Affordable and Secure Electronic Voting for University Elections: the SAVE Case Study

Xavier Ochoa
Escuela Superior Politécnica del Litoral
Guayaquil, Ecuador
Email: xavier@cti.espol.edu.ec

Enrique Peláez
Escuela Superior Politécnica del Litoral
Guayaquil, Ecuador
Email: epelaez@espol.edu.ec

***Abstract*—Traditional electronic voting systems are designed with national elections in mind. However, there are other types of institutions, such as Universities, that are required by law to conduct mid- to large-scale elections. The nature of these institutions and the different regulations that govern their election process made impractical the use of traditional voting systems for their elections. This work presents the SAVE system, an electronic voting system designed to be used in University elections preserving all the requirements that a secure voting system have while being affordable and flexible enough to adapt to the different regulations. The design and implementation of this system are discussed in detail and the results of its 10 years of continuous are presented as a case study.**

I. Introduction

Electronic voting or e-voting includes a wide range of possible implementations. In [1] there is a description of different types of systems, their differences and the use of e-voting in different contexts, within supervised poll-sites, unsupervised electronic kiosk, and "remote voting".

This case study refers to an "e-voting system" as the system that collects and counts votes. The collection and counting of votes has been particularly controversial worldwide due to problems with national electronic voting and integrity of the process in elections in some countries [2]. The fault-tolerance [3] and easy-of-use [4] of current technology has been questioned and also privacy concerns [5] are raised because voting machines are not supposed to keep records of any kind that associates the voter with the vote, because a ballot is supposed to be secret.

Another source of controversy and research motivation has been the security and trust beneath the "vote transaction" [2]; in this study a printed vote has been considered as the proper reflection of the voter choice and recorded as the voters selection. Printed votes could be used as a mechanism to show the voters choice and as a backup ballot that can be used to audit the process when the results are challenged [6]. Although, the printed vote given as a "receipt of the transaction" that records the choices made by the voter, the receipt alone does not assure that the choices made were counted in the final result, but the receipt constitutes the proof of which choices the voter made, and can be checked by the voter before it is deposit into the ballot box.

978-1-5090-4830-4/17/$31.00

E-voting systems are especially challenging because: Democracy demands verifiability, voter privacy and transparency; and, elections must be accessible and usable by the public [7]. The solution analyzed in this case study considers the different stages of the election process, for both in site as well remote voting; stages that start with the "preparation", involving managing the information about all the different voting process, types of candidates and ballot styles; "polling", which involves collecting the results from all the polling places; and, "counting", which involves consolidating all the votes for each candidate in each contest across all the ballots and ballot styles, hence with many contests on the ballot, computers can make this process much easier and error free.

This work discuss the design, implementation and use of SAVE, an e-voting solution for University elections. The structure of the paper is as follows: Section II discusses the context of electronic voting in Universities, considering aspects such as: legal, social, technological, economical and security involved. Section III, describes the architecture of a design and its implementation. Section IV, describes the components of the system analyzed. In section V, some security details are given. Section VI, presents how an election process is configured and implemented. Section VII, refers to the case of remote voting; and section VIII, shows some evaluation results; and finally some conclusions.

II. Electronic Voting in the University Context

Traditional electronic voting systems are designed with national elections in mind. These types of elections are governed by similar rules worldwide. However, there are other types of institutions, such as Universities, that are required by law to conduct large-scale elections. The nature of this institutions and the very different regulations that govern their elections made impractical the use of traditional voting systems in these contexts. This work focuses in the design and implementation of a e-voting system tailored for University elections. The following subsections describe the specific considerations that any electronic voting system should take into account in order to be useful and usable for academic institutions.

A. Legal Considerations

The main difference between elections at a national level and at academic institutions level is the legal and regulatory

framework that should be followed. While national elections are usually guided by the country constitution and primary laws, elections in Universities are governed by more flexible by-laws and regulations. Initially this can be seen as an advantage for an electronic voting system, however, the flexibility of the rules, and the variation between institutions, make it very difficult to design a system that could comply with all the different variations.

Differences in rules also made impractical the use of traditional electronic voting system inside institutions. For example, it is common in national elections that each vote has the same value. This is, after all, the principle behind democracy. However, as it is the case in Ecuador, the Universities assign different weight to different groups of voters. By law, a professor vote carries more weight than the vote of a student or a staffer. It will be very difficult to alter a equal-vote-value system to segregate the voters into groups and assign different weight to each one.

