballot Box, it will not appear in the list of transferred records. If the vote has been modified by the Tallier, it has to prove that it has got another vote with the same k_{dV} signed by all Administration and Intervention Systems; otherwise there is evidence of the Tallier committing mistakes or fraud.

Global verification, together with the Intervention Systems supervising the tasks of the Administration System, detects any unauthorised vote cast as it would not be provided with a correctly signed Authorization.

3.3.1. Individual verification

Once the voting period has finished, each Voter may independently check if his vote has been properly included. This verification is carried out by the Voter on his own initiative making use of the resources guaranteeing his anonymity and protection from coercion.

The Voter should go to the Verification Point (always by himself), and uses his card to ask to be shown the associated vote.

At the Verification Point, in order to guarantee the Voter's protection from external espionage, the same measures as those to cast the vote at the Ballot Point must be taken.

Relation between the Voter and the Verification Point

The Figure 2 illustrates the communication explained below:

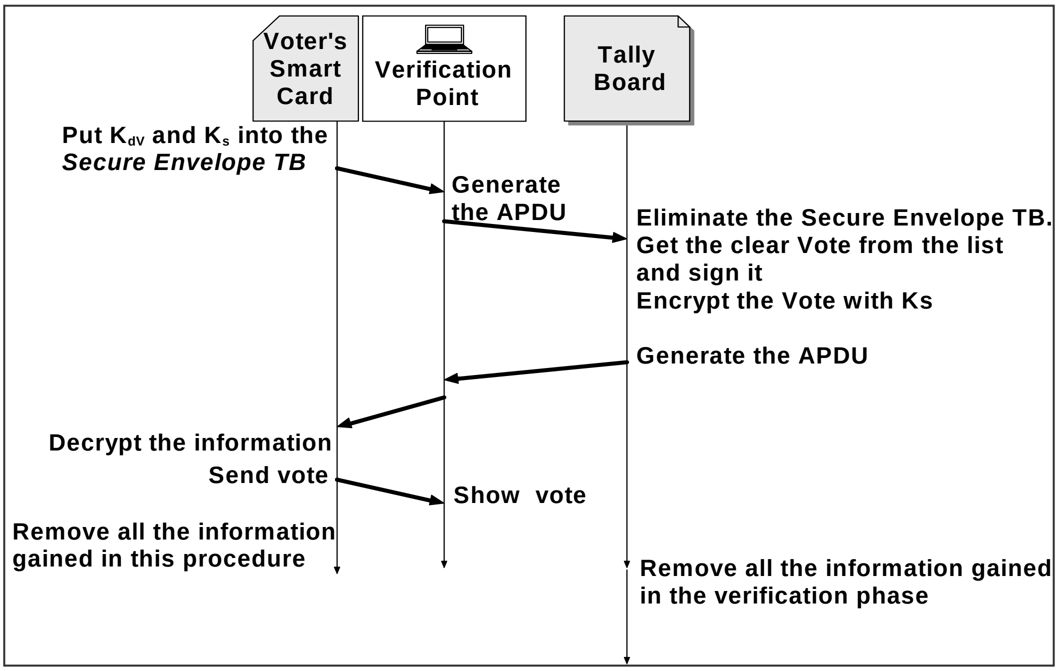
Voter's Smart Card
Verification Point
Tally Board
Put K_{dv} and K_s into the *Secure Envelope TB*
Generate the APDU
Eliminate the Secure Envelope TB.
Get the clear Vote from the list and sign it
Encrypt the Vote with Ks
Generate the APDU
Decrypt the information
Send vote
Show vote
Remove all the information gained in this procedure
Remove all the information gained in the verification phase

Figure 2. Dialogue among smart card, Verification Point and Tally Board

1) The system installed at the Verification Point has resources allowing communication with the Tally Board (TB). The Voter authenticates himself on the Voter Card in the same way as he did at AP (step 1 of Relation between the Voter and the Authentication Point).
2) By means of a dialoguing process between the Verification Point and the Voter Card, the Voter Card generates a symmetric key and creates a piece of information which contains the k_{dV} key and the symmetric key which are put inside the *Secure Envelope TB*. This Secure Envelope is immediately delivered confidentially to the Tally Board through the Verification Point.

