A Secure Electronic Election System for the Mexican Presidential Election

López García M.L., Leon Chávez M.A. and Rodríguez Henríquez F.

Centro de Investigación y de Estudios Avanzados del IPN
Departamento de Computación
mlopez@computacion.cs.cinvestav.mx
francisco@cs.civestav.mx
Benemerita Universidad Autónoma de Puebla
Facultad de Ciencias de la Computación
mleon@cs.buap.mx

Abstract. In 2006, the Mexican presidential election offered the opportunity for those Mexican citizens with residency in foreign countries to cast their vote through certified postal mail. The present work proposes an Internet Electronic System (SEVI after its name in Spanish, "Sistema Electrónico de Voto por Internet") that emulates the election of the President of the Mexican United States. SEVI automatizes the voting process by certified postal mail. SEVI was developed using the Unified Software Development Process on a client/server environment, it offers sound security services while it takes into account the electoral laws to guarantee the credibility of the vote.

1 Introduction

Recent advances in communication networks and cryptographic techniques have made possible to consider online voting systems as a feasible alternative to conventional elections [1].

Independently of the electronic device used for sending votes, getting started with a public election includes the creation of electoral laws that define the operation of the system and the exact procedures to be followed in the event of any contingency.

An electronic voting scheme can be defined as an election system that generates electronic ballots which allow registered citizens to cast their votes from an electronic device and to transmit them via Internet towards an electronic electoral urn, where they will be stored and counted at the end of the electoral day.

This type of systems offers a quick and comfortable form of casting a vote; however, these factors are not a substitute for the accuracy of the results and the trust in the electoral process [2]. Therefore, developing an Electronic System of Voting for Internet (SEVI) implies to comply with the following requirements:

– Since the Internet is an insecure means of communication, SEVI should provide sound security services in order to avoid either passive or active

A. Gelbukh, S. Suárez, H. Calvo (Eds.)
Advances in Computer Science and Engineering
Research in Computing Science 29, 2007, pp. 171-182

Received 04/07/07
Accepted 19/10/07
Final version 24/10/07

attacks, that is to say that the vote should not be intercepted, observed, amended, erased or fabricated.
- SEVI design should strictly comply with the electoral laws and it should cover all functional requirements that depend from the electoral process to be implemented.
- The basic properties of an electronic voting system must be fulfilled, namely, [3]:
  1. Authentication: only authorized voters should be able to vote.
  2. Fairness: no voter should be able to vote more than one time.
  3. Accuracy: election systems should record and count the votes correctly.
  4. Integrity: it should not be possible to modify, forge, or delete votes without detection.
  5. Anonimity: no one should be able to link any vote with the individual that casted it and voters should not be able to prove how they voted.
  6. Transparency: the voters should understand and know the voting process.
  7. Verification and Accountability: it should be possible to verify that the votes have been correctly counted at the end of the election and therefore, to prove their authenticity.
- Guarantee the dependability, scalability, flexibility and accessibility of the system [4].

In an electronic election system, privacy and security are mandatory features. However, it is not always obvious how to achieve these characteristics at a reasonable price, due to the fact that when an election process takes place, mechanisms that assure both, security and privacy may be too expensive for system administrators on one side, and inconvenient for users on the other. If the election system is at a national level, it implies that millions of voters and thousands of officials will be interacting, thus the reliability and precision of those systems become crucial [5].

Although in many countries only conventional elections have been instrumented, others have adopted information technology novelties, such as Brazil that captured 115 million votes through voting machines with the Windows NT operating system and touch screen monitors in 2002, and India in 2004 where 670 million electronic votes were issued [6]. In United States, during the primary and secondary elections of 2004, the system SERVE (Secure Electronic Registration and Voting Experiment) was utilized [7]. In that system, firstly voters were asked to perform a pre-registration step and later they were allowed to vote from any Internet-connected computer by establishing a secure session with the server. In Estonia, electronic voting was made by Internet in 2005 with an enormous citizen participation, probably due to the fact that Estonia's citizens are heavy Internet consumers [8].

