



University
of Glasgow

Cockshott, W.P. and Renaud, K. (2009) *HandiVote: simple, anonymous, and auditable electronic voting*. *Journal of information Technology and Politics*, 6 (1). pp. 60-80. ISSN 1933-1681

<http://eprints.gla.ac.uk/5941/>

Deposited on: 4 June 2009

Running head: RENAUD & COCKSHOTT

HandiVote: Simple, Anonymous and Auditable Electronic Voting

Karen Renaud & Paul Cockshott

Department of Computing Science, University of Glasgow

Abstract

We suggest a set of procedures utilising a range of technologies by which a major democratic deficit of modern society can be addressed. The mechanism, whilst it makes limited use of cryptographic techniques in the background, is based around objects and procedures with which voters are currently familiar. We believe that this holds considerable potential for the extension of democratic participation and control.

HandiVote: Simple, Anonymous and Auditable Electronic Voting

Introduction

Moses Finley, in his book *Democracy Ancient and Modern* (Finley, 1985), discusses the strange semantic evolution of the term 'democracy' over the past 250 years. He points out that during the 18th century, to call someone a democrat had the same disreputable connotations as calling somebody a communist does today. Governments and established opinion in Europe were unanimous in their condemnation of democracy and democrats. By the late 20th century there had been a complete turnaround. European governments and political philosophers were now of one voice in the advocacy of democracy.

One factor playing a part in this transformation has been the significant social changes accompanying the establishment of bourgeois or civil society in place of an agrarian aristocratic one. Furthermore, Finley argues that the meaning of the word *democracy* has also changed. Older political philosophers had understood by democracy a system of direct rule by the population at large, but now the term is applied to a system in which the people elected representatives to parliament to make the decisions for them. The 18th century discourse was still directly influenced by Ancient Greek sources, and the understanding people had of democracy came from writers like Plato and Aristotle (Aristotle, 1984) who, when they used the word democracy, were describing a very different sort of constitution from that of contemporary Europe.

In the sense used by Aristotle or Finley, current polities have a very limited degree of democracy. Such control as the people have over public policy is indirect — mainly taking the form of periodic elections of popular representatives to the parliament. This form of indirect representation contrasts with the direct democracy that operated in ancient Greece where the entire citizen body would gather in the town square to debate and vote on issues which affected them (Wilks-Heeg, 2008). The principle was that all major decisions were to be taken by the citizenry as

a collective body. Day to day administration was in the hands of a council drawn by lot from the citizens. This council had, among its duties, the preparation of the agenda for the citizens' assembly.

The ancient states of Greece were little more than we would now call large towns, and techniques that worked for a town became impossible in a modern nation state. A nation cannot physically gather its population into one place to deliberate on policy.

At the time it was introduced, the right to vote for representatives in parliament was a step forward. It was clearly better than having a parliament in which MPs were essentially appointed by the local aristocracy, but, when compared with direct democracy, it has inherent weaknesses.

During the lifetime of a parliament, an MP, let us call her Ms Gray, will vote on perhaps 100 different items of legislation. Even if we suppose that the system that elected Ms Gray was fair, all this means is that a majority of her constituents preferred Ms Gray to her rivals Mr Red, Ms Green, and Mr Black. It does not follow that each time Ms Gray votes in the Parliament, her vote will represent the wishes of a majority of her constituents. That would only occur if the population at large lined up neatly into political parties, with all Labour voters agreeing with every act brought forward by a Labour government, and all Tory voters agreeing with every act of their own government. It is quite possible, therefore, that the parliament will enact laws with which a majority of the population disagree.

On information theoretical grounds we can see the inherent weakness of electing representatives. Suppose elections are held every 4 years and that there are 8 candidates per seat. Each vote cast conveys $\log_2(8)=3$ bits, giving a bandwidth from each constituency to the political decision making process of only 3 bits per year. But if an MP will make 25 yes/no votes per annum, there is thus clearly a huge "impedance mismatch" in the channel.

On very major constitutional issues, national referenda or plebiscites can be held. Their infrequency stems both from their complexity and expense, and also from the reluctance of elected politicians to give up any of their power to the people they are supposed to represent. The advances

made in communications technology these last 50 years are so great that one is drawn to ask whether the benefits made possible by recent advances in technology could not be used to involve a larger percentage of the citizenry in the process.

The use of technology is by no means simple. It needs to be given careful thought and the processes must be evaluated carefully before being imposed onto an unsuspecting public.

Mobile Phones & Their Use

Mobile phones have become a ubiquitous and essential tool for large percentages of the populace. In some countries there are more mobiles than there are residents (Wallace, 2006), and in others people are switching to mobile phones rather than using landline infrastructures (Ling, 2004; Katz & Aakhus, 2008). Mobile phones are changing the way we behave (Srivastava, 2005). For example, one no longer has to organise a meeting as one did before mobile telephony — one simply coordinates with friends on-the-hop: using *micro-coordination*.

Market penetration by the mobile phone has been unprecedented in the history of communication media. For example, in the UK, PC penetration is currently at 76% (Deloitte, 2008) whereas mobile phone penetration is over 100%. As penetration increased, so did the uses. Some examples are payment for parking (Rannu, 2003), travel tickets (Valcourt, Robert, & Beaulieu, 2005), mobile commerce (Barnes, 2002), mobile positioning services (Drane, Macnaughtan, & Scott, 1998). In terms of voting, the entertainment industry has been allowing viewers to vote using their mobile phones for some time (Nightingale & Dwyer, 2006).