Systems designed for University elections should be flexible enough to accept very different rules and counting procedures to adapt to the variety of by-laws and regulations of diverse academic institutions.

B. Social Considerations

Universities are a very special subset of a country society. It is expected that the level of education and technical skill are higher than the country average. This difference removes some limitations that traditional e-voting systems have. For example, more sophisticated interfaces could be used in a university context. These interfaces has a direct impact on the complexity of the types of elections that can be executed. Also, less robust hardware can be used, given that it expected for the machines to receive less abuse from the voters. This hardware impacts the cost of the system, making it more affordable.

Another important difference is the technological culture of the University. Students and professor are usually more open to use technological means to conduct day-to-day activities. Introducing electronic voting in an academic institution is much easier than to do it in the general society.

C. Technological Considerations

In a University campus setting, the access to technological infrastructure is much easier than in a national election. For example, wireless networks could be used as part of the e-voting system knowing that connectivity will be there when needed. This is not true for national election systems. Also support personnel and backup-equipments are much easier to arrange in a campus or multi-campus setting. These advantages influence the design of the e-voting system reducing its complexity and cost.

Another consideration is that universities usually have technological elements, such as computers, printers, etc, that could be marshalled into voting equipment when needed. The e-voting system should have the flexibility to use heterogeneous components to assemble the electronic ballot box and counting systems.

D. Economical Considerations

Being part of their duties, national and regional governments usually have a dedicated agency and department to take care of the election process and electronic voting system. In the University context, on the other hand, elections are seen as an extraneous activity. As such, rarely Universities have a dedicated body to conduct elections and much less a sizeable budget to operate a electronic voting system. This has two important implications in the design of an e-voting system for Universities. It should be affordable enough to not be a burden to the institution budget and it should be easy to configure, install, use and maintain so any University member (student or professor) could be trained to be responsible of the different parts of the election process. Also, it will be a plus if the e-voting equipment could be re-purposed in the periods between elections as computers for the student or information kiosks.

E. Security and Trust

The final difference between national and university elections is the level of security and trust needed in the system. Due to the different stakes of the two types of elections, the security protocols required varied considerably. While at University level an expert or designated authority could be the guardian of certain encryption keys, a national election requires a more sophisticated multi-level multi-person set of keys. The main difference is reduced to the level of the trust that the voters have in the election authority. At national level the level of trust should be very low, while in the University context a higher level of trust is natural. This difference has a direct impact on the complexity of the system and its security protocols.

III. SAVE Design and Implementation

Based on the experiences of previous electronic voting implementations, the SAVE system was designed with four design principles in mind: Anonymity, Integrity, Fault Tolerance and Ease of Use. All these features and assurances have been added to the system to gain the trust of election authorities, candidates and voters about the validity of the results delivered by the electronic voting system. It does not rely on the ethics of any individual person or institution. It does relies on techniques and procedures that provide encryption and security that even the creators of the system cannot violate. Through these practical and visible security measures, users of the system can trust the system and welcome the benefits that this new type of voting system provides. These design principles are described in the following subsections, together with the technical and methodological implementation features required to meet them.

A. Anonymity, privacy and no coercion in voting

SAVE guarantees anonymity, privacy and lack of coercion when issuing a vote. That is, voters are able to vote in complete freedom and privacy, without the possibility of their identity being linked to their vote.

To ensure that at no time of the voting process the identity of the voter can be directly related to a specific vote, the following procedures were implemented:

- The voter identifies with the electronic ballot box through a magnetic stripe card chosen at random when the voters identified themselves to the election officials. This card, which identify the user as as a valid voter, does not carry any information about the identity of the voter. Each card contains a large random number (13 digits) generated just before the election. Each electronic ballot boxes only stores the information of the cards that are valid at that ballot box.
- The system does not record the time or order in which the votes are entered. Moreover, the system only delivers results on a consolidated basis.

These implementation details make it extremely difficult for election authorities, election officials, staff or any other person to know who issued a specific vote. Only direct observation of the voting process would violate the security of the employed technique.

B. Process Integrity

The integrity of the voting process means that the election made by each voter, as well as the intermediate and final results, can not be altered either by human or system error or deliberate fraud attempts.

