Electronic Voting: An All-Purpose Platform

Ricardo André Costa[1], Mário Jorge Leitão[2], and Isidro Vila Verde[3]

[1] Escola Superior de Tecnologias e Gestão de Felgueiras,
Instituto Politécnico do Porto, Rua do Curral – Casa do Curral – Margaride,
4610-156 Felgueiras, Portugal
rcosta@estgf.ipp.pt
[2] INESC Porto, Faculdade de Engenharia da Universidade do Porto,
Campus da FEUP, Rua Dr. Roberto Frias, 4200-465, Porto, Portugal
mleitao@inescporto.pt
[3] Faculdade de Engenharia da Universidade do Porto,
Campus da FEUP, Rua Dr. Roberto Frias 378, 4200-465, Porto, Portugal
jvv@fe.up.pt

Abstract. It is generally considered that a key component of electronic government in the future will be electronic voting, as a means of facilitating the participation of citizens in elections and public debates. However, a long path has to be pursued before electronic voting, particularly if based on Internet, is accepted as a reliable system alternative to conventional methods. In this paper, we propose a new and simple platform, based on open software, which can be used primarily in small to medium sized communities, as a means to build confidence and experience for future larger elections. We try to provide adequate answers to multiple requirements, such as accuracy, democracy, privacy, verifiability and mobility. This can be done by establishing a distributed system which supports the different roles of a voting system and by using cryptography techniques in the interactions between these components.

1 Introduction

In recent years, electronic voting has attracted a significant attention [1], [2], but little progress has been made, in terms of establishing mature systems trusted by citizens. One of the reasons is that the level of security requirements is very high for major elections, such as presidential or parliament, and, additionally, this kind of elections has different rules and procedures, history and social perceptions within the various political systems around the world. One alternative to overcome this difficulty could be to promote the use of electronic voting in small, less important and less problematic elections or opinion polls. In this case, it is possible to prove that, in many cases, electronic voting is more secure and accurate, and less problematic than the traditional format used for voting. This can be the case of professional institutions, associations and public organizations with elected bodies, as well as referendum on local matters [3], [4].

Our work envisages to define an all purpose electronic voting platform, that could be used in a broad range of applications. One major objective is to allow

M.A. Wimmer et al. (Eds.): EGOV 2005, LNCS 3591, pp. 309–316, 2005.

rapid deployment with minimum configuration, together with simple use at all levels: infrastructure administrators, election commission and voters. In addition, to attain the desired level of performance, we propose a secure, scalable system based on open-source code and GNU Public License, as a means to achieve rigorous evaluation through public inspection.

This strategy of introducing electronic voting using credible open source approach and in a gradual way in citizens' democratic life, is a very strong point of our proposal, in order to acquire the adequate level of user acceptance, based on trust and usability. Furthermore, we will show that, along with accurate technology, the proposed solution incorporates clear and well perceived roles, at various levels, demonstrating the transparency of the overall system and its components, as a key requirement for user confidence.

2 Voting Requirements

As in any conventional election, there are a certain number of requirements that must be implemented [5]. In our system we will focus on the following, which depend strongly on the model for the voting system:

- *Accuracy:* There should not be possible to alter a vote, to eliminate a valid vote or to count an invalid one.
- *Democracy:* Each valid voter has the right to cast one, and only one, valid vote.
- *Privacy:* The voter, or anyone else, cannot prove which choice was made.
- *Verifiability:* There should be possibly to independently recount the votes.
- *Mobility:* A voter should be able to vote independently from his location. The system must be aware of voter origin which may imply different electoral circumscriptions.
- *Auditability:* The voting system should be validated by external observers.

3 Architecture of the Electronic Voting Platform (EVP)

The Electronic Voting Platform (EVP) is a distributed system with different components interconnected through a network (LAN, MAN, WAN), as shown in Figure 1. The voter accesses the EVP via the network, although physical presence or non-physical presence options are available.

A top level description of the roles of the EVP components is given as follows. The Authentication System (AS) is responsible for the voter authentication during the election, and for delivering an anonymous voting credential and the electoral ballot to the voter.

The Ballot System (BS) is responsible for receiving encrypted votes, validating the attached credential, checking it has not been used before, and distributing the validated votes to replicated Vote Collectors (VC).

The Vote Collectors accept the votes from the BS only, store randomly the votes and allow counting at the end of the election. At this point, the votes may be made publicly available for recounting.

The option for multiple VC's is an essential feature of the proposed system, to provide adequate geographic redundancy for the collected votes. Replication of the AS and BS components is also possible to account for scalability – in this case, the voters could be segmented according to electoral circumscription.