In Mexico several electronic systems have been built. For example, the Extraterritorial Vote [9] and SELES [10]. Extraterritorial Vote was developed in the state of Coahuila during the presidential election of 2006, by free-lance developers. In that system, a citizen should first register to obtain a secret code that was then sent to him/her by postal mail. This password allowed him/her to vote

through any Internet connected computer. SELES was developed and implemented in the Computer Science Department of CINVESTAV-IPN for medium scale on-line elections with less than five thousand voters. It requires a preregistration and it guarantees security services by performing three phases: Voter authentication, vote cast and vote counting.

This paper presents the development of an Internet Electronic System (SEVI), especially designed for the Mexican presidential election of 2006. SEVI automatizes the voting process by certified postal mail of Mexican citizens with residence in other countries as it was legislated in the sixth book of the Federal Code of Institutions and Electoral Procedures (COFIPE) [11]. SEVI was developed using The Unified Software Development Process [12] and the Unified Modeling Language.

The rest of this paper is organized as follows: Section 2 describes the legal procedure of voting by Mexican citizens with residence abroad. Section 3 presents the models of cases of use, analysis, design, implementation and testing. Finally concluding remarks and perspectives of this work are presented in Section 4.

2 Vote of Mexican Citizens with Residence Abroad

COFIPE articles 273 to 300 describe the voting procedure for Mexican citizens with residence abroad, this procedure is summarized next.

The citizen should request his/her participation by filling out a registration form that she/he can obtain in Internet or diplomatic embassies close to where she/he resides. The form should be presented along with a copy of her/his voter credential and a proof of her/his real address. Then, that form should be sent by certified postal mail to the Electoral Federal Institute (IFE) in Mexico.

IFE should accept the documentation if the registration is properly filled. Afterwards, if the application fulfills all the requirements, the citizen request is granted and the citizen is included in the Electoral Nominal List (LNEE) while she/he is temporarily removed from the Voter's Nominal List (LNE) in Mexico.

By using citizen's postal address, IFE can inform the citizen the result of his/her request, either indicating the cause of its rejection or sending his/her the voting documentation.

In case of being accepted, the citizen should get ready to vote according to the following instructions: she/he should take the envelope with her/his elector key and then enclosed there the ballot with his/her vote. After that, the citizen must seal the envelope and place it in a second envelope labeled with her/his data. The citizen's final step is to send the second envelope to the IFE and to wait till the electoral date for verifying the result of the voting process.

In Mexico, IFE functionaries receive the envelopes, they annotate the arrival date and register them labeling the citizen's name with the legend "Vote" in the LNEE.

The election day, the president of each table of scrutiny will check whether the sum among the marked voters with the word "Vote" and the sum of the envelopes that contain the electoral ballots match or not. After having confirmed

the previous point, the ballot is extracted from the inner envelope and it is placed in the electoral urn, this way guaranteeing the citizen's anonymity.

At the end of the electoral day, the votes are counted by the tellers, in presence of the political parties' representatives, and the result is registered in the scrutiny act corresponding to each scrutiny table. The acts are grouped according to the corresponding electoral districts, where the sum of the votes is computed.

When the scrutiny process has totally concluded, the General Secretary, will let the General Council know the official results of all the votes collected from abroad in the President election of the Republic of the Mexican United States.

Using this voting procedure, the IFE accepted little more than 40,000 request and 32,621 votes were obtained [13] for the Mexican presidential election of 2006. After having assigned a considerable budget for this task, analysts perception was in the sense that the whole process was slow and quite expensive. Also, since the entire communication between the IFE and the citizens with residence abroad was made through the certified postal mail, at least two major problems were reported. The first one is that IFE election process obligated citizens with residence abroad to inform about their exact addresses, which caused that many citizens refrained from carrying out their application (due to privacy reasons and the fear that this information could be used against them by local authorities such as the ones in United States). The second problem was caused by the inefficiency that characterizes the Mexican Postal Service.

3 Electronic System of Voting for Internet (SEVI)

This work proposes an Electronic System of Voting for Internet (SEVI) that automates in a secure way the voting procedure of Mexican citizens with residence abroad as it was specified in COFIPE sixth book. SEVI will provide the services of Registration, Voting, Results and Audit as outlined in Figure 1.