It is a natural consequence that governments would start to consider how they could best make use of the opportunities offered new technology. Hermanns (Hermanns, 2008) points out that mobile phones are tools for “political activity, organisation and mobilisation” (p74). The latter was demonstrated in the Spanish elections on 2004, when voters mobilised each other and influenced voter turnout (Suárez, 2006). People have also organised protests by using text messages (BBC, 2000). The topic of interest for this paper is mobile phone enabled voting — so-called

m-democracy. The democratic process offers a number of opportunities for citizens to participate, specifically during plebiscites and elections. There is a real possibility that using mobile phones to allow participation in these processes would ease the process and encourage participation. Brücher enumerates four areas where mobile phone participation is superior to Internet-based voting (Brücher & Baumberger, 2003):

1. *Infrastructure*: mobile phone penetration is much higher than computer penetration.
 2. *Media capability*: people often don't trust transactions carried out over the Web, or do not understand how to use it.
 3. *Inhibition threshold*: people are often inhibited about using computers simply because they don't know where to start, and they would have to do so in a public setting, where they would be embarrassed by their ineptitude. Mobile devices are familiar and easy to use.
 4. *Dependence of location and time*: use of the Internet often dictates use of a computer, whereas use of a mobile phone is not restricted in that way. Even though the latest mobiles allow Web usage, a lot of mobile phone service providers make users pay dearly for this.
- There is therefore a real opportunity to use this ubiquitous technology in a context where it can make a real difference. The following section will consider the UK voting experience.

The UK Experience

In the UK there is a stable and well established system of paper voting and manual counting which has long been used in local and general elections. We shall describe the protocols used in the existing system later. In recent decades, however, the growth of the European Union along with growing disquiet about a possible democratic deficit in the political system has led to voting becoming more complex.

First came the introduction of plebiscites, over the issues of the constitutional status of Northern Ireland (1973, 1998), membership of the then EEC (1975), and over home rule for Scotland (1979, 1997). These introduced the principle that if an issue is sufficiently serious, a

referendum should be held. The doctrine of parliamentary sovereignty means that in the UK referenda are not binding, but in practice it is politically impractical for the government or parliament to ignore a referendum result. This was shown in 1994 when the Strathclyde Region held a referendum on water privatisation. Although privatisation was a matter within the power of central government, and although there was no parliamentary legislation authorising the referendum, the result was so overwhelming (97% opposed to privatisation) that central government abandoned plans to privatise water in Scotland. Referenda have subsequently been discussed by UK Government on the issues of European Monetary Union, the proposed European Constitution, and the Scottish Government has undertaken to hold one on the issue of Scottish Independence.

The results of these constitutional referenda have been to complicate the electoral system, both by introducing additional voting protocols to supplement the *first past the post* system used in Westminster elections, and by creating new tiers of government to which representatives had to be elected. In Scotland, Wales and Northern Ireland, there are now 4 tiers: district, national, kingdom, and union assemblies. In view of the danger that more elections might mean less participation and significant counting costs, there have been various experiments with other methods calculated to raise participation and automate the counting.

Postal ballots, which were long available to members of the armed forces were made available to voters who remained at home on election day, but would prefer not to go to the polling venue. After postal ballots were extended, a number of cases of large-scale vote rigging were discovered. In a court hearing which found six Labour Party councilors responsible for corrupt and illegal practices the judge in the case said:

“In the course of preparing my judgment, my attention was drawn to what I am told is an official Government statement about postal voting which I hope I quote correctly: ‘There are no proposals to change the rules governing election procedures for the next election, including those for postal voting. The systems already in place to

deal with the allegations of electoral fraud are clearly working.”

“Anybody who has sat through the case I have just tried and listened to evidence of electoral fraud that would disgrace a banana republic would find this statement surprising. To assert that ‘the systems already in place to deal with the allegations of electoral fraud are clearly working’ indicates a state not simply of complacency but of denial.”

“The systems to deal with fraud are not working well. They are not working badly. The fact is that there are no systems to deal realistically with fraud and there never have been. Until there are, fraud will continue unabated.”(Richard Mawrey QC, quoted in the Times of April 4, 2005).”

In the Scottish elections of 2007 electronic vote reading machines supplied by DRS performed very poorly. Over 140,000 votes were rejected as unreadable by the machines, amounting to about 7% of the votes cast. Given that the Scottish National Party defeated the incumbent Scottish Labour Party by a margin of only one parliamentary seat, this rate of failure meant there was some doubt about the validity of the final result.

At the same time as all this was happening, the use of telephone voting had become commonplace in reality television programmes. These programmes showed that the technology was able to allow rapid counting of votes cast from home by telephone. But these phone votes, used by commercial organisations without public scrutiny and regulation, have also shown themselves to be wide open to misuse. The question arises: *Could an electronic telephone voting system be made more secure and reliable than the existing systems, whilst retaining the ease of use that attracts television producers to it?* The following section examines the special requirements of e-voting before we present the HandiVote proposal.

E-Voting Requirements

If citizens are to trust the integrity of the democratic process, it is important that all stages — from voter registration to publication of the final result — are not only trustworthy but seen to be trustworthy by the electorate. For example, the registration of voters in the UK is flawed since voters do not have to produce any proof of identity before being entered on the electoral register (Wilks-Heeg, 2008). In the USA the electronic counting process is at best questionable (Green, 2004), as it was in the Scottish election of 2007 (Hadfield, 2007). The most recent example of a flawed publication procedure was the delay introduced by the Zimbabwe electoral commission in publishing the results of the election there (BBC, 2008). The metrics by which the veracity of an election can be judged are listed in the Universal Declaration of Human Rights, and includes vote secrecy, genuine elections, universal and equal suffrage and free voting.

