

Advanced Security to Enable Trustworthy Electronic Voting

Andreu Riera Jorba, José Antonio Ortega Ruiz, Paul Brown

Scytl Online World Security, S.A.

Entença, 95, 4-1

08015 Barcelona (Spain)

Phone: +34 934 230 324 Fax: +34 933 251 028

andreu.riera(a)scytl.com, jao(a)scytl.com, paul.brown(a)scytl.com

Abstract

Electronic voting (whether it is remote or poll-site) has a lack of transparency that makes its use controversial. Currently there is a lively debate regarding the deployment of electronic voting systems, with people arguing whether trustworthiness is only achievable by means of the use of backup paper trails. We believe that paper trails are not strictly necessary. In our opinion, the lack of transparency of electronic voting systems can be overcome to a great extent by using adequate security measures (technological, physical and procedural). Such security measures would provide clarity to the process and avoid the need to rely on complex and/or networked systems and/or proprietary closed systems.

Keywords: Electronic Voting, Security, Trust, e-Democracy.

1. Introduction

Lately, electronic voting has received much attention partly due to the electoral fiasco of the state of Florida during the US Presidential elections in November 2000. The problems revealed many deficiencies of the electoral equipment and of the systems in use (Cranor 2001, Baltimore et al. 2001). Faulty equipment, confusing ballots, registration mix ups, mistakes in polling place operations and absentee ballot problems caused the loss of between 4 and 6 million votes (Baltimore et al. 2001). Such situations shake the public confidence in democratic processes. As a consequence of this, funding initiatives have been set up by many governments worldwide, either to upgrade election equipment or to experiment with new voting methods. In October 2002, the US federal government allocated \$3.9 billion to upgrade older election equipment with the Help America Vote Act. In the EU, many countries are experimenting with electronic voting and defining adequate strategies for its deployment. While the Netherlands has had electronic voting machines since the 1970s, Belgium, Ireland and France are all expanding the use of these machines for their elections. Other countries like Germany and Norway have run or will run pilot projects involving electronic voting machines. Yet other countries are looking into remote electronic voting, with the UK, Netherlands, Switzerland, Italy, Spain, Germany, Finland, Greece and Estonia all at various stages of studying and testing remote electronic voting systems. Improving voter turnout is in many cases a primary objective.

The exploration of alternatives to current election systems has boosted the research into ways to improve elections through the increased use of advanced technology. Because of this, in the past few years electronic voting has been raised by politicians, the electoral industry and by independent experts of the electoral industry as an actual possibility. This has caused a heated debate regarding the convenience, advantages and risks of a full-scale implementation. While electronic voting does have an inherent lack of transparency that makes its use controversial, it is clear that if properly deployed it offers several advantages over conventional methods of voting, including greater speed and accuracy of ballot tabulation and greater convenience for voters.

In our opinion, electronic voting has the potential to not only modernize electoral processes but also to improve the interaction between citizens and their governments through e-participation platforms based on information and communication technologies (ICT). However, to take full advantage of the benefits and promises of electronic voting, advanced security measures must be deployed to compensate for the inherent lack of transparency and to increase confidence in the new system by both voters and election authorities.

In this paper, we present our views with regard to the security standards that must be set in electoral processes driven by electronic voting systems. In Section 2 we start by providing some definitions about electronic voting, and also listing the main advantages offered. In Section 3 we introduce the currently most debated risks and challenges posed by electronic voting. In Section 4 we present an overview of a security architecture that may be employed to circumvent these risks to provide trust to electronic voting. Finally, Section 5 includes some concluding remarks.