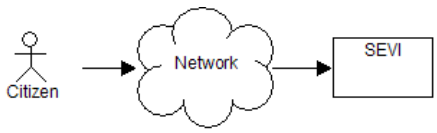


Fig. 1. Internet Electronic Voting System (SEVI)

For the sake of developing SEVI in a modular fashion, the object oriented programming was used, reason for which The Unified Software Development Process and the Unified Modeling Language were adopted [12]. Accordingly, the following models are reported next: Cases of use, Analysis, Design and Implementation.

Case of Use model

The user's requirements for the software system, whether functional or not, are captured in the diagram of cases of use shown of Figure 2.

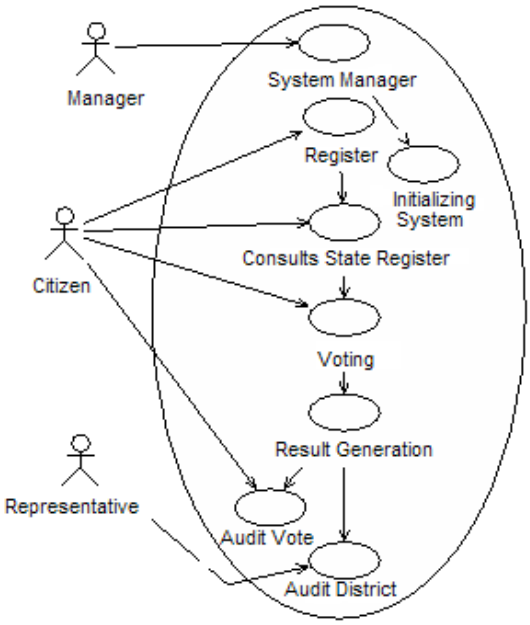


Fig. 2. SEVI Cases of Use Diagram

.

- Register: the actor Citizen requests her registration to the LNEE providing the information of his voter credential and attaching a copy of her credential and a proof of her/his actual postal address.
- State of Register Query: the Citizen queries the state of her request, which can be: pending, accepted or rejected. SEVI will validate the information provided by the Citizen against the LNE. If it matches, SEVI will temporary remove the Citizen from the LNE database and the Citizen will be included in the LNEE database.
- Voting: the Citizen, provided that a positive authentication has been accomplished, casts her/his vote using an electronic electoral ticket (ballot). SEVI receives the votes, it classifies them according to the section and electoral district and it stores them in the urn of the district.
- Result generation: SEVI counts the votes stored in each electronic urn by electoral district.

- Auditing the district: the Representative actor, which can be an electoral official of the district table or a representative of the political parties, can verify the validity of each vote stored in the district urn.
- Auditing the vote: The Citizen actor can verify that his vote was valid.

It is worth remarking that SEVI should enable each of the cases of use previously described during an interval of time. In accordance with the COFIPE, the registration is open from October first of the year previous to the election up to January 15 of the presidential election year. Votes are received by certified postal mail from May 21 up to twenty four hours before the electoral day.

Analysis Model: It is the detailed specification of the user's requirements. The oriented object approach; along with UML diagrams of classes/collaboration represent this model.

The Diagram of Classes of SEVI is shown in Figure 3. The classes Module IFE, Council and Stall are responsible of accomplishing the functional requirements of the system, maintaining communication with the databases for the registration of the citizens, the voting and the counting servers. The classes Secure Station and Secure Server are responsible of the execution of the implemented security protocol, which is discussed in the design model. For the sake of clarity, in the diagram of classes only the classes of the register and counting servers, and of the classes that are implemented through the personal computers used by the Citizens to interact with SEVI are shown. Due to space constraints we do not show the attributes or the class methods.

Design Model: It is the realization of the cases of use and it is a sketch of the implementation. This model consists of the refined diagram of classes and the diagrams of sequence and collaboration.

SEVI is a distributed system that was implemented in an architecture client/server, therefore, its classes are grouped in software components to be distributed among the computational nodes. The communication between the client and server is instrumented in a secure way using the SSL secure protocol [14].

SEVI consists of five phases: Register, Authentication, Voting, Counting and Auditing, which correspond to the cases of uses specified before. SEVI utilizes four databases administered in the same number of servers: Registration Server (RS), Authentication Server (AS), Voting Server (VS) and Counting Server (CS).