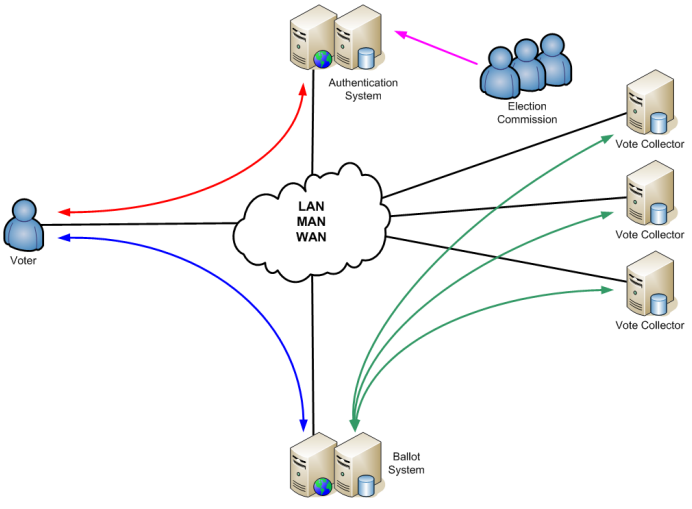

Fig. 1. Electronic Voting Platform

4 Operation of the Electronic Voting System (EVS)

The operation of the EVS requires the support of the voter registration, the initialisation of each component (AS, BS and VC) before the start of the election, the voting process itself and the ballot counting. All these actions are carried out under the control of the Election Commission (EC).

4.1 Voter Registration

Voter registration needs to be started well in advance of the election day, in order to determine which voters will be allowed to use the election right. One of the following scenarios could be adopted:

1. The voters need to be registered specifically for electoral purposes. In this case, usual registration techniques may be used either requiring physical presence of the voter or by electronic means, depending on the required authentication confidence.
2. The voters have already validated access to a system which can be used for electoral purposes.

This situation may be adequate to less critical elections, where voters are already registered in an organisation for other purposes, being able to access the system by electronic means in a controlled way, by a suitable authentication method.

4.2 Initialisation and Voting Process

Figure 2 represents the sequence of events for a complete initialisation and voting process. As it will be seen, the system adopts reliable asymmetric cryptographic techniques [6] and uses extensively secure communication channels.

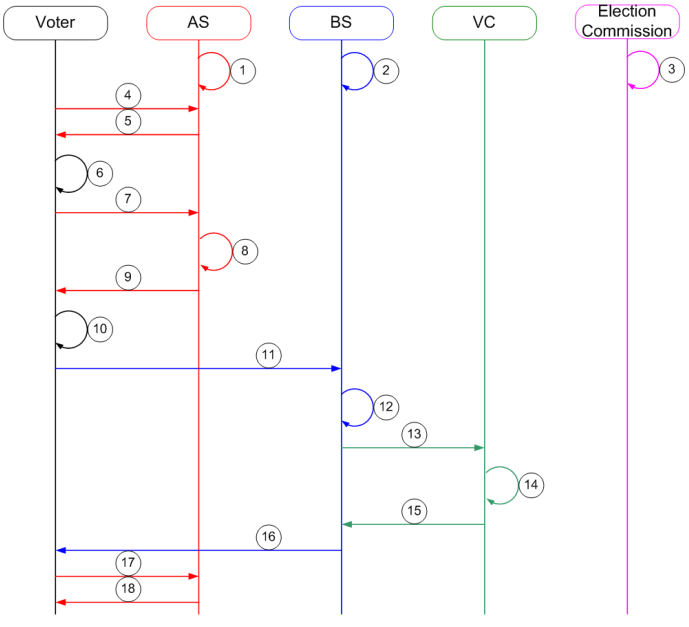

Fig. 2. Vote Sequence Diagram

Steps 1 to 3 refer to the initialisation phase. In steps 4 to 9, the voter obtains the credential and the election ballot from the AS. In steps 10 to 12, the voter submits the ballot to the BS. The replication of the votes in the VC's occurs in steps 13 to 15. Finally, steps 16 to 18 deliver success confirmation to the AS and the voter. Each step is described in detail as follows.

1. AS initialisation. This step will generate a public and private key pair for the AS (ASprvK, ASpubK), which will identify the AS from the beginning to the end of the election. The private key should never leave the AS and the public key is accessed by the voter and installed in the BS.