To provide security for the voting process and the subsequent storage and counting processes, SAVE implements the following mechanisms:

- The object code of the computer program that runs at the electronic ballot box is cryptographically signed by the central election authority and it is loaded into the voting machine the day of the elections by the Technical Manager of the polling station through a USB memory. This mechanism prevents that the software from being altered during the period that the device rests in the election precinct before the election.
- The electoral roll information, that is signed and encrypted, is loaded in the electronic ballot box by an election official when the election start through a USB memory.
- The vote is printed on paper, so even if the voting software has been fraudulently altered (in the hypothetical case of fraud by the system administrator), the voters can confirm that a physical evidence of their selection is stored in a physical ballot box and it will constitute an independent source of system verification (physical votes) that can not be altered electronically.
- Each printed vote contains a long random code that identifies it as a valid vote. This code can be easily verified to prevent votes not produced by the electronic ballot box from being introduced in the physical ballot box.
- The results are electronically stored in 2 USB memories. These reports are signed and encrypted, and can only be read by the central counting system. If someone were to change these results, the central system can detect and void the results of that electronic ballot box.
- When the electronic ballot box is closing, a report of the results is printed. This report may be contrasted against the information electronically stored in the USB memories if it is suspected that someone broke the cryptographic key (almost impossible in the short time between closing the election and the delivery of results).
- The information is also stored signed and encrypted on the hard drive of the computer, providing a fourth source of verification of results.

While there is a remote possibility that any of the 5 means of verification (paper votes, first USB memory, second USB memory, paper result report and the hard-drive in the electronic ballot box) could be altered, the time restriction (just hours to an electronic result) make it impossible to alter them all consistently practically impossible.

These multiple sources of verification (electronic and paper based) provides voters with the assurance that the system actually register their vote and that there are no practical means to undermine the integrity of the system.

C. Fault Tolerance

While technological resources demonstrate a high degree of reliability in general, technology is always exposed to faults (accidental or intentional). Electrical power failures, disconnecting cables or devices, attempts of physical alteration, etc. are failures for which the SAVE system is prepared. This is achieved through the following mechanisms:

- The status of the system is is saved regularly. If the power supply fails of the machine is deliberately turned off, it is only necessary to restart the system and the election process will continue from the receiving new votes. The machine will preserve the counting of the votes so far and allowed to finish any vote not completely issued.
- Being based on off-the-shelf machines, any part of the SAVE electronic ballot box (monitor, CPU, printer, keyboard, etc.) can be replaced in case of failure for another with similar characteristics, without the system integrity being compromise or the voting process being indefinitely interrupted.
- There is redundancy in the main access tokens (precinct administrator, election officials) and initialization information for the devices. These duplicates are under the responsibility of the Electoral Authority in each precinct.
- In case of removal of the memories or unauthorized system changes, the electronic ballot box will automatically close and it will not allow more votes to prevent electoral fraud.

These mechanism increase the robustness of the system and avoid delays in the voting process.

D. Easy to use

The SAVE system was designed to be easy to use, even without any prior training. If the person has used a keypad

(telephone, typewriter, computer, etc.) will be able to operate the system. To ensure the ease of use the following features are implemented:

- The system is touch-based. There is no need to learn any menu or tabs interface. Everything shown in screen is either information, a selection or an action.
- Photo of the candidate is included to help identify them.
- The voter can always go back and change your choice until the time finally accept and print your vote, giving process control entirely to the voter.

While no special training is needed to vote on the SAVE System, certain level of rule-following is needed to operate the machine as an election official. It is expected that they are able to read and follow the instructions to activate the electronic ballot box and close the process.

IV. SAVE Components

The SAVE system can be divided into hardware and software components. The following subsections describe each one of these components.

A. Hardware Components

These are all those computers or devices required for the system function. The SAVE design have been considered four main components:

1) Electronic Ballot Box: It is an electronic device that will be placed on each voting site. This device enable voters, once identified with the election official, to choose their preferences on a touch screen. Then, through a thermal printer, it prints the vote that can be validated by the voter and deposited in the physical ballot box. The votes will be counted electronically and stored in different physical memories, besides the paper record to allow multiple levels of security.

2) Central server: The results of each electronic ballot box are transmitted, through various means, to the central server. This server is a high-performance computer in which the calculation of the results will be made and distributed. During the election, it will be located in a secure facility with controlled access.