During the Registration phase, the Citizen connected from any computer, accesses remotely to the RS and fills out the registration format, which in our application is shown in a pop-up window. She/he must attach the files corresponding to the copies of her voter's credential and her address proof. The tasks of SEVI in this phase are: to verify the match between the information provided by the Citizen and the one stored in the Nominal List of Voters (LNE), to store the copy files for a post-processing and to accept or to reject the request. If the request is accepted, SEVI temporarily removes the Citizen from the LNE database and it includes her in the Nominal List of Voters Abroad (LNEE) generating the corresponding certificate and public/private keys; the Citizen will

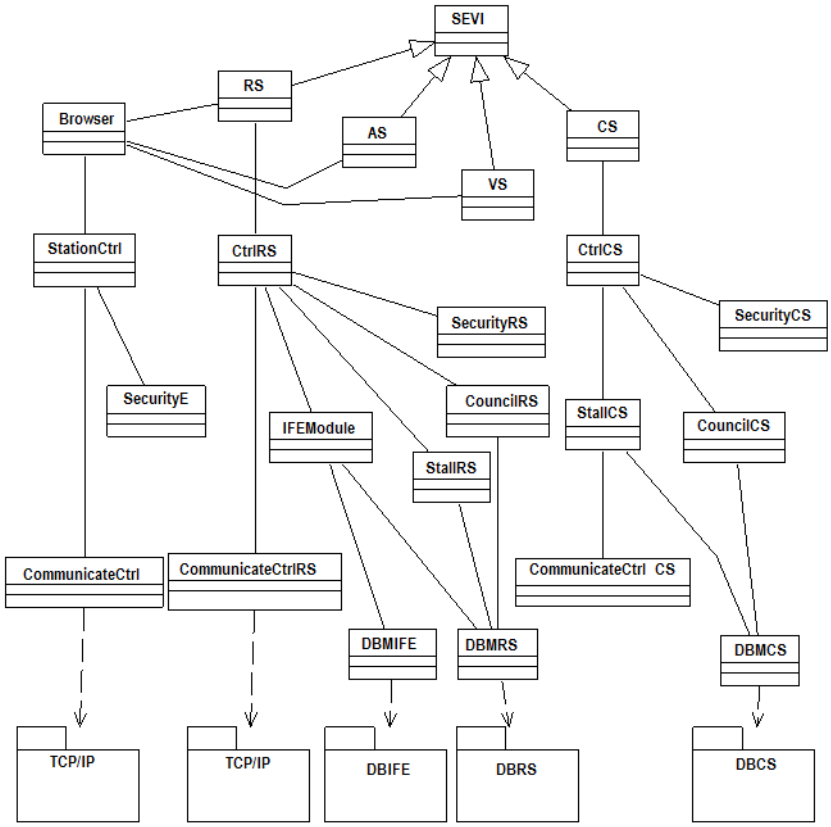


Fig. 3. SEVI Class Diagram

.

discharge this information within the case of use: query of transaction state, in order to continue with the following phases.

The following three phases will be carried out through the security scheme proposed by Lin-Hwang-Chang in [15] which is briefly described next.

Security scheme by Lin-Hwang-Chang: It is a protocol based on blind signatures. It protects the privacy of the voters and it is able to detect duplicity on votes. The last modification made to this scheme was reported in the SELES electronic voting system [10], where the digital signature ElGamal was substituted by the digital signature DSA.

SEVI implements the scheme with the aforementioned modification adding in the exchange of messages between the voter and the servers, the information of the voter's district (*de*), with the purpose of adjusting it to the electoral law

that is trying to mimic. This process is shown in Figure 4. In the Authentication

