Experimentation on Secure Internet Voting in Spain

Andreu Riera, Gerard Cervelló

Scytl Online World Security, S.A.
Entença, 95, 4-1
08015 Barcelona, SPAIN
andreu.riera@scytl.com
gerard.cervello@scytl.com

Abstract: A major step forward along the path towards the implementation of secure Internet voting in Spain was taken in November 2003. For the first time in this country, a non-binding remote electronic voting pilot was run in parallel to a public election, in particular the 2003 election to the Parliament of Catalonia. The e-voting pilot was also the first of this kind to gain the requisite approval by Spain's Central Electoral Council, ant it is still the most significant up to date. The objective of the trial was to evaluate the advantages, usability, security and reliability of this voting system in consideration of its potential use in future elections, mainly as a complementary channel to postal voting. The trial provided valuable empirical information regarding practical technological and social issues surrounding e-voting.

1 Introduction

Since 1996 the *Generalitat de Catalunya* (the government of the autonomous region of Catalonia located in the north-east of Spain) had run several pilots in parallel to public elections using electronic voting machines in polling stations [Aa99]. Following the interest in the development of Internet voting throughout Europe, the *Generalitat de Catalunya* organized its own non-binding remote electronic voting pilot that was run in parallel to the 2003 Elections to the Parliament of Catalonia [GC03]. This was the first time a *remote electronic voting* pilot run in parallel to actual public elections in Spain received approval by the Spanish *Central Election Council*[1].

The Generalitat wanted to evaluate the advantages, usability, security and reliability of this voting system in consideration of its potential use in future elections which would be mainly as a complementary channel to postal voting. For this reason, over 23.000 Catalans resident in Argentina, Belgium, the United States, Mexico and Chile were invited to participate using any computer connected to the Internet by means of a web browser supporting Java technology.

[1] The Spanish Central Election Council has been always very reluctant to this kind of e-voting pilots run in parallel to current elections.

The pilot was managed by the *Oficina de Coordinació Electoral de la Conselleria de Governació i Relacions Institucionals* of the *Generalitat de Catalunya*, and used Pnyx, the cryptographic technology for securing electronic voting developed by Scytl [SCT03].

In this paper, we present the Catalan remote e-voting experience along with our views with regard to the security standards that must be set in electoral processes driven by electronic voting systems, implemented in this pilot. In Section 2 we start by providing the objectives drafted by the Generalitat to judge the success of the pilot. In Section 3 we introduce briefly the currently most debated risks and challenges posed by electronic voting, along with the solution offered by Scytl's security architecture. In Section 4 we present an overview of the e-voting pilot phases. Section 5 shows the results of the e-voting pilot in comparison with the results from the real elections. Section 6 introduces the feedback provided by the users of the e-voting platform, and finally, Section 7 includes some concluding remarks.

2 Pilot Objectives

The Catalan Government set some specific objectives that were used to judge the success of the pilot. In this respect, the remote internet voting system had to:

- **Facilitate the participation of voters that are resident abroad.** At present these voters can only vote by mail, and many of them do not receive their ballot or have problems sending it back on time for it to be counted.
- **Guarantee the honesty of the electoral process**. The system must offer at least the same level of security and confidence found in traditional paper-based postal voting.
- **Facilitate participation in the election**. The installation of any specific software or hardware should not be required.
- **Extend the polling period without increasing the man-hours required to staff the election**. The current postal voting system entails a logistical challenge that new technologies can simplify and make less expensive.
- **Protect the voter's personal data from third parties.** This security measure is essential to ensure compliance with the Spanish Law of Personal Data Protection.
- **Obtain the results immediately after the polls close**. This permits the integration of the results from the remote voting with the results from the polling-place voting without having to wait several days for the postal votes to arrive.

3 Description of the Pilot

The *Generalitat de Catalunya* selected *Pnyx*, the e-voting security technology from Scytl Online World Security S.A. to run the project. The project was managed by the *Oficina de Coordinació Electoral de la Conselleria de Governació i Relacions Institucionals de la Generalitat de Catalunya*.