B. Software Components

These are all the programs developed to carry out the logic process required by all the different steps during an election. This steps include, for example, the generation of the electoral roll, the generation of the candidates lists and the report of the results. These programs run in different locations depending on their functionality:

1) Electronic Ballot Box: This is the application that runs in each of the electronic ballot boxes. It is responsible for managing the hardware devices of the electronic ballot box (printer, card reader, touch screen, etc.). This application checks that the voter is valid, presents the list of candidates, accepts the voter's selection, prints the vote and registers it electronically in several physical memories. This system also calculate the final result for that box. It also provides auditing routines before, during and after the election.

2) Local Database: All information needed for the operation of each Electronic Ballot Box is stored in a local read-only database. This database store all the elected positions, candidates and registered voters for that box.

3) Election Generation Application: This application will run on the Central Server. This is the application in which the election will be scheduled and the election parameters are set. For example this application will be in charge of generating the information to be stored in each Electronic Ballot Box. Also, in this application, the electronic ballots are designed.

4) Consolidation Application: This application will run on the Central Server. This application is in charge of calculating the results of the election, from the information that is transmitted by the individual Electronic Ballot Boxes. The transmission method is determined during election design.

5) Results Dissemination: This application is in charge of presenting the results of the election to authorities and, if required, to the general public, either through an application or a Web site.

V. Security details

The following is a list of different types of algorithms and programs that are used by the system:

- Software Signing: The software that is deployed to the Electronic Ballot Boxes is signed by the Central Server using a Symmetric Encryption Advanced Encryption Standard (AES) with a key length of 256 bits.
- Data Encryption and Signed: Data that needs to move between machines is encrypted and signed using a RSA Asymmetric Encryption with a key length of 2048 bits.
- Message Authentication: Messages passed between machines use the standard HMAC-SHA256

These security features are implemented using the Random Number Generator FIPS 140-2 from the Java Class SecureRandom. While the SAVE system could run over any Operating System that supports Java, it is recommended that a secure version of Linux is used both for the Central Server and the Electronic Ballot Boxes.

VI. Election Process

The electronic voting process is divided in three phases. Each of these phases requires a different procedure.

A. Election Preparation

During this phase the elections are designed and all the necessary software and identification tokens are generated. This phase takes place few months and weeks before the election.

1) The list of candidates and valid voters is delivered from the Election Authority to the SAVE Technical staff.
2) Based on the information provided by the Election Authority, the Election Generation Application is used to create the software for the Electronic Ballot Boxes and the configuration files for each Electronic Ballot Box. These programs are signed with the Central Server key

so the Electronic Ballot Boxes could verify their origin before being installed.
3) The identification tokens for technical administrators, election officials and general voters are generated. In case of the magnetic cards, this information is stored in the magnetic strip as a 13 digit number.
4) The election software and the configuration files, stored in USB memories, together with the corresponding identification tokens, is bundled in packages to be distributed to every electoral precinct.

The SAVE system was designed and implemented to support different type of elections:

- 1-out-of-2: The voters select one between two choices. This is typical of yes/no votes
- 1-out-of-N: The voters select one between N choices. For example, the voter select one out of many candidates for Rector.
- K-out-of-N: The voters select a predefined number (K) of options from a list of N possible choices. The voter can select less than K if desired. For example, this vote is used to select a list of representatives to a council.

The SAVE system support many election types in the same electronic ballot. All this is configured during the Election Preparation phase.

B. Electronic Ballot Box Activation and Voting

This phase starts few minutes before the actual start of the election and finished once the election period is closed. In this phase, the Electronic Ballot Boxes are loaded with the election software and configured for the given election. Also, during this phase the voters are able to use the Electronic Ballot Boxes to select the desired candidates. The procedure to cast the vote is described in the following steps (Figure 1):