2. BS initialisation. Similarly, this step will generate a public and private key pair for the BS (BSprvK, BSpubK), which will identify the BS from the beginning to the end of the elections. The private key should never leave the BS. The public key is installed in the AS to be accessed by the voter and in the VC to validate the votes, as explained below.
3. Tiefgestelltes n im Text: EC initialisation. This step will generate a public and private key pair for the EC (ECprvK, ECpubK), which will identify the EC from the beginning to the end of the entire process, including vote counting. The private key should be split between several EC members ($ECprvK_n$, n=1...N) and the machine used for it generation should be sealed. The public key is installed in the AS to be accessed by the voter.
4. The voter accesses the AS (previously announced web site) and authenticates himself as a valid voter.
5. The AS, after validating the voter, sends him a client-side application and the public keys generated in the AS (ASpubK), BS (BSpubK) and EC (ECpubK)
6. The client-side application generates a public and private key pair to identify the voter (VprvK, VpubK).
7. The voter then sends its public key (VpubK) to the AS.
8. The AS stores the voter public key (VpubK) in its database. Then, it generates a hash of the combination of the voter username and a random number. Subsequently, signs the result with his private key (ASprvK) and adds the voter Electoral Circumscription Identifier (ECI) to form the credential (Cred). The credential is then ciphered with the voter public key (VpubK).

$$\text{Cred} = (\text{Sign}(\text{SHA-1}(\text{user, rand}), \text{ASprvK}), \text{ECI}) \ . \tag{1}$$

$$\text{EncCred} = \text{Ciph}((\text{Cred}), \text{VpubK}) \ . \tag{2}$$

9. The AS returns the encrypted credential (EncCred) and the correspondent electoral circumscription ballot to the voter.
10. The client-side application presents the unfilled ballot to the voter to enforce his right to vote. After the choice is made by the voter, the application deciphers the credential (Cred) with the voter private key (VprvK), ciphers the ballot and the ECI with the VC public key (VCpubK) to form the ciphered ballot (CiB), joins the credential and ciphers the result with the BS public key (BSpubK), forming the double ciphered ballot (dCiB).

$$\text{Cred} = \text{Deciph}(\text{EncCred, VprvK}) \ . \tag{3}$$

$$\text{CiB} = \text{Ciph}((\text{Ballot, ECI}),\text{VCpubK}) \ . \tag{4}$$

$$\text{dCiB} = \text{Ciph}((\text{CiB, Cred}),\text{BSpubK}) \ . \tag{5}$$

11. The voter then sends the above double ciphered ballot (dCiB) to the BS.
12. The BS deciphers the dCiB, validates if the credential is signed with the AS private key (ASprvK) and checks if it was not used before. Then, signs the CiB with the BS private key, forming the signed ciphered ballot (SiCiB) and flags the credential as already used.

$$(\text{CiB, Cred}) = \text{Deciph}(\text{dCiB, BSprvK}) \ . \tag{6}$$

$$\text{Validate(Cred, ASpubK)} \ . \tag{7}$$

$$\text{SiCiB} = \text{Sign(CiB, BSprvK)} \ . \tag{8}$$

13. The BS submits the SiCiB to the VC, or, preferably, to multiple VCs.
14. The VC validates if the SiCiB has been signed with the BS private key (BSprvK) and save it randomly.

$$\text{Validate(SiCiB, BSpubK)} \ . \tag{9}$$

15. Each VC confirms to the BS the reception of the ballot.
16. The BS confirms to the voter the reception of a ballot with valid credentials.
17. The voter confirms to the AS that has already finished the voting process.
18. The AS will confirm to the voter that he as completed the voting process, thus not being able to vote again.

4.3 Ballot Counting

The count of the ballots is a very critical task [7]. We must guarantee that the ballot count is, without any doubt, truly representative of the electors' choice. For increased reliability and verifiability, distributed replication of ballots [8] can be adopted, as already mentioned in the above section.

After the end of the election, the split private key is merged and made public. However, the BS private key (BSprvK) should be destroyed first, in order to avoid changing and (re)signing the ballots.

In this phase, as everything is made public in each VC, different applications can be used for ballot counting, ensuring transparency and accuracy of the counting process. Furthermore, ballots from all VC's may be merged, eliminating duplicates and overcoming possible sporadic losses of votes in specific VC's. Overall, we obtain a more reliable set of ballots for final counting.

The above applications do not need to be provided by the EVP, once there is enough and public information for anyone to confirm the elections results accessing all the stored votes in the multiple VC's. Although the same results should be obtained, obviously, the official result counting process should be conducted by the Election Commission and all the parties' representatives.