The non-binding pilot was run in parallel to the 2003 Elections to the Parliament of Catalonia, held on November 16th 2003. 23.234 Catalans in Argentina, Belgium, United States, Mexico and Chile were invited to try the internet voting system from 10h00 on November 14th until 20h00 on November 16th. Voters could participate from any computer connected to the Internet using any web browser supporting Java, a technology required to cryptographically process every individual ballot to ensure its security. In addition, several "Casals Catalans" (Catalan cultural associations spread all over the world) allowed voters to use computers located in their offices overseas.

3.1 Creation and Distribution of the Voting Credentials

To cast a vote during the e-voting pilot, each voter had to be correctly identified in order to ensure his/her presence in the electoral roll and that he/she had cast no previous ballot. After evaluating several alternatives, the login/password option was selected, due to its usability and easy distribution, as the mechanism for accessing the e-voting platform.

For security reasons, the process for the creation and distribution of voting credentials ensured that no entity had access to both the voting credentials and the personal data of the voters. A 16 character voter identification key was randomly generated for each participant. This information was sent to a printing company that printed the keys in sealed PIN envelopes. A different company was responsible for the task of enclosing the sealed PIN envelopes, an invitation letter from the Generalitat, and some brief instructions into a larger envelope that was addressed and sent to each voter by surface mail 15 days before the pilot was to begin. This credential distribution process is identical to the one used to allow all Spanish citizens living abroad participate in the paper-based elections: they receive by mail all the ballots, and then they send their selection again by mail to the Spanish electoral authority before a deadline.

3.2 Pilot Promotion Campaign

The pilot did not have an extensive promotion campaign. Besides the letter sent to each voter, a brochure was sent to the Spanish Consulates and Casals Catalans in the countries involved. A website [GC03] was set up where the participants could access to information about the pilot and an e-mail address (gencat@e-lectoral.com) was created where questions regarding the pilot could be sent that would be responded to by Scytl technical personnel.

3.3 Constitution of the Electoral Board

The e-voting platform used in the pilot was designed to replicate the essential trusted security features of a traditional election [Ra03]. One important aspect of such elections is the oversight of an electoral board that is composed of several members who may have opposing interests in the election results. The e-voting platform empowers an electoral board whose role is to control the election electronically.

On November 13th at 18h00 a representative of each political party represented in the Parliament of Catalonia (5 parties in total), along with the director of the Oficina de Coordinació Electoral and a representative of Catalan Government assembled together to constitute an electoral board to manage the pilot. Following a short simple procedure, a cryptographic key that protects the confidentiality of the votes and that is necessary to start the tallying process, was generated and divided in 7 parts, one for each member of the electoral board. Immediately after, it was destroyed.

3.4 Vote Casting Procedure

Scytl's Pnyx-based electronic voting platform permits voting from any Internet-connected computer, running a browser that supports Java (virtually 100% of the browsers on the market). Java is needed to guarantee the security and confidence requirements of the Internet voting platform. It is used to create a secure cryptographic dialogue between the voter and the electoral board, ensuring that the vote is encrypted at the voter's browser and remains so until it is delivered to the electoral board. The Java applet that is downloaded onto the voter's browser is digitally signed for authentication and integrity purposes.

To cast their votes the participants had to follow a simple identification procedure on the voting website, using the credentials that had been sent to them by post, as explained before. Once correctly identified, the voter selected one candidate list from the selection presented on-screen (including the blank vote option), and then clicked on a button to cast the ballot. Before casting the ballot, the Java applet presented another screen to confirm the choice done by the voter, and, once confirmed, the vote underwent a series of cryptographic operations in the Java applet to encrypt the vote, which was sent over the Internet to the voting server. This series of operations lasted on average a couple of seconds.

Once the vote was sent and confirmed, the applet provided a voting receipt that enabled the verification of the vote's inclusion in the final tally. The voting receipt consisted of a unique vote identifier (the vote's serial number) and the control code (actually the digital signature of the vote identifier and other election data).

The Java applet controlled all of the important operations in the voting process, so that voter's trust only needed to be placed in this audited and digitally signed piece of software and in the electoral board that oversees the process.

3.5 Vote Tally and Verification of Results

The vote tally was performed on November 16th in the World Trade Center of Barcelona, the same location where the real elections outcome was spread from, once the polls were closed at 20h00. The ballot box was opened and the tally initiated by the 7 members of the Electoral Board in front of more than 20 national and international observers as well as representatives of the Electronic Voting Study Group of the Spanish Senate. It took only 23 seconds to decrypt the votes and to obtain the results after the polls closed. The results and the voting receipts used for the result verification were published on November 17th on the official website of the pilot [GC03].