Pieters and Becker (Pieters, 2006) argue for the following principles of elections, which encapsulate these metrics:

1. Correctness of results; only eligible voters vote, they only vote once and all valid votes are counted. (universal and equal suffrage)
2. Verifiability of results (genuine elections)
3. Secrecy of votes (vote secrecy)
4. No link between voter and vote (free voting)
5. A voter should not be able to prove which vote he or she cast (to prevent vote selling)

Any vote must guarantee both the voter anonymity and the integrity of the process (Cetinkaya & Doganaksoy, 2007). A paper based process satisfies these requirements but is expensive and somewhat error prone since it relies on humans counting votes. There has been a move to electronic voting in some countries. Evans and Paul (Evans & Paul, 2004) cite a report by the Caltech/MIT Voting project (Caltech/MIT Voting Technology Project, July 2001) which claims that only 1% of the US population used a paper ballot in 2000.

The paper system used in the UK has three significant loopholes, which can be understood

from the following description of the process. The first problem concerns the accuracy of the electoral register. The electoral registration office for each district council sends an inquiry form to every address. This is addressed to the householder and lists the people currently on the electoral roll for that house. It also contains several blank lines for new names to be added. The householder is supposed to return the form with appropriate corrections, which are then entered on the roll. The roll is then published, and can currently be purchased in digital format.

There is no check on what the householder returns. The head of the family might, for example, omit the names of offspring who have reached voting age, thus depriving them of a vote. On the other hand, the householder might add fictitious residents to the register.

Shortly before the election, the registration office posts a voter's cards to everyone on the voter's roll which lists their name, address and designated polling venue.

On the polling day voters go to the designated polling venue, state their names and optionally display their cards. Showing a card is not mandatory, to allow for people who may have inadvertently lost them. No other form of identity needs be produced. The voters' names are looked up in a copy of the register and ticked off to prevent duplicate voting. A paper ballot slip marked with the candidate names or referendum options, is then torn out from a prepared book of slips. The slip also has on it a perforated ballot number a duplicate of which number is on the stub from which the slip was torn. The electoral officials record the stub number associated with each voter.

Since there is no check against identity, there is no means of preventing impersonation of voters. Suppose a dishonest political party knows that certain voters have either died or left the locality, they can send in party supporters to steal the votes of those wrongly registered.

There is also no guarantee of anonymity, since a record is made of who got which ballot slip. Since the counting process sorts ballots slips into bundles according to the way they voted, it would be a relatively simple matter for the authorities to trace who voted for those they regarded as a threat: communists, fascists, Irish republicans, Islamic fundamentalists?

The voter marks his or her choice on the slip with a pencil in one of the boxes provided, folds it and places it in a ballot box. Counting takes place immediately after the close of polling by means of a manual sorting process in the presence of scrutineers nominated by the political parties.

Unfortunately, whereas people have long experience with paper ballot, and therefore have a measure of trust in them, electronic voting has had some bad press and therefore voters tend to be rather cynical about it. One wants to avoid, at all costs, the secrecy that has bedeviled electronic voting in the USA where it led to suspicion that the voting machine firms, who sympathise with the Republican party, could have rigged the results of elections (Wildermuth, 2007). The trio goals of anonymity, auditability and integrity encompass a number of requirements of e-voting systems.

In 2004 a trial of phone voting was carried out Liverpool and Sheffield. Voters were sent a PIN with their voter registration card. The PIN was used if the persons wished to vote by landline phone or mobile text. Voter turnout was raised from 24% to 36% , which was encouraging.

However, the problems with this scheme are:

1. There is no guarantee of anonymity. The local authority retains a CDROM containing a database which allows matching of voters to votes.

2. The accuracy of the counting software has to be taken on trust.

One of our primary aims is to ensure the anonymity of the vote, whilst providing a means of auditing the process. The Liverpool and Sheffield trial's design appears to have been based on the assumption that one cannot have anonymity and auditability simultaneously. Our scheme, we believe, provides both.

Pieters and Becker (Pieters, 2006) consider the particular characteristics of electronic voting, and propose that candidates be allowed to verify their votes if voting electronically. If candidates are permitted to verify their votes, then principles 4 and 5 mentioned previously cannot be guaranteed. Hence coercion, which is prevented in paper-based voting by the presence of electoral officers at the polls, is more of a problem in electronic voting. Any voting process that includes an electronic component will therefore have to incorporate a number of special techniques

calculated to offset this risk. Furthermore, recent electronic voting fiasco's have eroded public trust to such an extent that one has to include a number of checks and balances to ensure that the public do trust the outcomes of these elections (Oostveen & Besselaar, 2004). Hence, the following principles of electronic voting have been assembled from the publications of a number of researchers. The first five accord with Pieters and Becker's principles, but the list has been augmented to take account of the special requirements of electronic voting.

The *correctness* of the voting process is important (Cranor, 1996). We have to satisfy traditional transactional requirements (Bradley, Gilmore, & Thomas, 2006) including: atomicity (Bannet, Price, Rudys, Singer, & Wallach, 2004; Liaw, 2004) — one person, one vote; integrity (Gibson, 2006; Ibrahim, Kamat, Salleh, & Aziz, 2003) — the person's vote must be recorded correctly and the votes must be counted correctly; durability — votes should not be discarded; and non-interference (Bannet et al., 2004) — it should not be possible for votes to be altered en-route to the vote storage system, or once recorded by the system.

It should be possible for voters to *verify* that their vote has been recorded and counted correctly (Caltech/MIT Voting Technology Project, July 2001; Pieters, 2006; Ibrahim et al., 2003; Storer, Little, & Duncan, 2006) This should be engendered by a transparent and open process which encourages voters to trust the system. This is the point at which many US elections have faltered (Dill, Schneier, & Simons, 2003). Voters cannot check, once they have voted, whether their vote has been recorded properly. A truly verifiable electronic voting system *must* allow voters to verify that their vote was recorded correctly (Liaw, 2004; Kohno, Stubblefield, & Rubin, 2004).

