

GI, the Gesellschaft für Informatik, publishes this series in order

- to make available to a broad public recent findings in informatics (i.e. computer science and information systems)
- to document conferences that are organized in cooperation with GI and
- to publish the annual GI Award dissertation.

Broken down into the fields of "Seminars", "Proceedings", "Monographs" and "Dissertation Award", current topics are dealt with from the fields of research and development, teaching and further training in theory and practice. The Editorial Committee uses an intensive review process in order to ensure the high level of the contributions.

The volumes are published in German or English

Information: <http://www.gi-ev.de/service/publikationen/lni/>

The 2006 conference on Electronic Voting took place in Castle Hofen near Bregenz at the wonderful Lake Constance from 2nd to 4th of August. This volume contains the twenty papers selected for the presentation at the conference out of more than forty submissions. To assure scientific quality, the selection was based on a strict and anonymous review process. The papers cover the following subjects: e-voting experiences, social, legal, political, democratic and security issues of e-voting, as well as solutions on how to (re)design election workflows, and finally how to implement and observe electronic voting systems.



Robert Krimmer (Ed.): Electronic Voting 2006

P-86

GI-Edition

Lecture Notes in Informatics

Robert Krimmer (Ed.)

Electronic Voting 2006

2nd International Workshop
Co-organized by Council of Europe,
ESF TED, IFIP WG 8.5 and E-Voting.CC

August, 2nd – 4th, 2006
in Castle Hofen, Bregenz, Austria

Proceedings



Maintaining Democratic Values in e-Voting with eVACS®

Carol Boughton

Software Improvements
Unit 20, 16 National Circuit
2600, Barton ACT, Australia
carol@softimp.com.au

Abstract: The principles of equality, secrecy, security and transparency apply to any democratic election system irrespective of whether paper ballots, mechanical or electronic means are used to conduct the election. All these principles were mandated as requirements, designed into, and successfully operated as features of, eVACS®, the electronic voting and counting system used since 2001 by the Australian Capital Territory Electoral Commission. How eVACS® achieves these requirements is described in this paper, with particular emphasis being given to security and transparency and the approaches adopted to ensure verifiability via electronic audit trails.

1 Introduction

All democratic election systems have many features in common no matter where a particular system is applied.

In the UK [Wa02], six principles were initially identified as forming the minimum requirements of a democratic election procedure. Public consultations established wide community support as well as leading to their simplification to three principles.

1. the **doorkeeper** principle: - Each person desirous of voting must be personally and positively identified as an eligible voter and permitted to complete no more than the correct number of ballot papers.
2. the **secrecy** principle: - Admitted voters must be permitted to vote in secret.
3. the **verification, tally and audit** principle: - There must be some mechanism to ensure that valid votes, and only valid votes, are received and counted. The system must be sufficiently open and transparent to allow scrutiny of the votes and subsequently the working of the political process.

More recently three democratic values were identified as being essential to any voting system adopted in the USA [To04]:

- i) **equality** (of political participation), including racial equality; multi-lingual access; disability access; inter-jurisdictional access (or no differential treatment to voters based on the county or jurisdiction where they reside);
- ii) **security** (the resistance of votes and vote totals to fraud and other forms of manipulation); and
- iii) **transparency** (the capacity to produce auditable results in which both candidates and voters can justifiably have confidence).

These values or principles of **equality, secrecy, security** and **transparency**, apply to any democratic election system – no matter whether the election is conducted using paper ballots, mechanical or electronic means. Exactly these requirements were recognised and specified in 2000 for the electronic voting and counting system eVACS®, successfully used by the Australian Capital Territory (ACT) Electoral Commission in the 2001 and subsequent ACT Legislative Assembly elections [EI02] [EI05]. Descriptions follow on how eVACS® ensures **equality, secrecy, security** and **transparency** with particular emphasis on the approaches adopted to ensure verifiability via electronic audit trails.

2 Equality

The voting set-up is identical for all users. For the vision impaired, or voters with poor reading skills, audio is provided and, if required, a larger screen. Privacy is maintained by the use of a headset, with voters able to use their own headset or a disposable one. The use of a (special) keypad to record choices/preferences enables voters with a range of physical impairments to vote without assistance. For preferential or proportional election systems in which voters are required to indicate a sequence of numbered preferences, selection of a candidate automatically assigns the next number in the sequence ensuring there are no missing or repeated numbers. Thereby ensuring voters do not unintentionally vote informally.