2. Electronic Voting Definitions

Electoral processes in developed countries always include some sort of ICT at some stage. This happens most of the time in the “back-end” of the election systems (in counting centres where partial results are added up and in the broadcasting of totals). In contrast, the “front-end” of the voting system is likely to be completely non-electronic. In most European countries voters have to use paper ballots indicating their intention. These ballots are sealed in envelopes, which are in turn placed into the voting urn. The urn is controlled and monitored during the election by an electoral board. At the end of the voting period, the electoral board opens the urn and starts the manual counting process, to provide a partial tally. In some countries, individual ballots are destroyed after the partial tally has been computed and agreed upon, while in other countries the paper ballots are stored for recounting purposes. No electronic devices or systems are involved in this kind of traditional voting front-end process. There is a direct, human interaction between voters, electoral board members, and polling place staff. They all only have to deal with physical elements such as envelopes and physical urns. A variation of this traditional method involves the use of optical scanning machines to speed up the counting process by electoral boards. However, such systems are still essentially paper-centred.

Electronic voting incorporates ICT in the front-end of the election system. An electronic device is used to record the voter’s intention directly in a digital form into the device. Therefore, instead of dealing with conventional paper-based physical ballots, voters deal with electronic devices that have some form of interface that presents virtual digital ballots. After making their choices, voters do not need to deliver ballots to the electoral board. Some form of ICT-based system will do this task on their behalf (involving communication networks and/or digital storage systems). The existence of ballots in a digital form from end to end has a number of potential advantages over traditional paper-centred voting systems. It:

- Increases the speed and accuracy of ballot tabulation.
- Saves materials required for printing and distributing ballots.
- Offers better accessibility for people with disabilities.
- Offers a flexible ballot design that can be modified at the last minute.
- Provides multiple-language support for the ballots.
- Permits the access to more information regarding voting options.
- Prevents unintentional mistakes by voters (both in overvoting and undervoting).

Electronic voting systems may be classified in two main groups depending on where the casting of the ballot takes place: poll-site or remotely. Poll-site voting systems consist of so-called Direct Recording Electronic (DRE) devices situated at polling places, which allow voters to cast their ballots directly through the machines – typically by means of touch-screen apparatus. Voters have to go to the polling stations, and they are identified by conventional means. DREs have a graphical user interface that presents the voting options available, allows voters to make a choice and requires a confirmation before the vote is definitively recorded and added to the total.

Remote electronic voting systems fully exploit the potential of ICT. Voters still use a graphical user interface as with DREs, although the casting of ballots is done remotely, such as from home using one's own personal computer, or from computer kiosks at embassies or at hospitals. The basic idea behind these systems is to move digital information (the votes) through communication networks instead of obliging people to move to the voting location. Remote electronic voting offers the same advantages as poll-site electronic voting while adding the following:

- Economies of scale with respect to the size of the electoral roll (i.e. an increase in the size of the electoral roll does not increase the cost of the election linearly).
- Allows geographic independence of the voters and the resulting convenience of use.
- Facilitates increased electoral participation.

3. Electronic Voting Risks and Challenges

As explained in the previous section, electronic voting has the potential to improve our electoral processes in many ways. This sort of technology also promises to enable efficient participatory (e-consultation or e-participation) platforms with the objective of building trust in governments by allowing people to have their say in the decision-making process. Electronic voting and electronic consultation therefore become exemplary tools for enhancing democracy.

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 (Mercury and Neumann 2003, Neumann and Parker 1989, Alexander 2001). These risks and challenges can be broadly classified in three categories: legislative, socio-political and technological. Legislative challenges appear as a consequence of the introduction of new electoral legislation, as current electoral laws do not usually allow for electronic voting procedures (Watt 2002). Socio-political challenges and risks are consequences of the impact on the electorate of new ways of voting and in particular of ICT-based voting systems (Mitrou et al. 2003). The *digital divide* is often referred to as the primary socio-political issue (Hoffman and Cranor 2000). With respect to technological risks and challenges, the most important relate to security and confidence. An analysis of several socio-political and technical concerns with electronic voting can be found in (Riera et al. 2002).

This paper focuses on the currently most debated risks and challenges that relate to security, trustworthiness and confidence. Electronic voting systems are in their nature very different from traditional, physical voting methods. Because of these differences, four main sources of risks can be encountered:

- The digital nature of the ballots.
- The complexity of the systems used.
- The lack of transparency – to the voters and electoral authorities – of the systems used.
- The existence of people that have special abilities and/or privileges in the systems used.