4 Electoral Results

Table 1 contains a list of the aggregated results of the pilot vote. No invalid votes were received (as it was expected) with 11 blank votes received, and 719 votes received for candidates for a total of 730 votes cast on the e-voting platform, which means a participation of 15.23% of the voters who cast a ballot by mail. These results were considered a success by the *Generalitat of Catalunya*.

Electoral Roll	Real Votes Received	Pilot Votes					
		Votes Received	Abstained	Invalid votes	Blank votes	Votes for Candidates	Valid Votes
23,234	4,794 (20.63%)	730 (3.14%)	22,504 (96.86%)	0 (0.00%)	11 (1.51%)	719 (98.49%)	730 (100.00%)

Table 1: Aggregated Results of the Pilot Vote

Table 2 compares participation rates of postal voting with those of Internet pilot.

Country	Electoral Roll	Method of Voting	Votes Received	Abstained	Participation Rate	Internet as a % of Postal
Total	23,234	Post	4,794	18,440	20.63%	**15.23%**
		Internet	730	22,504	3.14%	
Argentina	10,539	Post	3,034	7,505	28.79%	**9.56%**
		Internet	290	10,249	2.75%	
Belgium	1,876	Post	632	1,244	33.69%	**8.70%**
		Internet	55	1,821	2.93%	
USA	4,210	Post	409	3,801	9.71%	**38.63%**
		Internet	158	4,052	3.75%	
Mexico	4,528	Post	68	4,460	1.50%	**226.47%**
		Internet	154	4,374	3.40%	
Chile	2,081	Post	651	1,430	31.28%	**11.21%**
		Internet	73	2,008	3.51%	

Table 2: Comparison of Postal Votes to Internet Votes

The participation figures for the pilot highlight some interesting results. While over 15% of voters who voted by mail also participated in the pilot by voting a second time by Internet, there was a large variance in participation rates depending on which country the voter voted from. The lowest participation rate was 8.7% for Catalans living in Belgium while in Mexico it was 226.47%, meaning that more than twice as many people voted in the pilot than returned a postal vote in the real election. Over one third of the Catalans resident in the U.S. who voted in the election also participated in the pilot (38.63%).

There are probably at least two important factors affecting these rates: the level of Internet penetration in the country of residence, and the speed / reliability of the postal service in these countries. One might expect that the participation in the United States to be higher than that of Argentina due to the higher penetration and use of the Internet in North America. It has been suggested that the very low participation rate in Mexico was due to problems receiving the postal ballot in time to return it to Catalonia to be counted before the deadline. This latter case neatly highlights one of the biggest advantages of Internet voting, in that it enables higher participation rates, especially among those who experience difficulties voting by mail. Regarding the participation from the Casals Catalans, Scytl is only aware of about 40 people voting from three different ones located in Argentina and Mexico.

5 Voter Feedback

One of the electronic remote voting pilot's aims consisted in evaluating the opinions of the voters regarding this new voting method. After voting, voters were asked to fill in a simple survey located on the same voting website. From the 730 voters that participated in the pilot, 563 (over 77%) answered the survey, with 216 voters providing comments. Table 3 provides a summary of the survey responses.

Survey Questions	#Resp.	%	Survey Questions	#Resp.	%
1. In general, how would you describe the remote electronic voting pilot experience?					
Very satisfactory	397	70.52%	Satisfactory	151	26.82%
Unsatisfactory	10	1.78%	Very Unsatisfactory	5	0.89%
2. What confidence does the remote electronic voting process give you?					
Much confidence	286	50.80%	Reasonable	255	45.29%
A little confidence	18	3.20%	No confidence	4	0.71%
3. How would you rate the electronic and remote voting process?					
Very easy to use	347	61.63%	Easy to use	206	36.59%
Complicated	9	1.60%	Very Complicated	1	0.18%