1) The system administrator, in the presence of the election officials, use his/her identification token (magnetic card) to start the installation process of the Electronic Ballot Box. The system will then request the connection of the USB flash memories that contain the software for that particular election. The administrator is the only person who has that the memories with that program. The Electronic Ballot Box will only accepts programs signed by the Central Server. When the election software finishes its installation, it will require the disconnection of the USB flash memory. After that, the elections software starts automatically.
2) The election official must use his/her identification token (magnetic card) to start the voting phase. The system prompts the connection of the USB flash memory that store the election configuration files (candidates and valid voters). After this configuration, the system will require the USB flash memory to be removed and immediately request the connection of the two USB flash memories that will store the votes. After the configuration is finished, the SAVE Electronic Ballot Box is ready to accept votes.
3) The voter approaches the voting place and identifies with the election officials.
4) The vote picks a random voter identification token.
5) The voter swipe the token into the Electronic Ballot Box.
6) The voter chooses his/her preferred candidates from the pictures on the screen.
7) When the voter is sure about his/her selection, the system prints the vote on paper and stores it in the different memories.
8) The voter deposits his/her vote and the magnetic card in an physical ballot box.
9) After the election, the election officials closes the electronic ballot box.
10) The Electronic Ballot Box prints the results in 3 copies and the system shuts down.

C. Counting

This is the last phase of the election. The results from the different Electronic Ballot Boxes, stored in the USB memories are compiled by the Consolidation Application in the Central Server. The steps are as follows:

1) Upon completion of the election process and printing of the results, the election official removes the two USB flash memories that store the votes.
2) The two USB memories should be taken to the Central Server by different persons through different paths.
3) The Electronic Ballot Box is deactivated and sealed.
4) The USB of each Electronic Ballot Box is connected to the Central Server and recognized by the Consolidation Application.
5) The Consolidation Application provide the final result once the information from all the Electronic Ballot Boxes is entered to the system. The Consolidation Application can provide intermediate results depending on the type of election.
6) The result date is passed to the Result Dissemination Application to be shown to the Election Authorities and the general public

VII. Remote Voting

The architecture of the SAVE system does not limit the Electronic Ballot Box to be a physical entity. This Ballot Box could be deployed as a Web application in order to enable remote voting. However, to preserve the design principles some changes are needed. First, the Virtual Ballot Box could not receive magnetic cards as authentication tokens. Moreover, there are no elections officials that could validate the identity of the voter before the election. To solve this problem, two solutions are available

1) A covered identification token is physically sent to any valid voter abroad to be used to authenticate himself/herself with the Web application
2) A separated Authentication Web Application could be used to enable voters abroad to generate the voting token (code) through a secure user/password authentication.

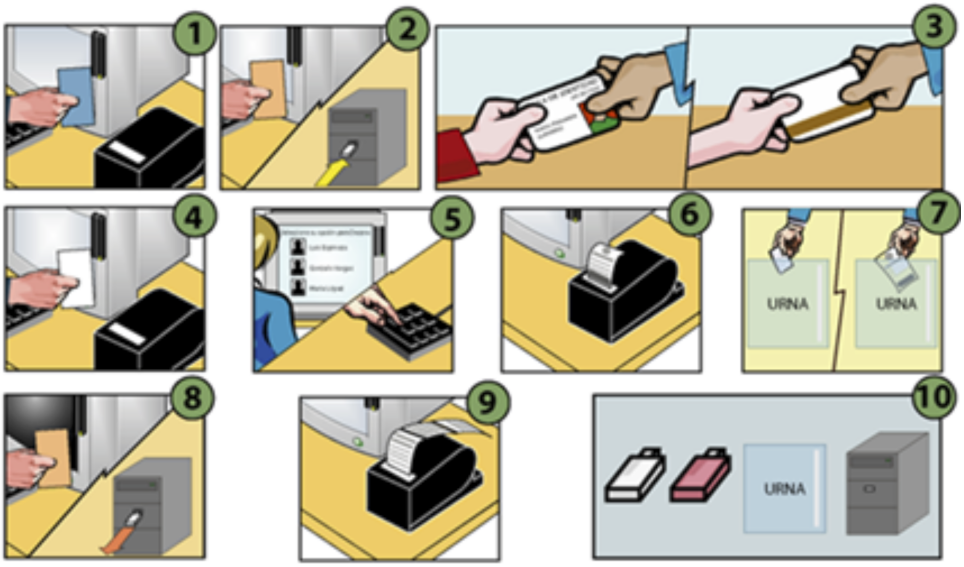

Fig. 1. Voting process

The recommended method is number one, mailing the covered authentication code to the voters abroad, but the second option require less expenses and logistic preparation.

Another difference with physical voting is the lack of paper record. While this reduce in one the levels of verification for the SAVE voting system, the other methods (USB memories and Hard driver) remain.