These four factors act as the source of a whole range of particular threats and attacks. To name a few, electronic equipment may malfunction, software may contain intentional or unintentional programming errors, ballots may be deleted or manipulated by privileged actors, and voters' privacy may be undermined. All of these problems are very serious and can threaten the integrity of elections and undermine confidence in democratic processes as well. As the final range of problems is extensive, there are a large number of publications detailing security and integrity risks that can be found in electronic voting (Mercuri 1993, 2000, Phillips et al. 2000, Rubin 2000, Riera et al. 2002, Neumann 1993, Burmester and Magkos 2003). From the above, it is clear that an electronic voting system not suitably protected will face a large list of security problems.

In the past few years, and especially after 2000, a debate at many levels – academic, governmental and industrial – has taken place to discuss both the advantages and the security risks of electronic voting. Although most of the hype was initially placed on remote voting over the internet, this debate has been recently extended to all kinds of electronic voting, and it is currently including DRE-based poll-site voting systems. In the context of this debate, some computer scientists have championed the need to complement computerised electoral systems with a physical record (usually paper) of each vote that can be visually verified by the voter before being cast (Mercury 2002, Neumann 2000).

The call for a voter verifiable physical trail has recently received much attention and publicity in the USA as witnessed by the “Resolution on Electronic Voting” (Dill 2003) that has been endorsed by over one thousand people so far. In line with their arguments, in May 2003 Rep. Rush Holt of New Jersey introduced a bill, "The Voter Confidence and Increased Accessibility Act of 2003", in which a voter verifiable paper trail is required (Rush 2003).

The above resolution demands the incorporation of a paper trail in DRE machines. According to the resolution, DRE systems, although superficially attractive to both voters and election officials, hide many dangerous problems that can only be solved by the addition of a paper printer. The objective of such printer is to create a physical record of each vote, verifiable by voters in real-time, and useful for recount purposes. Without printers, they argue, DRE machines must not be used in elections in the US. In our opinion, there is room for improvement in current electronic equipment used in elections worldwide, although we believe that other solutions are possible that do not rely on the extensive use of paper. We believe that the ultimate goal is to have secure, reliable and auditable voting systems, rather than to have paper-centred voting systems.

Security, reliability and auditability of electronic voting may be achieved without a paper trail. Although the inclusion of printers in electronic voting systems is possible and gives an additional layer of confidence, it involves its own list of problems. Printers often have paper jams and they run out of paper. There are high costs in printing, securing and transporting paper ballots. The extensive use of paper poses, in general, administrative headaches for election officials. From our point of view, putting a paper trail in an electronic voting system

is like removing the engine from a brand-new automobile and pulling it around by a horse. It is possible, but it is senseless. Even the authors of (Baltimore et al. 2001) who for the short-term propose paper-based systems, recognise that the future is in the use of electronic voting systems. They state that “*in an increasingly large and diverse society, with many languages spoken and many different ballots required, paper is increasingly difficult to administer. Paper is not always as secure and indelible as we would like. It is virtually impossible for a blind person to vote without assistance. And, at the end of the day, voters may still lack confidence that their votes are counted. [...] We see a promising future for electronic voting, despite its problems today.*” (Baltimore et al. 2001, p. 56) We believe that adequate solutions must be devised to bring trust to pure electronic voting systems.

4. Enabling Trustworthy Electronic Voting

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 of traditional systems 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.

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, be they web servers or DRE machines) are by definition complicated machines and difficult to protect or to certify. These are usually closed proprietary systems that are exposed to some extent to the risk of internal attacks by privileged operators. In the case of servers connected to the internet, the number of risks clearly grows. This means that the effort to protect such machines becomes an extremely difficult task, and trusting them is not a good policy. We feel that opponents of electronic voting are correct on this point.