Voters should be able to record their vote without other voters or officials being able to observe them (Bradley et al., 2006; Ibrahim et al., 2003; Storer & Duncan, 2004), ensuring *secrecy*.

Voters should not be linked to their vote in case this could be used against them at a later stage (Klonowski, Kutylowski, Lauks, & Zagórski, 2005), ensuring *anonymity*. Assurances from those in power may well not be sufficient to reassure voters; the system must be demonstrably and verifiably anonymous;

A voter who is eligible to vote should be able to vote (Juang & Lei, 1997) thus ensuring *free and fair voting*.

The process should be *resistant to coercion* (Caltech/MIT Voting Technology Project, July 2001; Storer & Duncan, 2005; Liaw, 2004);

Resistance to cheating needs to be addressed. It should be possible for all voters to satisfy themselves that the government has not cheated and that the outcome is indeed the will of the people (Lin, Hwang, & Chang, 2003);

It is important to lower barriers to participation. There should be multiple ways for the voter to cast his or her vote, by means of various devices, so that both house-bound voters and traveling voters are accommodated, for example (Gibson, 2006; Liaw, 2004).

Review of Related Work

There have been a number of efforts to automate various parts of the voting process, which is unsurprising as the number of issues on which votes are being held has increased. The basic stages involved in voting are: registration, allowing voters to place their vote, counting the votes and publishing the result. Registration can only be automated if a measure of inaccuracy is tolerated in the eventual voters roll. If this is not acceptable then a human being *has* to scrutinise the person's identity document and verify the veracity thereof as well as the person's right to vote in the country's elections and plebiscites. Some proposals automate only the counting process, (Ryan, 2004; Hadfield, 2007), maintaining a paper-based vote placing process. Very few proposals facilitate post-election verification of votes recorded and only ours, as far as we know, automates this process.

Estonia introduced web voting in 2003 (Maaten, 2004). Voters use id cards containing a chip to identify themselves. The voter inserts the card into a card reader and software on the computer then enables him or her to vote via a web-page. In the process their choice is encrypted and digitally signed before being sent to a server maintained by the national electoral commission.

On arrival, the vote is split into digital signature (identifying the voter) and the vote itself. A list of who has voted is formed and a separate list of votes for each candidate is compiled to be sent to counting software.

This system has a number of points of vulnerability that we avoid in our proposal:

1. There is a restriction imposed by the limited number of computers with attached card readers; this further accentuates the Digital Divide over and above the restriction imposed by using computers in the first place.

2. There is no guarantee that the software that is running on the user's voting computer has not been compromised by a Trojan horse or other spyware which could result in:

1. loss of privacy or

2. in more extreme cases, the malware may send and sign a different vote from the one which the voter intends to send.

3. The server run by the national electoral commission is a central weak point. It is subject to possible insider attacks:

1. an insider, working on the software, may send by a covert channel, details of who voted in which way to the security services or one of the political parties.

2. Since there is no independent verification available to the voter that their vote has been correctly recorded, an insider may introduce subtle bugs in the software of the decryption routines that cause a certain percentage of votes for one of the political parties to be decrypted as votes for one of the other parties.

3. There is no guarantee that an insider attack does not result in the introduction of fraudulent (digital signature, vote) pairs being inserted into the system by an insider with access to the database against which voters digital signatures are checked.

4. Some privacy is supposed to be provided by the splitting of lists of voters and lists of votes into distinct files which are sent to different systems. If, however, an agency, state or private, were to come into possession of both files, they could correlate voters with votes cast.

(Drechsler, 2004), discussing the Estonian e-voting system, makes the criticisms that it is likely to skew results because of the Digital Gap between those with and without internet access. He also argues that the virtual communities created by the internet cause people to become deracinated and disconnected from politics in the real national community in which they live. Our proposal for phone voting avoids, we feel, these criticisms. The digital gap is much smaller than the phone gap; social coverage by the telephone network is much wider than computer networks. It is not universal; not everyone has a telephone, but our suggestion backs up access via private telephones with free access to the voting system by public telephones and voting booths. The second main electronic apparatus that we propose to use is television which, again, has a very wide diffusion. We suggest that electoral programs involving broadcast debates with studio audience participation be followed with details of how to vote by phone on the issue being debated.

It is arguable that the relationship between television and the national community is quite different from that of the Internet. The common viewing of a particular programme, for example the US presidential debates, by a large fraction of the population has a centripetal effect, quite distinct from fragmented participation in Internet fora. In the UK it was until recently the practice for party election broadcasts to go out on all TV channels. A similar provision could be made for the key debates which culminate in a national vote.

Similar objections to the Estonian case appear to hold for the system used in Geneva. Braun (Braun, 2004) describes how, in Geneva in 2003, a system with some similarities to our own was used. But, in this case secure voting was achieved by means of the use of a scratch-off PIN on the voter's cards which are routinely issued by the Canton. Voters have to enter their date of birth and commune of origin to confirm their identity when voting. Thus, in principle, a record is kept associating the vote with the voter identity, even though Braun reports that these can not be matched because they are 'kept in two distinct files'. Whilst in the Swiss context, where there is high trust in the electoral authorities, this may be perfectly adequate, we are not convinced that this would be satisfactory in other contexts. The fact that these two files exist is not a very strong

precaution to ensure anonymity. One would have to show that:

1. no algorithmic procedure existed which, given the two files, could reliably match voters to their votes.