Other features addressing equality include instructions being provided in the voter's language of choice, as well as the local language of the region, using any alphabet or character set. If permissible by law, voters are able to vote away from their normal polling place. The hardware can be placed to give voters their choice to either sit or stand to vote.

3 Secrecy

Vote secrecy is maintained in five ways. First, the voting screen is positioned so that no other person is able to see a constructed vote. Second, the system fits in a normal (cardboard) voting booth. Third, for the standard arrangement no noise signals are emitted to alert anyone else as to how a voter may be voting.

Fourth, because voters ‘navigate the electronic ballot’ using the keypad, it is extremely difficult for anyone else to be able to discern who is being voted for. And fifth, a voter can ‘hide their vote’ if they need to seek assistance from an official.

In addition, all of the equality features (described in Chapter 2) increase the number of people who can vote without assistance, and thereby vote in secret.

4 Security

Security involves a number of design and operational aspects covering software and hardware, including a log of all activities. Automated set-up arrangements ensure that an election is run from a series of auditable write once CDs, and on loading the software, the hard disk/s are reformatted thereby removing any existing operating system and other software. Limited functionality, for voters and officials, means software cannot be modified during an election.

At the polling place each voter is randomly assigned a barcode, from a restricted set of barcodes internally generated by the system. The barcode determines in which election/s a voter is eligible to vote, ensures only completed votes are stored, and identifies incomplete votes if the network is disrupted. Whether a barcode has been used is checked automatically before voting commences and may also be checked manually.

All votes are cast in a public polling place over an isolated LAN with votes only stored on physically secure voting servers. No votes are stored on voting machines used by voters. The votes are stored simultaneously in two separate databases to guard against loss of votes due to hardware failure. Additionally, the outcome of a rerun in sequential order of voter keystrokes must match with the voter’s choices before a vote is recorded and stored. Downloading of votes at the end of polling requires password and encryption keys, not transmitted to polling place officials until after polling closes. Votes are encrypted and downloaded to two write once CDs with checksum. Both disks have to be loaded into the counting server and match the checksum.

The combined auditing and internal security features ensure a court is able to verify the CDs that were used for a specific election, and that the election result is accurate and has not been tampered with in any way.

4.1 Security of hardware

The election software runs on any hardware that supports the Linux operating system. The degree of in-built security of hardware can vary significantly between equipment. Consequently, there is an emphasis on maximising security via the software with physical security an added feature where available.

Used in the 2004 ACT Legislative Assembly Election, the ROC - Rugged Operations Computer - specially designed for electronic voting [Ro04] [E105], provides advantages over standard PCs in respect of ease of set-up and use, as well as better protection against external damage from liquids, solids, heat and physical damage. Each polling place LAN network is also physically protected against attempts to break into the system.

5 Transparency

In paper based voting systems transparency is managed by having observers/scrutineers present at different stages of the voting and counting processes, such as: empty ballot box and then securing (eg by sealing or locking) the box at the start of polling; ballot boxes remaining secured until after close of poll; only those people who actually attend the polling place are marked off the electoral roll at that polling place; assistance to voters incapable of marking their ballot paper by themselves; only voters place the appropriate ballot papers in the ballot box during polling; emptying of ballot box at the close of polling; counting of ballot papers after close of poll; secure transportation and/or storage of the votes; and recounting of votes.

Electronic voting and counting must, by necessity, change the nature of scrutineering, but computerising the voting and counting processes ought not prevent elections from being transparent, nor prevent scrutineers from observing all aspects of the voting and counting processes. *“A computerised voting and/or counting system is in essence a series of mechanical steps, facilitated by computer hardware and computer programs. A thorough understanding of the way in which the hardware and programs work – the electronic trail – should serve to demonstrate that the system is transparent, and in particular, that ‘what goes in is what comes out’.”* [Gr03]

There are some activities of scrutineering that are outside the scope of electronic voting. To ensure the anonymity of votes there can be no connection between the voter’s details and their vote. Any system for marking people off the electoral roll (either paper or electronic) must be independent of the voting and counting processes. Hence, the observation process to ensure only eligible people vote continues independently of eVACS®.

As with paper ballots, transparency in an electronic election has a number of stages, grouped into five levels, none of which is sufficient by itself to demonstrate the required transparency for an election. Each level of transparency must be completely fulfilled.