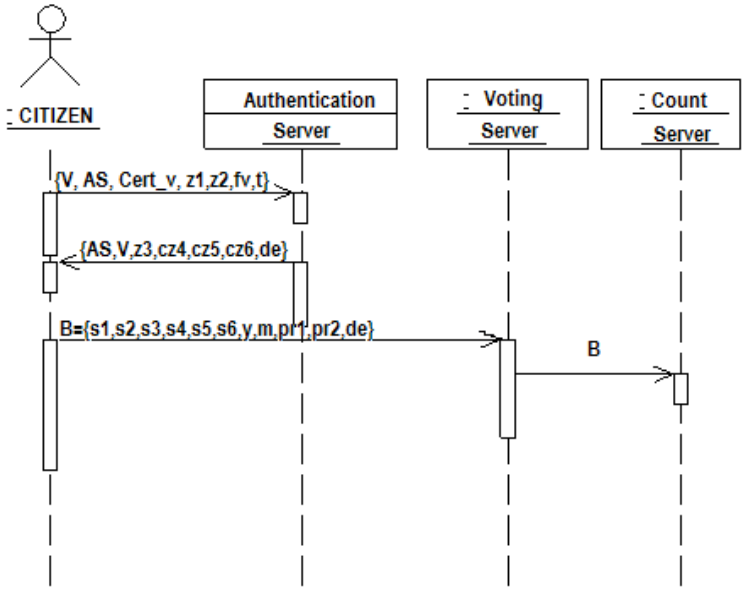


Fig. 4. Security Scheme adjusted to the Electoral Law

.

phase, the Citizen sends the message of equation (1) to the AS, which contains the following parameters: Citizen's name (V), citizen's Digital Certificate ($Cert_v$), two blind signatures z_1 y z_2 (computed based on RSA with two blind factors and two random numbers (k_1, a), which have been previously chosen by the voter, plus the DSA parameters), a timestamp (t) and the voter's digital signature (f_v).

SA receives the message and verifies the digital signature by recovering the citizen's public key from her certificate $Cert_v$. If it is valid, it generates and assigns a unique identifier k_2 for the voter, identifying the electoral district where the citizen is registered and performing the calculations required for sending the message of Equation (2).

$$\{V, SA, Cert_v, z_1, z_2, t, f_v\} \tag{1}$$

$$\{SA, V, z_3, ((z_4 + t)^{e_v} \bmod n_v), ((z_5 + t)^{e_v} \bmod n_v), ((z_6 + t)^{e_v} \bmod n_v), d_e\} \tag{2}$$

In z_3 k_2 gets encrypted, whereas z_4, z_5 and z_6 are the SA's encrypted signatures, which have been encrypted separetedly using the voter's public key.

The citizen receives (3), it decrypts it and it obtains k_2, z_4, z_5 y z_6. This phase is accomplished by removing the blind factors in z_4, z_5 y z_6 thus obtaining the SA's signatures s_1, s_2 y s_3, with which the validity of the vote could be proved by the Voting Server (SV).

In the voting phase, the citizen casts his/her vote, signs it using DSA and it sends it to the SV. For that computation the private and public keys x and r, respectively are utilized. As a unique identifier k_2 and k_1 chosen during the authentication phase. The vote is signed using the operations indicated in Equations (3) and (4), where m is the vote contents, q is a DSA parameter and a is a random number.

$$s_4 = x_1^{-1}(m + ar_1) \, mod \, q \tag{3}$$

$$s_5 = x_2^{-1}(m + ar_2) \, mod \, q \tag{4}$$

Finally, the values pr_1 and pr_2 are computed and encapsulated taking advantage of the Chinese Remainder Theorem. This is done with the purpose that the SV performs the corresponding verifications by using the n_{sa} modules (SA public key) and q (DSA parameter). The message that the voter sends to the SV is:

$$B = \{s_1, s_2, s_3, s_4, s_5, y, pr_1, pr_2, m, de\} \tag{5}$$

Where y is a DSA parameter and m is the vote data.

The SV task is to verify the five signatures in order to validate the vote and store it in the electoral district database specified by the parameter de. Three of the signatures are performed modulus n_sa (corresponding to the AS public key), and two are performed in arithmetic modulo q. If the five signatures are correctly verified, the vote is stores and after the end of the election day, the VS sends all received votes to the Counting server (CS).

In the counting phase, the CS receives the valid votes and it counts them and finally, it publishes the results. A voter trying to cheat the system by voting more than once can be easily detected by comparing the two votes shown in Equations (5) and (6) and by obtaining k_2 from equations (7) and (8). Let us recall that k_2 is the citizen's unique identifier.

$$\hat{B} = \{s_1, s_2, s_3, \hat{s_4}, \hat{s_5}, y, pr_1, pr_2, \hat{m}, de\} \tag{6}$$

$$x_1 = \frac{\hat{m} - m}{\hat{s_4} - s_4} \, mod \, q \qquad x_2 = \frac{\hat{m} - m}{\hat{s_5} - s_5} \, mod \, q \tag{7}$$

$$k_1 = x_2 - x_1 \qquad k_2 = x_1 - k_1 \tag{8}$$

With this computation the security protocol is accomplished. However, the auditing phase must still be calculated. The auditing phase is divided into two steps: vote auditing and district auditing.