2. that even if the software running on the voting servers was compromised by an insider inserting spyware, it would still be impossible to match voters with their votes.

Most other proposals for electronic voting are concerned with elections rather than plebiscites. An exception is the system trialled in Geneva, which was indeed used in a plebiscite (Braun, 2004). An important factor is that in a system of participatory democracy, voting will be more frequent and must therefore be more accessible. Our proposal has something in common with the proposals of Storer and Duncan (Storer & Duncan, 2004, 2005). Like their system, it allows voting by telephone. We consider this to be an important factor because mobile phones are available to a larger portion of the population than computers, especially in poorer countries. We thus rule out of consideration any procedure that requires voters to have access to personal programmable computing devices. It has to be possible to use simple telephony.

The differences between the systems are that whereas Storer and Duncan's system also involves the use of personal voting cards with unique numbers on them, their system has three numbers: the voter ID number, the Personal Candidate ID Number used to vote for a candidate, and a Receipt ID, which is sent back to confirm the vote. In Storer and Duncan's system the voter verifies by matching the candidate name and RCID tuple on the list, which is somewhat demanding. Finally, they do not guarantee voter anonymity.

In Storer and Duncan's system, the State posts cards to voters and thus can match the voter to the voter card numbers. They propose a complicated system of subdivision of agencies issuing the numbers to protect anonymity, but the voter still has to take it on trust that these State Agencies are not colluding. Their system is not secure against the insertion of fraudulent votes in the event of collusion between the various State agencies administering it. Because we have completely anonymous voter card numbers, we can allow a fully public audit of the voting results that would

detect any such fraud.

Ryan and Schneider (Ryan & Schneider, 2006; Ryan, 2004) propose Prêt á Voter. The voter is issued with a voting form which is perforated in the middle to allow the voter to remove the names to maintain secrecy of the vote. The voter takes the paper to an official manning a scanner so that the vote can be entered into the system. The voter receives a “receipt” with a serial number printed on it. This number can be entered into a kiosk to check that the vote has been recorded correctly. Their system preserves voter secrecy, verifiability of vote and ensures no direct link between voter and vote. There are some problems with it, however. The first is that the scanners need to be manned since they sometimes fail to scan the result correctly. The people manning these scanners can see how people have voted if they fail to remove the one half of the sheet before presenting it to be scanned. This erodes vote secrecy. If the voter retains the receipt and another person obtains it from them, they can prove which way they voted, so that votes could be sold hence the system delivers low resistance to cheating.

The most serious objection, however, is that there appears to be no pressing reason why a more complex paper based system with electronic counting should replace the existing manually counted paper based system except that counting is simplified. The electronic nature of the process, while undoubtedly making counting fast and easy, has some disadvantages which appear to outweigh the advantages. Since the Prêt á Voter system only allows voting at the polls, no attempt is made to lower barriers or facilitate voter mobility. At the same time it faces the hazards and unreliability of OCR machines which became all too evident in the recent Scottish election.

Cetinkaya and Doganoskoy (Cetinkaya & Doganaksoy, 2007) propose an e-voting scheme that, at the most abstract level, is analogous to ours. The big idea in our approach is that votes use an untraceable voter ID, rather than any document which can be tied to them, when they vote. This voter ID can then be used in a public listing of votes which the voter can inspect. The same idea has occurred to Cetinkaya and Doganoskoy, and they term these voter IDs ‘pseudo identifiers’. Whilst our proposal and theirs is similar at an abstract level, in concrete details they differ substantially.

They use a complex electronic communication protocol involving blind signing (Caltech/MIT Voting Technology Project, July 2001) in order to distribute the pseudo identities. We use the low-tech, but reliable, approach of people putting their hand into a shaken jar to draw out an identity.

In consequence of the complex communications protocols being used, their approach demands that voting be done using computers connected to the Internet. Our approach allows lower cost and less sophisticated terminals such as mobile phones or even old fashioned land line telephones.

We believe that it is a mistake to create voting systems whose security systems are so sophisticated that only people with a training in cryptography can understand them. Ordinary citizens will use the voting system, so the way it works should be easily understood by ordinary citizens or they will not be convinced of its integrity.

It is also a mistake to require something as expensive as a computer for the voting terminal. For example in (Liaw, 2004) the voters are all required to have secure tamper resistant smart card readers attached to computers, which is even more restrictive. Telephones, particularly mobile phones, are much cheaper and more widely disseminated than computers. As soon as you assume that the voting is to be done using a computer, the voter has to put his or her trust in the software that runs on the computer. How does he or she know that, behind the scenes, the software on the computer is not sending messages to the secret police telling them how she or he voted. An expert may tell her that that basic protocol being used is secure, but how can she or he tell that the computer is not using some other channel to send details of his or her real identity to the authorities? This is a real problem now that public trust in experts is waning (Pfadenhauer, 2006).

We believe that Occam's razor should be applied to the problem. No more complexity or technology should be used than is strictly necessary.

Handivote

Every voting process has a list of guiding principles, which act as a strategy document dictating and constraining the design. HandiVote's principles include:

1. Voters shall choose a random voter card when they present their identification to the electoral office and this identification matches the name on the voters roll. This ensures that only eligible voters vote and that they can vote anonymously.
2. Voters may place their vote using a variety of devices including mobile phones, landline phones, public phones and the polling booths. This lowers barriers to participation and facilitates mobility of voters.
3. A re-vote on a particular voter card number will void the previous vote if it is different from the original vote. This discourages voter card theft and offers some level of protection against coercion.
4. Lists of voter cards together with votes cast are made publicly available once the election period has concluded. This provides the transparency often lacking in current e-voting processes. It is also possible for any voter to check the accuracy of the count. It also ensures that no person or group will know the intermediate outcome and have time to mount a massive coercion-based attack to swing the outcome of the plebiscite. Lauer argues that having a voter verified audit trail is the only effective countermeasure against cheating (Lauer, 2005).
5. Finally, our system is characterised by the simplicity of the voting process. Voters either enter use the voter card in the polling booth or contact the voting line by phone, provide their card number and PIN, and choose an option. There are no complicated extra steps involved as is the case for other e-voting schemes.