3) The Tally Board obtains the k_{dV} key coming from the Voter's Card and accesses the previously published list containing the k_{dV} key besides the vote.
4) The Tally Board returns to the Verification Point one signed piece of information containing the vote associated to this k_{dV} key and encrypted with the symmetric key recently received inside of the *Secure Envelope TB.*
5) The Verification Point transfers this piece of information to the Voter's Card.
6) The Voter's Cards decrypts the received information, checks the TB's signature and if everything is correct, sends the clear vote to the Verification Point showing the Voter the associated vote in such a way that the Voter is the only one who can read it.
7) All the information collected during this transaction with the Verification Point is removed from the Voter's Card.
8) Once the established period to carry out individual verification has finished, the destruction process of all information (including the private key from the Tally Board) will be audited.

In case of non-agreement with the option seen, the Voter may lodge a complaint with the Election Authority.

After receiving the Voter's Card the Election Authority may unequivocally prove correct or incorrect vote processing, as it has resources independent of the previously described networks allowing confidential access to:

- The Voter's k_{dV} key stored in his card.
- The voting receipt sent by the Ballot Box to the Voter.
- The Tallier's records which relate the k_{dV} key signed by the Administration and the Intervention Systems, the clear k_{dV} and the vote encrypted with k_{eV} key.
- The information supplied by the Ballot Box while transferring its content to the Tallier and to the Tally's Intervention Systems.

Once in its possession and relying on the robust cryptographic evidence, the Election Authority will determine if the system has falsified the data.

There is a Secure Envelope (between the Voter and the Tallier) signed by the BB and encrypted with the EA's public key in the Voter's Card. As soon as the EA accesses the contents, it will verify that this piece of information has been supplied by the Ballot Box to the Tallier (and to the Tally Intervention Systems). If this is not the case, there is evidence of the vote's destruction by the Ballot Box. If this information has been transferred, the Election Authority will use the Tallier's secret key in order to "open" the *Secure Envelope T* stored in the card and will verify the result of the vote decrypt which must match with the information supplied by the Tally Board. An anomaly at this final stage will be also detected during global verification. Basically, this individual verification will prevent the Ballot Box from an attempt to exclude votes.

3.3.2. Global Verification

As has been already stated, after closing the Ballot Point, the Ballot Box will transfer all the *Secure Envelopes T* to the Tallier and to the Tally Intervention Systems which are to verify the correct performance of the Tallier.

As the Ballot Box has provided persons responsible for management and supervision of the electoral system with the same information transferred to the

Tallier, the Tallier assumes full responsibility for the correct processing of each vote.

Each Scrutineer will have his own machine (Tally Intervention System) where the said copy will be loaded. This machine has been previously audited by the experts in order to guarantee that it will only be able to tally. Any difference between the results obtained by the Tally Intervention Systems and those published by the Tally Board will be an indication of an anomaly. So neither the Tallier, nor the Tally Board may alter (add, exclude or modify) votes transferred from the Ballot Box without being detected.

The list of the records received by the Tallier and the Tally Intervention System will be destroyed after the voting process is considered valid. This information destruction will have to be audited.

4. CONCLUSIONS

The technical solutions adopted to develop a voting system have very real social impact on preserving and enhancing citizens rights and liberties and, consequently, on the development of democracy in the Information Society.

The design of the Digital Democracy systems must have as its base a critical and exhaustive analysis of the experiences and proposals previously made and it must include multidisciplinary methodologies (technological, sociopolitical, and legal) in order to determine the requirements and evaluate the final system to be developed.

The VOTESCRIPT system, by means of applying this multidisciplinary methodology, has obtained more efficient solutions than previous models. It has contributed valid procedures to defend telematic voting from the disqualifying arguments of, for example, Mercury Report [7], with which this research group was fully in agreement. Our experience till now has answered citizen demands for guarantees of cleanliness in the voting process, leaving the control of the system's *honesty* in the hands of a technological elite.