Our focus consists in maintaining a clear separation of critical and non-critical modules. In this way, it is only necessary to trust the two modules located at the extremes of the system (at the beginning with the voter and at the end with the electoral board). By means of end-to-end, application-level cryptographic protocols, a direct “secured voting dialog” can occur

between the voter and the corresponding electoral board. In this way, the electoral process integrity 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 with physical and/or logical security. All the critical functions described below are realised 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 either in the voter's browser or as an add-on to DRE software. 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. In the case of DRE-based poll-site voting, maximum security would be attained if the voting agent ran on a simple hardware device attached to the DRE machine.

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. This software should be open and extensively audited by several parties. It runs on a very simple specific-purpose hardware system, directly operated by election authorities and constantly monitored by several parties. It is connected to a dedicated network or, even better, totally disconnected from any network at all. Physical security is extremely important to protect this module.

At this point it may be noticed that the main principle of this security architecture changes the current paradigm of electronic voting, in which the DREs or in many cases the remote voting platforms group the casting, recording and counting of ballots in a unitary, complex system, more easily accessed by technicians than by electoral board members. We propose a new paradigm that permits a secure and trustworthy use of such complex proprietary DRE devices or remote voting platforms that offer the advantages of usability, flexibility, and support for multiple languages and for the disabled.

Let us provide an overview of how our two key software modules operate in order to circumvent the problems that plague unprotected electronic voting systems. During the ballot casting period, after the voter has been properly authenticated, the voting agent performs security functions on his/her behalf. For instance, the voting agent becomes the hands of the voter, cryptographically sealing the virtual ballot for him/her.

This takes place when the voter makes his/her choices on a virtual personalized ballot that is presented through the DRE device or the web pages that constitute the remote voting platform. Once the choices are made, the virtual ballot is not directly recorded by the DRE nor sent back to a ballot collecting server. Instead, the virtual ballot is passed to the voting agent, which seals it in a digital envelope. The digital envelope protects the confidentiality and integrity of the ballot, as it is created by using a public (encryption) key for which the private (decryption) key does not exist.

Other additional tasks performed by the voting agent include attaching a proof of authorship to the digital envelope (to ensure its authenticity) and obtaining a validated voting receipt. The voting receipt contains a unique identifier for the ballot. This unique identifier is not known by anyone as its creation and subsequent validation take place in a blind cryptographic

process. A copy of the identification number is placed into the digital envelope along with the virtual ballot, while the voter keeps a copy of the voting receipt (it can be saved to disk or printed on paper if desired). When the election outcomes are published the voting receipt will allow the voter to check whether his/her ballot has successfully reached the electoral board. If not, the receipt will allow the voter to complain with irrefutable proof, as it incorporates a digital signature proving its validity. It is important to stress that the voting receipt does not allow for systemic coercion or vote-selling, as it does not show who the voter voted for. This voting protocol enables the creation of ballot boxes that are secure even from privileged personnel that have programmed and/or are operating the systems that manage the ballots and the ballot boxes.

At the end of the election, the digital ballot boxes are securely transferred to the second critical software module, the electoral board agent. In the most secure scenario, this electoral board agent runs on secure and simple hardware completely disconnected from any network. This would require that the transfer of the digital ballot boxes is done by physical means in such cases. To open up the digital ballot boxes, a predetermined threshold of electoral board members must present their cryptographic credentials to the electoral board agent. This replicates the distribution of trust principle used in conventional elections in the digital domain. The collaboration of the members of the electoral board allows the reconstruction of the private key needed to open the digital envelopes that protect ballots. This is done simultaneously with a cryptographic mixing process (Chaum 1981), which breaks the correlation between the voters and the contents of their ballots, eliminating any possibility of the violation of their privacy. Moreover, as the ballots collected during the ballot casting period can only be decrypted with a non-existent key, this also ensures the secrecy of intermediate results (an important issue if the election takes place over several time zones or in the case of extended periods of voting).