Processes

The processes we propose incorporates a number of checks and balances to ensure that votes are counted correctly and that the entire process is as transparent as possible. Due care is required

in the various stages of the process.

The voting process will be initiated by the election commission, who will issue a set of consecutive valid voter card numbers. A facsimile card is shown in Figure 1. The voter card has printed on it two voter-related numbers, a voter ID number and a PIN. On the back of the card is the list of toll-free numbers which can be used to register a vote.

Each manufacturer will be given the beginning and ending card numbers for the cards to be produced at their factory..

Once the list of card numbers has been received, they will be manufactured. A random PIN will be generated and printed on the card and the card will then be securely sealed within an tamper-resistant envelope in a mechanical fashion and not by a human agent.

The pairing of the voter card number and the associated PIN will be encrypted using the electoral commission's public key and electronically transmitted to the central system controlling the plebiscites.

The cards, in their individual envelopes, will be packed into secure dye-protected containers before they leave the factory. The cards are delivered, by using secure transport, to the local election registration offices. The head official will open the container using the correct physical key and will verify that the number of cards recorded on the docket are contained within the container. Only once this tally has been checked and double checked, will the receipt be signed and stamped with the local election authority's seal. This receipt may be used by the manufacturer to obtain payment. Any discrepancy between the number of cards on the docket and the number of cards delivered will lead to immediate invalidation of all cards in that number range and a full investigation will result, with the manufacturer's contract being reviewed and possibly lost.

Voters register, in person, presenting a recognised form of identification to the registration officers. A record of their registration is taken to ensure that they do not register multiple times.

They then choose one of the sealed envelopes containing voter cards from a jar. Note that only the voter him or herself will know which voter ID number is associated to him or her.

At registration the voter may also use a device, made available by the electoral authorities, to specify that their vote is only to be allowed from the polls. This option allows the voter to pre-empt and thereby prevent any coercion attempts he or she might anticipate.

In order to encourage participation, the registration period will end a short period, perhaps a number of days before the plebiscite or election is due to be held.

Current registration in the UK does not require voters to present themselves to the election authorities in order to register and the current voters roll is therefore suspect. There is a danger, therefore, that the HandiVote proposal will decrease participation due to the extra effort required in order to register. Active registration, however, is used in many other countries, and offers some guarantee as to the validity of the voters roll. This new requirement may impact disproportionately on low-income or marginalised groups. To offset this, we recommend that election registration kiosks be made available at libraries, job centres and even in supermarkets in the period immediately preceding an election or plebiscite.

It is possible, however, to benefit from psychological studies into voting to make this registration process play a positive role in raising uptake during elections and plebiscites. Greenwald et al. (Greenwald, Carnot, Beach, & Young, 1987) found that if voters were asked to predict whether they would vote or not before an election, and they said they would, then they were more likely to vote than if they had not been asked. It appeared that by asking people whether they will perform a socially desirable action makes them more likely to take the trouble to perform the action later. The registration office could make use of this finding by displaying posters which ask “Will you vote on election day?” in order to prime the voters to vote on the day in question.

Finally, this registration period would serve very effectively to weed out fictitious people on the electors roll, something that is currently a cause for concern.

When registration is closed, the local election authorities each return a list of unused and used cards to the election commission. These are then recorded in the HandiVote Validation system and also published via the Web. The purpose of publishing this is to ensure that this list can be

compared to the final list of votes cast. This will make it possible to uncover any attempt to pad the final vote list with invalid voter card numbers.

When the voting period commences, the voter can use this card to place a vote. The vote can be placed either at the polls, or via a number of electronic channels, as shown in Figure 2. In all cases the voter card number and the PIN have to be used to tag the vote. Only correct combinations of card number and PIN will be registered as valid votes. Note that since only the voter him or herself knows which card number is on the card, the voting process remains anonymous.

Votes are counted electronically and the final result published. After the voting period has concluded, the voter is able to verify that his or her vote has been recorded correctly. Because the entire list of voter card numbers is published (on the web and in the press) this allows voters to check that their vote was correctly registered and anyone with access to the published list of votes can verify that the count was correctly performed.

Once the election is over, an audit process will verify that the votes have indeed been counted correctly. It should be possible to identify any insider interference at this stage and to narrow down the culprit in the case of fraudulent activity being uncovered. The HandiVote voting process is illustrated in Figure 3.

HandiVote Infrastructure

Two major software systems are required by HandiVote. The first is the Validation centre. This system holds the list of valid card numbers. It can be queried by submitting a card number, and will respond yes for a valid card number, and no for an invalid one. Interaction with this software system is depicted in Figure 3.

The other system records the votes and performs the counting process once the plebiscite is over. Specialised interfaces are provided for each of the input devices. The connection to each of these will occur via recognised channels and based on the requirements of the input device. These systems will communicate with the voter registration system. There will also be two specialised

output handling systems to send the lists of voter numbers and choices to a website and TV channel. Finally, this system will update a counter displayed on a special monitor every time a vote is placed. A camera will send this to a television station so that the voting process can be monitored by all citizens throughout the voting period.