The VOTESCRIPT system provides an individual verification system allowing each voter to check, at specific locations and within a determined time period, if his vote has been correctly included, and without being exposed to any kind of coercion or the chance of vote selling. Likewise, the presence of Scrutineers enables control of the whole electoral process by citizen or candidature groups authorized to this target, so that this control is spread out in such a way that it does not fall to a corrupt group.

The VOTESCRIPT system's strength lies in the auditability of the well-known software and hardware, in the publication of the additional information together with the final results and in the participation of the citizens through the Scrutineers or individual verification. Precautions have also been taken throughout the process so as to prevent fraud or coercion by any agent or collusion among agents.

As the authors of this paper see it, all intellectual and material efforts made in this area are worthwhile if they lead to a qualitative improvement of democracy, reinforcing its legitimacy.

We understand that this improvement basically lies in researching the telematic networks' potential to facilitate and encourage citizen participation while offering the guarantees demanded by democracy.

5. REFERENCES

1. Carracedo, J., Gómez, A., Moreno, J., Pérez, E. and Carracedo, J. D., (2002). Votación electrónica basada en criptografía avanzada (Proyecto VOTESCRIPT). II Congreso Iberoamericano de Telemática. CITA'2002. Mérida, Venezuela.
2. Fujioka, A., Okamoto, T. and Otha, K., (1993). A Practical Secret Voting Scheme for Large Scale Elections, Advances in Cryptology, AUSCRYPT´92, Lecture Notes in Computer Science 718. Springer-Verlang, Berlin, pp.244-251.
3. Cranor, Lorrie F. and Cytron, Ronald K., (1996). Design and Implementation of a Practical Security-Conscious Electronic Polling System, WUCS-96-02, Informatic Department of the University of Washington, St. Louis, USA.
4. Ohkubo, M., Miura, F., Abe, M., Fujioka, A., Okamoto, T., (1999) An Improvement on a Practical Secret Voting Scheme. Lecture Notes in Computer Science 1729, Springer-Verlag, Berlin, pp. 225-234.
5. Riera i Jorba, A., (1999). Design of Implementable Solutions for Large Scale Implementable Voting Schemes, Phd at Universidad Autónoma de Barcelona, Spain.
6. Carracedo, J. and Carracedo, J. D., (2001). Telemática y sociología. Apuntes para una investigación multidisciplinar: tarjetas de crédito anónimas y democracia electrónica. I Congreso Iberoamericano de Telemática. Cartagena, Colombia.
7. Mercuri R., (2001). Testimony presented to the U.S. House of Representatives Committee on Science. http://www.house.gov/science/full/may22/mercuri.htm (visited 22.06.2005).
8. Informe sociológico sobre la experiencia en El Hoyo de Pinares, at disposal at the Observatorio para la Democracia Digital y los Derechos de Ciudadanía en Internet. http://www.ucm.es/info/demodigi/inves/vera.php (visited 22.06.2005)
9. Kohno, T., Stubblefield, A., and Rubin, A.D., (2003). Analysis of an Electronic Voting System. http://avirubin.com/vote.pdf (visited 22.06.2005).
10. Carracedo, J., Gómez, A. and Carracedo, J.D., (2003). Sistema VOTESCRIPT: Una propuesta innovadora desarrollada para resolver los problemas clásicos de votación electrónica. 2º Congreso Iberoamericano de Seguridad Informática (CIBSI'03), México D.F.
11. Carracedo, J., Gómez, A., Pérez, E., Moreno, J. and Sánchez, S., (2004). Use of Java Cards in a telematic voting system. CollECTer LATam 2004, Collaborative Electronic Commerce Technology and Research, Santiago (Chile).
12. Research group VOTESCRIPT. http://vototelematico.diatel.upm.es (visited 22.06.2005).

13. Call for a collective implementation of a telematic voting system under Creative Commons licence which will guarantee the citizens' rights through VOTESCRIPT system. http://www.vototelematico.org (visited 22.06.2005).

14. Carracedo Gallardo, J. Seguridad en redes telemáticas, Ed. McGraw-Hill, 2004.