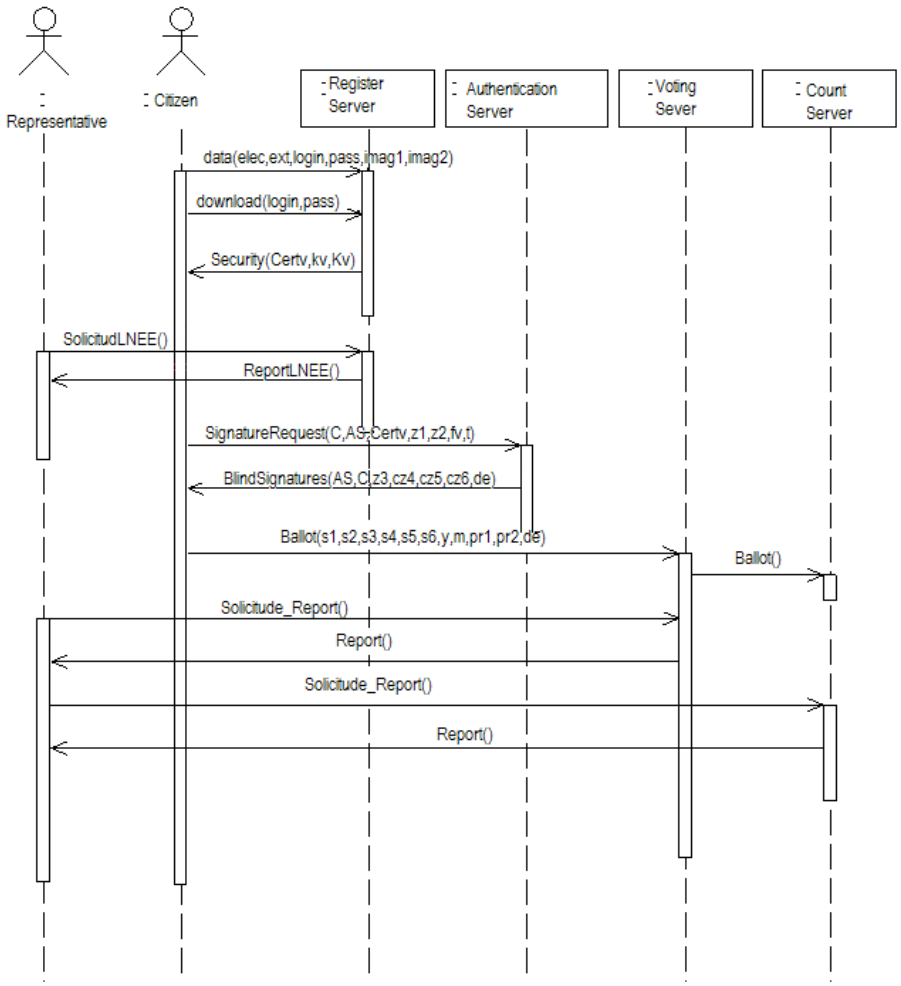
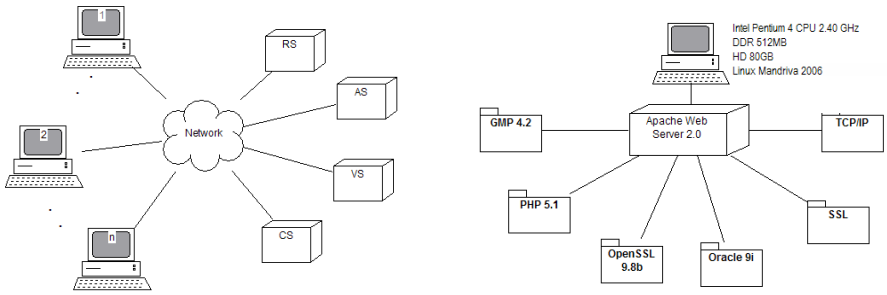


Fig. 5. Registration, Authentication, Voting and Counting SEVI Processes

.