4. What factors are most important to you when using a remote electronic voting platform like the one in the pilot? (Multiple answers are possible)					
Comfort	411	73.00%	Security	187	33.21%
Ease of use	146	25.93%	Others	15	2.66%
5. Would you have chosen this voting system if it had been a real (and binding) alternative to postal voting?					
Definitely	471	83.66%	Probably	82	14.56%
Unlikely	3	0.53%	Definitely not	4	0.71%

Table 3: Summary of Survey Results

The voter's opinions showed a clear approval of the system: over 97% were satisfied or very satisfied with the experience, 96% found that the system gave much or a reasonable amount of confidence, 98.2% considered that the voting process was easy or very easy to use, and 98.2% definitely or probably would have chosen this system to vote if the process would have been binding. Finally, of the factors that the voter considered as the most important in using the system, the comfort of easily voting from home is chosen (73%) as a big advantage of Internet voting, and the security offered by the system represents the next important thing to consider (33.2%).

6 Security risks and proposed solution

As broadly accepted, electronic voting and electronic consultation have the potential to improve our electoral processes and enhance democracy in many ways [HD00, Ch02, CM03, Ra02]. However, electronic voting is not problem-free. A whole new set of risks and challenges is created by this new voting scenario that is based on the use of electronic voting systems [MN03]. These risks and challenges can be broadly classified in three categories: legislative, socio-political and technological. An analysis of several socio-political and technical concerns can be found in [Ra02].

This section focuses on the currently most debated risks and challenges that relate to security, trustworthiness and confidence [Ra02, BM03, Jd04], proposing solutions to address them.

Traditional paper-based voting systems obtain their confidence through the direct, face-to-face interaction between voters and election authorities, as well as the physical evidence (paper ballots) that remains after the polling places close. Ballot secrecy and integrity is preserved by paper envelopes and physical ballot boxes. The fairness of the tallying process relies on the fact that electoral boards are composed of (and/or monitored by) people of opposing interests (e.g. members of different parties), which presumably prevents any collusion to alter the election results. Moreover, independent third parties and observers supervise the entire electoral process.

In contrast, pure electronic voting introduces a totally new interface between voters and election authorities and it removes the *physical* audit trails. The straight human-to-human interaction is substituted by a variety of hardware and software components, whose inner workings are not easily accessible or understandable. A new and complex technological infrastructure is interposed between the voters and the election authorities who in the end will tally the votes, obscuring the transparency of the ballot casting process. In addition, to create and administer this new infrastructure, technicians control the computer systems that are between the voters and the electoral board. Through their positions and functions, these technical people have many privileges that could be used to corrupt the electoral process. Therefore, naively implemented electronic voting systems can pose very serious threats to election integrity and shake the public's confidence in elections. Advanced security measures are clearly needed, to achieve the desired level of trust

We propose a security architecture for electronic voting that replicates the conventional security measures found in traditional elections. The principal objective of this architecture is to avoid putting all of one's trust on the computing infrastructure and on the technical people operating between the voters and the electoral authorities. The group of systems that compose the front-end of an electronic voting system (the systems that capture the ballots, e.g. web servers) are by definition complicated machines and difficult to completely protect or to certify, even more if connected to the Internet.

Our proposal consists in maintaining a clear separation of critical and non-critical modules. In this way we propose changing the current paradigm of electronic voting, in which the casting, recording and counting of ballots is grouped in a unitary, complex system, more easily accessed by technicians than by electoral board members. We propose to place all the critical tasks on two simple modules located at the extremes of the system (the voter and the electoral board). By means of end-to-end, application-level cryptographic protocols designed specifically to address the problems associated to electronic voting, a direct secured voting dialog can occur between the voter and the corresponding electoral board. The integrity of the electoral process is no longer exposed to the rest of the electronic voting infrastructure, systems, components and technical personnel interposed in between. These two modules at the extremes are very simple, auditable, open, and protected by physical and logical security. All the critical functions described below are realized in these two extremely simple modules.

The first module is the voting agent used by voters. It is a light-weight piece of software that can take the form of a digitally-signed applet of a couple hundred kilobytes, running in the voter's browser. The certification of such an applet avoids all of the complexity associated with the host operating system, the ballot presentation software, the network interface and so on. For improved security in remote electronic voting, the voting agent could run on a "clean" operating system version loaded from a bootable CD-ROM provided by the electoral authorities.