In the first level of transparency code is available so others can assure themselves that the software does what it is meant to do and nothing else. The Electoral Commission arranged for independent auditing of the software code used for acceptance testing and then in an election. The audited code was released publicly.

After the 2001 election, researchers from the Australian National University independently verified the counting algorithm and replicated the results of the 2001 ACT Assembly election.

The second level of transparency requires the correct operation of the vote recording and paper ballot data entry processes, and votes counted accurately according to the specified election system. Extensive testing prior to the software being put into service was undertaken, plus acceptance testing by the customer prior to auditing with representatives from political parties and disability groups observing.

For the third level of transparency, the software used for an election can be shown to be exactly the same software that passed first and second levels.

The fourth level of transparency involves Officials demonstrating the in-built features of the closed system ensure the limited functionality cannot be tampered with during use in an election, there is an empty electronic ballot box at start of election, the number of votes (formal/informal) in electronic ballot box, the initial results (for specific polling places), and secure downloading of votes. Downloading of votes is security controlled both to download and when uploading into counting server with encryption of votes, password access and checksums on CDs.

To achieve the fifth level of transparency voters and officials have to be confident that none of the recorded votes are lost, and that only completed votes are recorded. Activities to meet other levels demonstrate the former, while the barcode provided to each voter is used to start and end a voting session and ensure only completed votes are recorded.

In addition, there must be a well-documented 'electronic trail' with all the development artefacts and code available for independent auditing, and the source code published for examination by interested persons.

On the introduction of computer technology as applied to electoral matters in Australia, the then Commonwealth electoral authority's explanation for its reluctance to move too rapidly into computers in 1982 was: *It is absolutely essential not only that an election system be fair, but that it is seen to be fair. The safeguards built into the current system are the product of many years of experience. The full-scale introduction of a new, and much more complicated system could create opportunities for illicit interference, or allegations of such interference, with the electoral process. A completely new security process would have to be developed – one which would be acceptable to the electorate, the candidates and the political parties. (op cit Hansard V.129 1982 1614). [Mc01]*

While new steps in computerisation of the election process have subsequently been taken each year, they have not been submitted, step by step, to parties and candidates for open debate, let alone to the electorate (*page 166 of [Mc01]*).

In Ireland the Commission on Electronic Voting in its first report [Ir04] was unable to recommend use of the chosen electronic voting system because the accuracy and security could not be established as: i) there was not sufficient time to fully test the system, ii) the full source code had not been made available, iii) the version to be used was unknown and therefore the accuracy of the system could not be certified, and there were concerns that secrecy of the vote might be compromised.

In marked contrast, the development and introduction of electronic voting and counting in the Australian Capital Territory occurred with public participation. eVACS® was developed after direct public consultation had led to legislative changes to enable electronic voting and counting, undertaken in association with a Reference Group (with representatives of candidates, political parties and the public) whose members were able to participate in the acceptance testing, and the source code released for public scrutiny before use in an election.

Apart from ensuring a completely transparent electronic trail, elimination of opportunities to tamper with election results is another benefit of electronic voting. Opportunities such as ballot box stuffing, completed ballot papers from a polling place being “lost” and completed ballot papers deliberately inserted in the wrong stack for counting.

Electronic votes cannot be prepared in advance; voting must occur at the polling place and under the direct observation of others. The period when electronic voting is available at any polling place is logged by recording the time whenever the system is activated (start voting) or deactivated (stop voting). A unique barcode must be obtained for each electronic vote.

Electronic votes are stored in duplicate on the voting server at a polling place. The votes are downloaded twice onto separate write once CD-ROMs with a checksum. Details from both CDs are loaded into the counting server and confirmed with the checksum before the votes are added to the counting database. The only option for downloading votes is to download all votes stored on the voting server. Votes for a particular polling place can only be added once to the counting database. A report is available of polling places from which votes have not been imported into the counting database.

Once confirmed by a voter, the limitation of functionality means there is no way to interfere with the content of an electronic vote. There is no means to change the counting program once a specific election has been set-up.

5.1 Recounts and petitions

Recounts were introduced to address the known failings with manual counting of votes, and usually occur when the result of an election is very close. Either the electoral agency or a candidate may seek to have the votes recounted. Also, in some jurisdictions there is a mandatory requirement to recount a proportion of all votes to check the accuracy of the manual count. Whereas in other jurisdictions, a candidate, a voter or the electoral agency may dispute the validity of an election via a petition to a court.