Vote auditing refers to the accounting process performed in order to verify that the citizen's vote was indeed counted and included in the election's final tally. District auditing refers to the analysis, verification and validation of the register process perform by the political parties representatives according to the Articles 281-282 [11]. During this step also the members of the scrutiny table must validate the registration process as specified in Articles 291 through 293 [11]. The sequence diagram of Figure 5 shows the message exchange among actors and SEVI servers.

Implementation Model: SEVI is a design that strives for automating the election process of Mexican citizens with residency abroad. The security services are guaranteed by the Lin-Hwang-Chang protocol as it was implemented and tested in SELES [10]. In our case, it was decided that SEVI was going to utilize the Oracle 9i database modulo. Also, in order to guarantee the process fairness and the information security, the four SEVI servers must be physically independent. The client/server architecture is shown in Figure 6.



Client/Server Model Architecture

Fig. 6. Implementation Model

Each server has a Web Apache 2.0 modulo implemented under the operating system Linux Mandriva 2006. We used PHP 5.1 as the programming language along with the cryptographic libraries OpenSSL and GMP 4.2.1, respectively. Figure 7 shows the server organization.

Testing Model: After the presidential elections, the IFE institute reported that more than 40000 votes were received from citizens with residence abroad. Out of them, little more than 30000 were accepted and counted with the rest of the votes emitted in Mexico. To test this situation in our system we simulated 40000 registers in our database and we simulated the voting process in a sample of 123 citizens with valid results.

4 Conclusions

Due to the problems identified in the presidential election process of 2005-2006 for the Mexican citizens with residency abroad because of the usage of the certified postal mail and taking advantage of the information technology tools, this paper has presented an electronic voting system (SEVI), which represents an efficient, reliable and secure option for accomplishing the same process in an automated way.

References

1. Xenakis, A., Macintosh, A.: E-electoral administration: organizational lessons learned from the deployment of e-voting in the uk. ACM International Conference Proceeding Series **89** (2005) 191–197
2. Grove, J.: Acm statement on voting systems. Communications of the ACM (2004) 69–70
3. Foundation, N.S.: Report on the national workshop on internet voting: Issues and research agenda. ACM International Conference Proceeding Series (2001)
4. Carroll, T., Grosu, D.: A secure and efficient voter-controlled anonymous election scheme. Information Technology: Coding and Computing, IEEE 2005 **1** (2005) 721–726
5. Bryans, J., Littlewood, B., Strigini, L.: E-voting: dependability requirements and design for dependability. Availability, Reliability and Security, ARES, IEEE (2006)
6. Kaminski, H., Kari, L., Perry, M.: Who counts your votes? (vev electronic voting systems). e-Technology, e-Commerce and e-Service, IEEE (2005) 598–603
7. Jefferson, D., Rubin, A., Simons, B., Wagner, D.: A security analysis of the secure electronic registration and voting (serve). New York Times Article (2004)
8. Trechsel, A., Breuer, F.: Voting: E-voting in the 2005 local elections in estonia and the broader impact for future e-voting projects. ACM International Conference Proceedings Series **151** (2006) 40–41
9. y de Participación Ciudadana de Coahuila IEPCC, I.F.E.: Voto extraterritorial, http://www.iepcc.org.mx/ademocracia/a01.html (2004)
10. García, C., Rodríguez, F., Ortiz, D.: Seles: an e-voting system for medium scale online election. Computer Science, ENC 2005. (2005) 50–57
11. Electoral, I.F.: Codigo federal de instituciones y procedimientos electorales cofipe, http://ife.org.mx (2005)
12. Jacobson, I., Booch, G., Rumbaugh, J. In: The Unified Software Development Process. Addison Wesley (1999)
13. Electoral, I.F.: Resultados de la votacion extranjera, http://mxvote06.ife.org.mx//pdf/resultados_03_06.pdf (2006)
14. Hirsch, F.: Introducing ssl and certificate using ssleay. Web Security: A Matter or Trust, World Wide Web Journal **2** (1997)
15. Lin, I., Hwang, M., Chang, C.: Security enhancement for anonymous secure e-voting over a network. Computer Standards and Interfaces **25** (2003) 131–139