The second module is the electoral board agent. It consists of software, which is used to generate sensitive cryptographic keys and other critical data, and perform the critical process of opening digital ballot boxes, breaking the correlation between the voters and the contents of their ballots using cryptographic mixing processes [Cd81]. This software should be open, at least to the electoral authorities and political parties, which should extensively audit it. It runs on a very simple computer or specific-purpose hardware system, totally disconnected from any network and directly operated by election authorities and constantly monitored by several parties. Physical security is extremely important to protect this module.

A more detailed description of the security architecture introduced before, which was used in the Catalan pilot, can be found in [Ra03, SCT03]. Also, a summarized description of how the previously introduced security architecture addresses most of the security concerns raised in the SERVE security report [Jd04] can be found in [Ra04].

7 Concluding Remarks

Judging from the voter participation rates, survey results and the technical problems that were reported, we conclude that the 2003 Catalan electronic remote voting test pilot was a success. Given that this was a non-binding pilot where voters would have to vote twice to participate – once for real by mail, and a second time for the pilot by Internet – and where the promotion of the pilot was scarce, a 15.23% participation of postal voters can be considered as an excellent result. The participation rate demonstrated the interest among the voters in an alternative voting channel, as stated by many electors who indicated their predisposition to use this electronic system in binding elections in the future. The main objectives introduced at the beginning of this document, which reflect the main advantages of the remote electronic voting, were fully achieved, facilitating the participation of Spanish citizens living abroad with a secure and user-friendly e-voting system.

Another great success of the pilot was that it led to the identification of some areas of improvement, basically related to usability, and they have already been solved. The pilot also helped the Generalitat to detect some things not initially considered key in which remote electronic voting technologies can help: (1) to allow citizens who are not necessarily abroad to vote remotely, (2) to reduce the resources needed to manage the election, (3) to facilitate the management of the electoral rolls, and (4) to get voters' opinions on governmental actions between elections.

In the last few years, several governments around Spain and Europe have run different kinds of e-voting pilots, in order to test the technology and the social response to this technology. We believe that, after carefully considering the security and usability issues, the technology is mature and that the society demands it. Now it is time for legislators to step up and amend the, usually old, laws regarding electoral processes and citizen participation in order to cover the use of these new technologies

Bibliography

[GC03] Generalitat de Catalunya: Eleccions al Parlament de Catalunya 2003, http://www.gencat.net/governacio-ap/eleccions/e-votacio.htm. (In Catalan)

[Aa99] Ambrosio, A.: Electronic Voting Experiment, Generalitat de Catalunya, 1999.

[SCT03] SCYTL: Pnyx Electronic Voting System White Paper", http://www.scytl.com/voting.html

[Ra03] Riera, A. et al: Advanced Security to Enable Trustworthy Electronic Voting, Proc. 3rd European Conference on eGovernment (ECEG), Dublin, 2003.

[HD00] Hacker, L., J. Van Dijk: Digital Democracy. Issues of Theory and Practice, Sage Publications, London, 2000.

[Cd81] Chaum, D.: Untraceable electronic mail, return addresses and digital pseudonyms, Communications of the ACM, vol. 24, issue 2, pp. 84-88.

[CM03] Canals, I., Martí, JL.: *L'Àgora Digital. Internet al Servei de la Participació Democràtica*, Fundació Catalunya Segle XXI, Barcelona 2003. (In Catalan)

[Ra02] Riera, A. et al: Electronic Government: Design, Application and Management (ed. Gröndlun A.), Idea Group Publishing, London 2002, pp 78-98.

[Jd04] Jefferson D. et al: Serve Security Report, http://www.servesecurityreport.org, 2004

[Ra04] Riera, A: Comments by Scytl on the SERVE security report, http://www.sctyl.com/docs/Scytl_comments_on_SERVE.pdf, 2004

[MN03] Mercuri, R., Neumann, P.G.: Verification for Electronic Balloting Systems, Secure Electronic Voting (Ed. Gritzalis, D.A.), pp. 31-42. Kluwer, Boston 2003.

[BM03] Burmester, M., Magkos E.: Towards Secure and Practical E-elections in the New Era, Secure Electronic Voting (Ed. Gritzalis, D.A.), pp. 63-76. Kluwer, Boston