A. Remote Voting Procedure

The steps to cast a remote vote using the SAVE system are (see Figure 2):

1) The Electoral Authorities provides the SAVE technicians with a list of voters who are abroad.
2) The SAVE systems provides voters abroad an application where they can generate their voting code once. To issue this code, the system requests the a user and password, then verify that this voter is in the list previously provided by the Electoral Authorities and he/she has not obtained his/her code previously. The system then generates a unique voting code. The code generation system will be available up to 3 days before the day of the election.
3) This application saves the generated codes, without relating them with the name of the voter. These codes are used to generate the Electronic Voter Register of Virtual Ballot Boxes.
4) The voter will use the assigned voting code to access a Web application called the Virtual Ballot Box. If the code is valid, the voter proceeds to register his/her vote. The Virtual Ballot Box is available from 48 hours before the end of the election.
5) The record with the results of Virtual Ballot Box will not be printed to preserve the anonymity of remote voters. It will only be recorded in the electronic memories. The Consolidation Application will deliver total results, similar to any election.

VIII. System Usage and Evaluation

This is a first report of the operational track of the system and an user based evaluation of the voting experience. An implementation of the SAVE system is currently being used at ESPOL University, a middle-sized polytechnic located in Guayaquil, Ecuador. A change in the national Higher Education law required all Universities to move to general elections for most positions (Rectors, Vice-rectors, Deans, etc.). Previously, only a small electoral college, with delegates from professors, students and staff (usually no more than 100 individuals) were required to vote in order to elect those positions. The electoral college elections were conducted with paper ballots. The SAVE system was designed and implemented as a response to the necessity to move from an electoral college of 100 individuals to a universal voting system with over 10,000 voters.

The SAVE systems has also been used in two other institutions of similar size in Ecuador. The same equipment and software used in ESPOL has been re-used in these contexts. Only the interface of the system and the election configurations has been changed.

This implementation of the SAVE system was contextualized to the Higher Education laws in Ecuador. The main change to traditional voting systems is the need to distinguish three types of voters: students, professors and staff. This differentiation is due to the fact that,by law, the weight of each vote is different depending on the group the voter belongs to. For example, the vote of a professors, could be worth 50 student votes and 100 staffs votes. To work at ESPOL, SAVE needed to implement those changes.