Electronic voting and counting has significant impact on the conduct of recounts and for contesting election outcomes in the courts. The demonstrable accuracy of electronic voting and counting avoids the unnecessary recounts when election results are close. Mandated recounts are not practical with electronic voting, although a random set of votes could be printed and counted manually with less accuracy. With petitions, the issues are not ones of ‘who did or did not do what’ or ‘what was permissible under the election legislation’ but whether the computer program used met the appropriate standard of accuracy, reliability and trust. The transparency has to enable a court to independently establish the accuracy, reliability and trust in the election system.

5.2 Electronic voting and voter verifiable audit trails

There is no question about the need for voter verifiable audit trails with electronic voting. However, as per [To04], a ‘voter verifiable audit trail’ is not synonymous with ‘*paper* ballot replicas’.

Voter verifiable *paper* audit trails are often cited as the solution to addressing problems encountered with electronic voting in the USA. Yet as has been shown [To04] [E105], whether a voter verifiable paper audit trail is both a practical solution and an effective means of preventing fraud is highly questionable. For example, the tape for a voter verifiable paper audit trail system used in Clark County, Nevada, USA, contain 64 voter verifiable paper ballots from one voting machine, is a strip of 10cm (four inch) wide paper, just under 120 metres in length (318 feet) and “it took a four person team - one counting votes, one verifying and checking for errors and two recording results – about four hours to check one tape, or nearly four minutes per ballot” (photograph in [eo05]). The ability of election officials to accurately determine election results under such circumstances becomes a costly exercise in checking and cross checking.

The USA is not the only country where concerns have been raised about the electronic voting system used. Others are Brazil [Re03] and the NEDAP Powervote system trialled in Ireland [Ir04].

There are some who believe no electronic voting system can be trusted and therefore a paper audit trail is absolutely essential [Me01]. Yet others caution against sacrificing the voting rights of disabled voters and non-English speaking citizens in order to achieve the admirable goal of enhancing election security and transparency [To04]. A voter verifiable paper audit trail is obviously not an option for the vision impaired, poor readers, or voters who cannot read the language of the print out.

Not all the issues raised with electronic voting have been about ensuring votes are recorded accurately at the polling place. There have been reports of vote databases being accessed by the public, uncertified software being used, bug fixing occurring during an election, and equipment being certified without meeting certification requirements [B105]. With an appropriate ‘voter verifiable audit trail’ none of these issues should eventuate.

All of the concerns with electronic voting have arisen where there has been no transparency of the software used nor any serious attention to security issues prior to implementation of the system. In contrast, with eVACS® all of these issues were addressed before the system could be used in an election.

6 Voting is not everything

Maintaining democratic values does not simply apply just to the voting process. The third principle (see Chapter 1 and [Wa02] and [To04]) is to ensure that only valid votes are counted and that the counting process is auditable and transparent. Incorporation of this requirement starts with the set-up for a particular election, and applies equally to all other phases of the election process.

One of the major benefits of electronic elections is the speed at which election results can be determined. To achieve these benefits though, all votes need to be available electronically. Wherever postal voting or the equivalent is available not all votes will be recorded electronically, so there is need for a module that will convert paper votes into electronic votes. Ensuring the same level of accuracy and trust, as for electronic voting, in this conversion process is absolutely critical to ensuring only valid votes are counted.

Having a fully auditable process throughout all phases of an election therefore means that features of transparency and security have been applied to all modules of the eVACS® system, as well as to the interconnections.

6.1 Set-up election

Reference is made in Section 4 to an election being run from a set of auditable write once CDs, and to limited functionality such that the software cannot be modified during an election. In practical terms, the auditable set-up election CD is loaded on to a standalone PC – the set-up election server, and the hard disk reformatted. The set-up election server is then used to generate the voting server and data entry/counting server CDs for a specific election. All CDs are treated with the same degree of protection as ballot papers when being transported but in addition have in-built checksum and encryption features to ensure what was downloaded from one part of the system is identical with what is loaded into another part of the system.

eVACS® is referred to as a ‘closed system’ since there is no interaction with any other software.