All this counting process is safe because the ballots can be validated and deciphered, but not changed once they are signed by the previously destroyed BS private key (BSprvK).

$$\text{Validate(SiCiB, BSpubK)} \ . \tag{10}$$

$$\text{(Ballot, ECI)} = \text{Deciph(SiCiB, Merged(CVprvK}_1\text{, CVprvK}_2\text{, .., CVprvK}_N\text{))} \ . \tag{11}$$

5 Proof of Voting Requirements

We have previously presented the voting requirements of a voting system. Now we will present how we achieve each one of them with the new proposed system.

Accuracy: This requirement is satisfied in three phases. The first one, when the ballot is deposited in the BS, it is impossible to change it, because it is ciphered

with the VC public key and the correspondent private key is not accessible. The second one, when the vote is deposited in the VC, it is impossible to deposit an invalid vote because a valid one must be signed with the BS private key, which has been previously destroyed, as explain above. The third one, when the votes are being counted with the VC private key made public, no extra votes may be created for the same reason.

Democracy: The AS only gives one valid credential to each voter. This credential is obtained trough a one time process of deposit of the voter public key. After that, the voter in the AS database will be flagged to make impossible to deposit a different one. However, if the same public key is used, the previous credential will be returned. The valid credential may be used only one time for ballot delivery. Each credential will be flagged in the BS database, not allowing ballot duplication.

Privacy: It is not possible to associate a voter with his credential, and subsequently with his ballot. This requirement is satisfied by the AS, since the credential contains no information regarding the voter [9].

Verifiability: As the ballots may be made public, as well as the EC private key (used to decipher the votes), anyone can recount the votes at any time after the end of the elections.

Mobility: The AS guarantees credential distribution to the voter independently of his location. The SiCiB created with the BS and stored in the VC will allow vote counting for the corresponding electoral circumscriptions, once it contains the ballot and the respective circumscription identifier.

Auditability: The EVP is Open Source (GPL) and ballot counting is totally open.

6 Conclusions

We have shown that our system is able to satisfy the main voting requirements and we hope that the release under the GPL license will allow a rapid evolution under public scrutiny. We point out that the separation of roles creates some kind of similarity between the Electronic Voting Platform and well established conventional elections, but adds some interesting functionalities.

We concentrated our study on the satisfaction of model dependent requirements, without forgetting the importance of technology and organisational measures. For instance, geographical separation of components may not be mandatory but it is highly recommended, as well as the use of physical and logical isolation trough the use of very restrictive access rules to each component.

We believe the major advantages of our system are not only the solid technical base, but also the potentiality to show to the voters why they can trust it. Before being concerned with large scale systems, we focused building a secure platform that can, and should, be first used in small, less problematic elections. Proceeding in this way, we can contribute to the involvement of citizens with information society technologies, allowing a gradual validation of the assumptions

of electronic voting systems towards usability and acceptability. We believe this is the only way we can aspire to have electronic voting systems introduced in social and political life.

Acknowledgements

We would like to thank the referees for their comments and suggestions, which helped the improvement of the paper.

References

1. Dini, G.: Electronic Voting in a Large-Scale Distributed System, Networks, Volume 38, issue 1, pages 22-32, John Wiley & Sons (July 2001)
2. Selker, T., Goler, J.: The SAVE system – secure architecture for voting electronically, BT Technology Journal, Volume 22, issue 4, pages 89-95 (October 2004)
3. Schryen, G.: Security Aspects of Internet Voting, Proceedings of the 37th Hawaii International Conference on System Sciences (January 2004)
4. e-Democracy: in Search of Tools and Methods for Effective Participation, Journal of Multi-Criteria Decision Analysis, Volume 12, issue 2-3, pages 93-100, John Wiley & Sons (April 2004)
5. Cranor, L.: Electronic Voting – Computerized polls may save money, protect privacy. ACM Crossroads (April 1996)
6. Schneier, B.: Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition, John Wiley & Sons (1996)
7. Franco, A., Petro, A., Shear, E., Vladimirov, V.: Small vote manipulation can swing elections, Communications of the ACM, volume 47, issue 10, pages 43-45 (October 2004)
8. Saltman, R.: "Accuracy, Integrity, and Security in Computerized Vote-Tallying," U.S. Department of Commerce, National Bureau of Standards Special Publication 500-158 (August 1988)
9. Chaum, D.: Security Without Identification, Transactions Systems to make Bib Brother Obsolete, Communication of the ACM, volume 28, issue 10, pages 1030-1044 (October 1985)