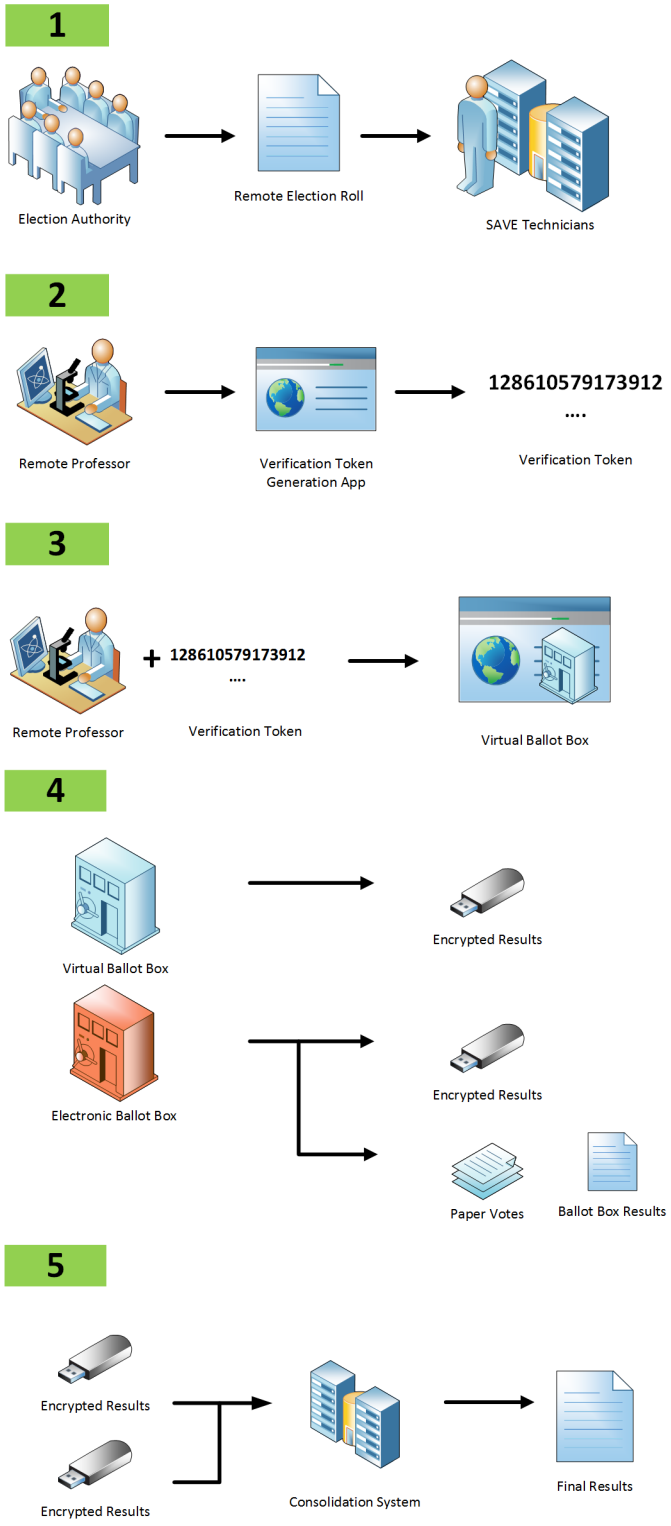

Fig. 2. Remote SAVE Voting Procedure

A. Usage Data

The SAVE System was implemented in 2006 and has been in continuous use in ESPOL since then. From 2006 to 2014, SAVE system has been used in 159 small and large elections for different positions in the University. Since 2012, some of those elections include a remote vote capability, usually reserved for professors that are doing their sabbatical year abroad or that are known to be absent during the election period. Table II provides a summary of the amount of different kind of voters that used the system each year. It is clear that the number of student voters is, in average, ten times bigger than the number of professors and staff for any given year. Also, it is clear from the table, that remote voting, while used, represent a very small fraction of the total amounts votes per year when available.

The system has been used for all types of elections. From the large rector elections with the participation of most students, professors and staff, to small elections to select the professor representative to a faculty steering commission with few dozens of voters. The types and number of elections during the 2006-2014 period can be seen in Table I.

TABLE I
ELECTIONS BY TYPE IN THE PERIOD 2006-2014

Type	Average Voters	Times
Rector / Dean ViceRector / ViceDean	1,655	22
Student / Staff / Professor Associations	1,570	31
Student / Staff / Professor Representatives	457	106

B. Costs and Resources

The cost of SAVE system can be divided into three main categories: Initial development, Electronic Ballot Hardware and Election preparation. The initial development of the software took a team of 4 individuals: one senior software developer, two senior programmers and one security expert. This team worked for 4 months creating and testing all the software components of the system. The Electronic Ballot Hardware comprised of an industrial touch-panel, a thermal printer and a case could be build with a cost of 1500 USD. Each Electronic

TABLE II
AMOUNT OF DIFFERENT TYPES OF VOTERS IN SAVE CONDUCTED ELECTIONS FROM 2006 TO 2014

Year	Students	Staff	Professors	Online Prof.	Total
2006	6,571	330	207	0	7,108
2007	23,958	1,028	748	0	25,734
2008	20,066	393	626	0	21,085
2009	12,020	48	461	0	12,529
2010	21,831	329	555	0	22,715
2011	1,744	198	436	0	2,378
2012	20,908	1,407	735	49	23,099
2013	5,140	1,003	606	82	6,831
2014	13,725	193	89	6	14,013
TOTAL	**125,963**	**4929**	**4463**	**137**	**135,492**

Ballot could serve 300 to 400 voters (depending on the complexity of the election and the time available for voting). This Electronic Ballot can be reused for at least 10 years. The initial 15 Electronic Ballots build for ESPOL in 2006 are still fully operational. The preparation of each election requires a team of 2 technicians to configure the election and record the unique identifier in the magnetic cards. The day of the election, a technician is required at each electoral precinct.

C. Users Perception

In order to obtain information about the experience that the voters had with the system, a survey was conducted in 2012. The voters were questioned after using the system during a real large election. A total of 4,000 responses were obtained from students (3,000), professors (500) and staff members(500). Only local voters were questioned. Remote voters did not participate in the survey. Given the small number of remote voters, their absence do not alter the conclusions drawn from the survey. The participating students varied from years in the university from 1 year (17,5%), 2 years (17,5%) 3 years (30,0'%) and 4 or more years (7,5%).