Threats

This section discusses some threats to the process that need to be considered. During the preparation of the cards, someone working at the manufacturing site may well record the numbers of some of the cards. This is complicated by the use of tamper-resistant envelopes but is not impossible to do. If the card is issued to a voter and the insider has abused his knowledge to “steal” the person’s vote, the legitimate card holder will detect this as soon as he tries to vote and he will be able to contact the help number to void the vote already cast. The different voiding options we could use to deal with this eventuality will be considered in the following section.

At registration, one of the election officers could theoretically steal a card, but this is easily detected by requiring a copy of the voter’s identification document to be made for each card issued. On the other hand, someone could attempt to register by using a fake identity document. This threat is common to all voting mechanisms and cannot be alleviated by our proposal.

During voting someone, either a person, group or foreign power, could write code to flood the system with voter card numbers and guessed PINs to register false votes. This will not work unless they can guess the matching PIN and the chances of this happening are 1 in 10000 for a 4 digit PIN. Any repeated incorrect PIN entries will be logged in order to alert the system administrator to possible attempts to register illegal votes. Each incorrect entry of a PIN would cause the registering computer to impose a delay before it would accept another attempt. The timeout delay should double after each attempt. This should be sufficient to prevent automatic challenge systems being able to guess the PIN within the voting period.

It is possible to use computers connected to the telephone system to send SMS. The

bandwidth of sending these messages from a computer would be far higher than could be obtained by hand messaging. Let us look at a worse case scenario. Suppose that the initial timeout after a failed voting attempt is one minute. Suppose further that there are 1 million electors and that a computer systematically tries all 1 million possible voter numbers, and sends in a fraudulent voting attempt on each one starting with a guessed PIN of 0000. On grounds of probability we can expect that 100 voters would actually have a PIN of 0000, so the fraudster has bought 100 votes for the cost of 1 million SMS messages. The cost of sending these SMS's would be of the order of £100,000. The cost of automatically buying a vote will be £1,000 per vote, which is not negligible. One minute later the computer can make a second pass through all the voter numbers. Since the hacking system does not know which 100 PINs it guessed correctly, it will now re-attempt to vote the correct PINs with an incorrect PIN. Repeated such attempts will be noted and reported to election authorities. Now consider how many passes through the voters list the hacker can make. If the voting day is 12 hours = 720 minutes, we have the following series:

First attempt		
Second attempt	1 minute later	elapsed time 1 minute
Third attempt	2 minutes later	elapsed time 3 minutes
Fourth attempt	4 minutes later	elapsed time 7 minutes
...		
Ninth attempt	256 minutes later	elapsed time 511 minutes
Tenth attempt	512 minutes later	elapsed time 1023 minutes too late voting has closed

This would be sufficient to prevent more than 900 votes being fraudulently gained, but the effect of the delays would amount to a Denial of Service (DoS) attack. This is because the delays would also impact on legitimate voters, delaying their votes by a considerable amount of time and potentially preventing them from exercising their democratic rights.

Such attacks could be partially offset by allowing votes at the polling stations to have a privileged status and therefore not being subject to imposed delays. In reality the worst case

scenario is that everyone would have to repair to the polling places to vote if such a widespread attack occurred.

It would be costly and risky for individuals within the country holding the vote to mount DoS attacks but if the source could be a server plugged into the SMS core infrastructure then a DoS attack could be launched by this device and source addresses spoofed. This kind of attack could conceivably be mounted by a hostile foreign intelligence service. But such attacks on key political institutions fall so close to warfare as not to be a compelling reason not to adopt electronic voting. Today, many other government digital services could potentially be disrupted by hostile powers, but this in and of itself is not a compelling reason why digital services should not be used.

It is possible for someone to coerce the voter and to vote on his behalf. We have built two safeguards into the system to alleviate this. The voter can, at registration, request that the vote only be accepted from a polling booth where he or she can be protected from coercive activities.

A voter card may be stolen and used by the thief to place a vote he or she is not entitled to. Since the card is not linked to the voter there is no way for the system to void such votes.

A voter could be paid to vote in a particular way. The undeniable fact is that anonymity and verifiability make uneasy partners. In order to provide a system that engenders trust by allowing users to verify that their votes have indeed been recorded correctly, we make it possible for voters to prove how they have voted. We believe that this is preferable to voters not trusting the system.

During the verification period someone could hack into the website that is used to publish the results and insert fictitious numbers into the files. This could be alleviated by updating this list at regular intervals from the vote recording site and by ensuring that all communication with the site is encrypted.

It might be possible for a rogue computer operator to insert a vote into the software system using a legitimate voter card number. An opportune time to do this might be in the last 5 minutes before polling closed. If software could determine that particular voter numbers had not been used, these could be added to the voter tally with a high probability that it would not be detected by the

legitimate voter. We propose two simple mechanisms to uncover this kind of fraud.

1. The published list of votes cast at the conclusion of voting will show when each vote was cast, as well as the channel which was used to cast the vote.

2. An LED display of a running counter is continuously and publicly displayed throughout the voting period. Figure 4 demonstrates the proposed setup of the tally display. If such a rogue operator were to insert a large number of votes *via the legitimate HandiVote software* in the last few minutes, the counter would reflect this and spin in a suspicious fashion. On the other hand, if he/she inserted the votes directly into the database holding details of votes case, there would be a discrepancy between the displayed totals and the recorded votes, which once again would uncover the fraud and trigger an investigation.

The fact that both the tally and the final list with times are publicly available, means that independent agencies can satisfy themselves that such fraud has not occurred.

This is alleviated by displaying . When voting concludes, the software system immediately prints out a list of voter card numbers in the system.

The final tally will be widely published. This means that any later attempts to insert fraudulent votes can be detected because the tally will no longer be correct. Fraudulent voter numbers are easily detected from the printed list.