The voting receipts that we described above fulfill the important mission of improving the voter's confidence in the system: the immediate reassurance that every ballot has been taken into account, that occurs when paper-based ballots are physically cast in front of the electoral board, is lost in electronic voting. In our proposed security architecture, all the unique ballot identifiers are published at the end of the election, electronically and/or in newspapers or official bulletins. Since each identifier is protected into the same digital envelope that contains the actual ballot, the publication of an identifier guarantees that the corresponding ballot has been received and processed by the electoral board (and therefore has not been lost or manipulated at any point between the voter and the electoral board). This is at least the same degree of assurance as that provided in conventional elections systems when the voter sees the paper envelope being placed into the urn that is controlled by the electoral board. Therefore, these voting receipts are an essential part of electronic voting that establish voter confidence in the system.

Conventional voting processes also provide an additional physical audit trail that allows verifying the fairness of the election by any trusted third party. The main component of this verifiable audit trail is paper-based and consists of the ballots themselves. In principle, electronic voting eliminates this well-known audit token (although it is also subject to threats, fraud and errors). Therefore, electronic voting systems must provide alternative means of independent verification. This issue has raised well-founded concerns (Mercury 2002), regarding specifically how to demonstrate after the election that all valid ballots (and only valid ballots) have been counted.

As explained previously, one proposed solution for DRE systems is the generation of printed ballots as a back-up paper trail. We feel that the current technology can and must go further, and provide audit trails that are safer and more dependable than paper-based ones. In the proposed security architecture, as every valid ballot incorporates a proof of authenticity that only the legitimate voter is able to create, this prevents privileged personnel from adding invalid ballots or from modifying the valid ballots. All the critical system operations are logged (using trusted, auditable software subsystems devoted to handling the voting protocol) and cryptographically protected with the aid of chained digital signatures created in tamper-resistant cryptographic hardware modules. The counting of ballots is a very sensitive process, and so it should take place in a very simple, tightly monitored, and physically-protected device. The software in this device must be subject to the highest software certification standards, and possibly including the requirement of being open-source (at least open to the proper certifying institutions). In addition to being constantly monitored, the device cannot initiate the opening of the ballots' digital envelopes until the members of the electoral board gather together.

We believe that electronic audit trails can totally substitute paper trails if so desired, but by no means prevent their use; in a way they can be an excellent complement to paper trails, reinforcing and enhancing them with the addition of the digital signatures validating the ballots in the printed records (properly encoded, e.g. using bar codes).

An implementation of the proposed architecture is already available (Scytl 2003) and it is currently being integrated in governmental systems and in ASP platforms providing voting to the private and public sectors. In this system, the voting agent is implemented as a small Java applet that can run in a wide range of client platforms, including the vast majority of desktop computer browsers, PDAs and interactive TV set-top boxes. The product can also be deployed in poll-site systems, providing a much needed trust boost to DRE-based electronic voting systems.

5. Concluding Remarks

When technology is carelessly applied to elections, it can create several risks and challenges that will shake the public's confidence in elections. However, the technology itself can offer proper solutions. It is necessary to raise the bar of security standards to maintain the integrity and confidence of elections, and in this work electoral authorities, the election industry and experts should participate. We should take advantage of the current momentum as well as the funding available in some countries to improve election equipment properly. The opportunity exists now, and we should not let it go by. We should also be wary of precipitating towards the first available solution that is offered which will probably tend to be reactionary and as such not well-thought out; the purchase of election equipment is a decision for the long term. We should therefore pay attention to the questions relating to security to maintain or even increase the public's confidence in elections while at the same time improving the speed of the recount and the convenience for the voters.

For our part, we have presented a security architecture for electronic voting that permits the avoidance of the problems occasioned by interposing computer systems and technical personnel between the voter and the electoral board. The architecture is based on replicating the conventional security mechanisms and in segregating all critical functions into very simple systems that are audited, monitored and physically secured. This security architecture minimises the number of components that must be trusted to only two, namely, the software

generating the encrypted ballot and the software opening the digital ballot boxes and the envelopes therein. This addresses one of the main causes of trouble in electronic voting systems, namely, the need to trust overly-complex systems like DREs, web browsers, operating systems or Internet servers.