For questions were asked on the survey:

1) **How easy was to whole voting process?** This question obtained information about the whole voting experience. This experience included the identification process, the use of the Electronic Ballot Box and casting the vote. A 5-point Likert scale was used from "Very hard" to "Very easy". The answers are presented in Figure 3. It is clear from the results that most voters find the whole voting process very easy (80%)
2) **Was it easy to use the Electronic Ballot Box?** This question focused on the Electronic Ballot Box experience. A "Yes" and "No" option was given to voters. The results show than a large majority (90%) consider the Electronic Ballot Box interface easy to use.
3) **Did you experience any technical problem?** This question tried to estimate the percentage of voters that are confronted to any technical problem during the election. While always solved, these problems could create delays and be inconvenient. A "Yes" and "No" option was given to voters. The results suggest that only 5% of the voters encounter any type of technical problem.
4) **Do you recommend to use the system for the next election?** This last question confronted the voter with the choice of a traditional voting system or the current method. A "Yes" and "No" option was given to voters. All the questioned voters (100%) recommended the use of the SAVE system for the next election showing that even the technical issues are minor difficulties compared with the generally positive voting electronic voting experience.

The results, obtained after several years of use of the system, are very positive. Most users find the whole experience easy, very few experience problems and all of them want to keep the electronic system.

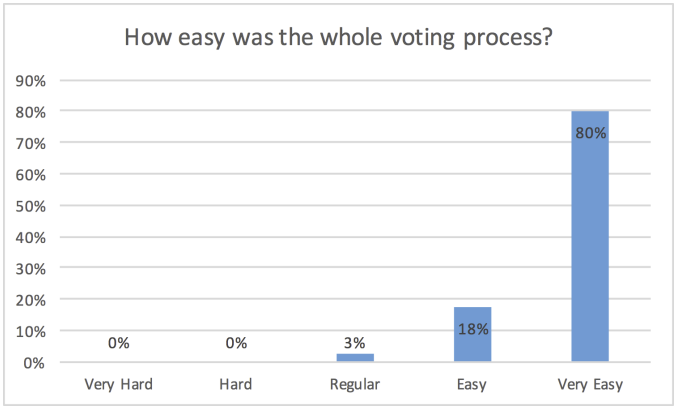

Fig. 3. Results for how easy was the voting process

IX. Conclusion

The SAVE system was designed to serve as an ideal electronic voting system for University elections. Its main advantage and contribution is being flexible enough to easily adapt to the regulations of different Universities, where more traditional electronic voting systems available in the market will require much more complex adaptations.

The main advantages of the SAVE system are:

- **Affordability:** thanks to the potential to reuse existing technology available in the University context and the lack of dependence from any one vendor.
- **Speed:** due to the complete electronic records of votes, the results could be computed almost intermediately after the election.
- **Trust:** the very visible security mechanism allow the voters to trust the system
- **Remote Voting:** the architecture of the system enable electronic voting through Virtual Ballot Boxes

The last conclusion of this work is that e-voting systems should not only be restricted to national elections, but can also be designed for different types of institutions that require affordable solutions for their elections.

References

[1] B. Jones, "A report on the feasibility of internet voting," Internet Voting Task Force, State of California, Tech. Rep., 2000.
[2] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach, "Analysis of an electronic voting system," in *Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on*. IEEE, 2004, pp. 27–40.
[3] P. G. Neumann, "Security criteria for electronic voting," in *16th National Computer Security Conference*, vol. 29, 1993.
[4] B. B. Bederson, B. Lee, R. M. Sherman, P. S. Herrnson, and R. G. Niemi, "Electronic voting system usability issues," in *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 2003, pp. 145–152.
[5] A. M. Keller, D. Mertz, J. L. Hall, and A. Urken, "Privacy issues in an electronic voting machine," in *Privacy and Technologies of Identity*. Springer, 2006, pp. 313–334.
[6] M. I. Shamos, "Paper v. electronic voting records-an assessment," in *Proceedings of the 14th ACM Conference on Computers, Freedom and Privacy*, 2004, pp. 1–23.
[7] G. Z. Qadah and R. Taha, "Electronic voting systems: Requirements, design, and implementation," *Computer Standards & Interfaces*, vol. 29, no. 3, pp. 376–386, 2007.