6.2 Entry of non-electronic votes

The original eVACS® uses a data entry process for incorporation of non-electronic votes with double entry of the paper ballot details and separate authorisation for editing when entries do not match. Scrutineers are able to observe the entire process.

Developments in scanner technology since 2001 mean there may be an alternative to data entry for managing non-electronic votes, but with two issues that need to be addressed. First, scanning of all paper ballots is not always achievable, and second, particularly when preference numbers are written, not every paper ballot can be scanned with 100% accuracy. As a consequence an auditable and traceable editing process equivalent to that provided for data entry in eVACS® is necessary to ensure that only valid votes are entered and counted.

6.3 Counting and reporting

Counting has different facets that must all be proven to be auditable and transparent: the actual counting algorithm; the process by which electronic votes from different sources are merged for counting; and the actual reporting of results.

Counting algorithms don't just count votes. They determine which votes are valid (or formal) votes. Also, they may need to cater for different interpretations of vote information from votes received by a candidate who dies before the election results are announced. Additionally, when two or more candidates receive the same number of votes there may be a formal separation process that needs to be initiated during the counting process.

For many elections, votes from a number of sources such as different polling places, or electronic and non-electronic votes need to be merged for counting. Ensuring that votes can only be included once is critical to undertaking an accurate count.

Another, often overlooked aspect is the potential for manipulation of results after a count has been undertaken. It is important that the results are not accessible before printing the official election results.

7 A final comment

As with any new development, lessons are learnt from use. In the reviews of each of the 2001 and 2004 elections, enhancements were recommended [E102] [E105] and agreed by the ACT Government [E103]. What is significant about these enhancements is that none sought to change the basic equity, secrecy, security and transparency features designed into the system.

The 2001 recommendation to improve 'the set-up process to automate the loading of election details, particularly candidate names and sound files' was implemented by establishing the set-up election module which turned eVACS® into a 'closed system', thereby further enhancing security.

References

- [BI05] The Official Blackbox Voting Website <http://www.blackboxvoting.org/>
- [eo05] electionline.org “*Recounts: From Punch Cards to Paper Trails*”, 2005
http://www.electionline.org/Portals/1/Publications/ERIPBrief12_FINAL.pdf
- [EI02] Elections ACT, “*The 2001 ACT Legislative Assembly Electronic Voting and Counting System Review*” ACT Electoral Commission, 2002 at
<http://www.elections.act.gov.au/Elecvote.html>
- [EI03] Government response to the 2001 ACT Legislative Assembly Electronic Voting and Counting System Review <http://www.elections.act.gov.au/EvoteRG.html>
- [EI05] Elections ACT, “*2004 ACT Legislative Assembly Electronic Voting and Counting System Review*” ACT Electoral Commission, 2005 at
<http://www.elections.act.gov.au/Elecvote.html>
- [Gr03] Green, Phillip Chapter on “*Transparency and Elections in Australia: The Role of Scrutineers in the Australian Electoral Process*”, in *Realising Democracy: Electoral Law in Australia*, G. Orr, B. Mercurio and G Williams (eds), The Federation Press, 2003, pages 226-228.
- [Ir04] Ireland Commission on Electronic Voting First Report on *Secrecy, Accuracy and Testing of the Chosen Electronic Voting System*, 2004
http://www.cev.ie/htm/report/first_report/pdf/00Index.pdf
- [Mc01] McGrath, Amy “*The Frauding of Votes*” with an Introduction by Bob Bottom, Tower Books Wholesale, ISBN 0-9587104-3-0, 2004.
- [Me01] Mercuri, Rebecca, *Rebecca Mercuri’s Statement of Electronic Voting*
<http://www.notablessoftware.com/RMstatement.html>, 2001
- [To04] Tokaji, Daniel P: *The Paperless Chase: Electronic Voting and Democratic Values*. Ohio State Public Law Working Paper No. 25, 2004
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=594444
- [Re03] Rezende, Pedro AD: *Electronic Voting Systems - Is Brazil ahead of its time?* Paper prepared for the First Workshop on Voter-Verifiable Election Systems Denver, USA, 2003 <http://www.cic.unb.br/docentes/pedro/trabs/election.htm>
- [Ro04] Rugged Operations Computer <http://www.roc-solid.com/>
- [Wa02] Watt, Bob: *Implementing electronic voting in the UK: The legal issues* Office of UK Deputy Prime Minister <http://www.odpm.gov.uk/index.asp?id=1133606>