The cryptographic voting protocol that is part of this security architecture allows voters to independently verify that the electronic voting system correctly delivers their ballots to the electoral board. Third parties (such as candidates or observers) have reliable means to gain confidence in the accuracy of the election. A conundrum is solved; voter privacy is ensured while every voter is properly identified before casting their ballot.

In our opinion, this architecture relaxes the need to use paper trails to have confidence in electronic voting. Nevertheless, if paper is to be used, the architecture allows improving the security offered by the physical paper trail by introducing cryptography to it.

Bibliography

Alexander, K. (2001), *Ten Things I Want People to Know about Voting Technology*. Presented to the Democracy Online Project's National Task Force. National Press Club, Washington, DC

Baltimore, D., Vest, C. et al. (2001) *Voting, What is, What it Could Be*, Caltech-MIT Voting Technology Project, [online], <http://www.vote.caltech.edu/Reports/index.html>.

Burmester, M., Magkos E, (2003) *Towards Secure and Practical E-elections in the New Era*, Secure Electronic Voting (Ed. Gritzalis, D.A.), pp. 63-76. Kluwer, Boston.

Chaum, D. (1981), *Untraceable electronic mail, return addresses and digital pseudonyms*, Communications of the ACM, vol. 24, issue 2, pp. 84-88.

Cranor, L.F. (2001) *Voting after Florida: no Easy Answers*, Ubiquity, Issue 47 ([online] <http://lorrie.cranor.org/voting/essay.html>).

Dill, D. (2003) *Resolution on Electronic Voting*, [online], <http://verify.stanford.edu/evote.html>.

Hoffman, L.J., Cranor, L. (Eds.) (2000), *Internet voting for public officials*. Communications of the ACM, vol 44, issue 1, pp. 69-85.

Phillips, D.M. & Jefferson, D. (2000) *Is Internet voting Safe?*, VIP Report, [online], <http://www.voting-integrity.org>.

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

Mercuri, R. (1993) *The Business of Elections*, Computers, Freedom and Privacy '93, Burlingame, CA. Available online at <http://www.cpsr.org/conferences/cfp93/home.html>.

Mercuri, R. (2000) *Voting Automation (Early and Often?)*, Inside Risks, Communications of the ACM, vol.43, n.11.

Mercury, R. (2002) *A Better Ballot Box?*, IEEE Spectrum, October 2002, p. 46-50 ([online] <http://www.spectrum.ieee.org/WEBONLY/publicfeature/oct02/evot.html>).

Mitrou, L., Gritzalis, D., Katsikas, S., Quirchmayr, G. (2003) *Electronic Voting: Constitutional and Legal Requirements, and their Technical Implications*, Secure Electronic Voting (Ed. Gritzalis, D.A.), pp. 43-60. Kluwer, Boston.

Neumann, P.G. (1993) *Security Criteria for Electronic Voting*, Proceedings of the 16th National Computer Security Conference, September.

Neumann, P.G. (2000) *Perspectives on Election Processes*, The Risks Digest ACM Forum, vol. 21, iss. 13, [online], <http://catless.ncl.ac.uk/Risks/21.13.html>.

Neumann, P.G., Parker D.A. (1989), *A Summary of Computer Misuse Techniques*, Proc. Of the 12th National Computer Security Conference, October.

Riera, A., Sánchez, J. and Torras, L. (2002) *Internet Voting: Embracing Technology in Electoral Processes*, Electronic Government: Design, Application and Management (ed. Gröndlun A.), Idea Group Publishing, London, pp 78-98.

Rush Holt of New Jersey (2003). *The Voter Confidence and Increased Accessibility Act of 2003*, [online], <http://holt.house.gov/issues2.cfm?id=5996>.

Rubin, A. (2000). *Security Considerations for Remote Electronic Voting over the Internet*, October, Sunworld.

Scytl (2003), *Pnyx Electronic Voting System*, <http://www.scytl.com/voting.html>.

Watt, B. (2002) *Implementing Electronic Voting*, [online], <http://www.lcd.gov.uk/elections/e-voting/pdf/legal-report.pdf>