After voting has concluded, somebody could fraudulently add voter card numbers and PINs to the list which corresponded either to cards which were never handed out, or to cards which never existed. With the use of these numbers they could then make fraudulent votes. To guard against fraudulent insiders of the latter type we have proposed that valid voter card numbers are issued by the electoral commission and therefore it will be futile to insert card numbers outside this range. The attempt would easily be detected. The insertion of cards which were not handed out is also easily dealt with since details of those card numbers are published at the end of the registration period and therefore such deception is easily uncovered.

The vote counting computers should be run by an organisation distinct from the Validation

Centre. When votes occur, voter numbers that have been phoned in are checked, over a secure channel, with the Validation Centre, after having first been checked against the published list of unused voter cards. The Validation Centre returns a yes/no for each query.

At the end of the registration period, the original list of cards is compared to the list of votes cast by voter card numbers. It is possible for any private organisation with modest computing facilities to check if any of the published votes cast in the period were by cards that had not been validly issued. In the case of a discrepancy the suspicion would fall on a small group of known individuals. The near certainty of malfeasance detection should be an incentive adequate to ensure honesty in this group.

Any significant numbers of complaints must be considered worthy of a large-scale investigation, in order to identify and punish the miscreants.

One procedural matter that requires special mention is that of a vote being cast using a valid voter card number for which a vote has already been recorded, in other words when a person detects prior fraud on their card, or where they realise that they have pressed the wrong button. The following section will discuss some options to deal with this eventuality.

Voiding Options

If a vote is placed for a card which has already been used to record a vote, there are several courses of action that could be followed.

- Void the card number altogether and issue the voter with a new card, using the same anonymous drawing process as initially used to issue cards. This partially compromises anonymity, if the voter is recognised by the officials when handing in their old card.
- Simply void the vote and allow the voter to place his vote. This again has the disadvantage of potentially violating the anonymity of the card-holder, but it does allow people to correct mistakes made if they inadvertently voted the wrong way.
- Detect contradictory votes in software and automatically void them, but do not allow

voters to re-vote. Anonymity is protected. This would not allow voters to fully correct mistakes. They could convert a yes vote to an abstention but not convert it to a no vote and vice versa. This reduces, but does not totally eliminate, the gain made by a fraudster. Lists of contradictory, and hence voided votes, should in this case be published, to allow detection of fraud. One would expect a certain number of contradictory votes to be cast by people who had changed their minds or made a mistake. The difficulty would be to distinguish between genuine mistakes like this and real fraud.

- accept this limitation imposed by the anonymity requirement, and write it off as a negligible risk. It should be born in mind that the numbers of votes that can be fraudulently inserted into the system from the outside is very low – since guessing pins or stealing them is not practical on a large scale.

Note that in either of the voiding options the theft of significant numbers of voter numbers by the manufacturer of the cards would be detected by an unusually large number of complaints about duplicate votes having been cast. The certainty that there would be a resulting police investigation should be sufficient deterrent against this sort of crime. The situation here is analogous to that of secure printing firms who produce banknotes, passports etc. The commercial survival of such firms depends on the maintenance of integrity.

Simulation

We carried out a simulation of the proposed process. The procedures proposed above were followed as closely as possible but where budgetary constraints made the use of particular channels impossible we substituted a Web page for that channel. The stages were carried out as follows:

Preparation : Voter cards were printed. We used a plain cardboard card with the voter number, PIN and expiry date printed on the one side, and voting instructions printed on the other, as shown in Figure 5.

Registration : Participants registered during a lecture. They brought their student identification cards with them. The electoral officer took a photograph of the student's card and they were

requested to take a sealed envelope from a jar. At the end of the voting period the sealed envelopes were opened and the unused card numbers submitted to the system so that they could not be used to place votes.

Voting : The voters had a 24 hour period to record their votes. They could use web pages which simulated the following channels (Screen shots of phone types shown in Figure 6):

- Public Telephone Kiosks
- SMS
- ATM Machine¹

Verification : Voters were given a link to a web page where a list of votes cast — either for or against — was provided as shown in Figure 7. Voters could verify their votes. The web page also provided a tally of votes for and against the plebiscite issue.

Participants completed a questionnaire when the plebiscite was over. They were generally positive about the anonymity, privacy & confidentiality, verifiability and lowering of barriers aspects. They did not feel that the system provided coercion resistance, which is true, since in HandiVote coercion resistance is provided by having voting booths centrally available where people could place their votes if they felt they might be or had been coerced at home or at work. The participants overwhelmingly preferred the ATM interface, feeling that the SMS-based interface was overly complicated to use. This was rather surprising since the participants were final year Computing Science students. We will therefore have to consider a question-response protocol for the SMS-based voting, which might work as follows:

- Voter sends voting card number by SMS to polling software.
- An SMS is returned which requests the PIN.
- The voter returns the PIN.
- An SMS is returned asking for the vote.
- The voter returns a yes or no vote.

This protocol requires the voter to use an identifiable mobile number, and this could mean that anonymity is lost. It is not current practice in the UK for the phone companies to record the content of text messages, but this might change. The problem could be offset if a special mobile phone SIM chip was included in the envelope with the voter card and placed within a mobile phone to permit SMS messages and calls to be sent only to the voting number.

The simulation process was valuable in that it highlighted some areas where the process could be improved:

- The protocol of voiding a vote whenever a duplicate vote is placed acts as a defence against someone stealing a voter card after a vote has been placed but does not really defend against votes placed as a result of coercion. To defend against that, we confirmed the need to allow voters to vote at the polls, and thereby cast a privileged vote, the final, definitive vote from that voter. If someone is coerced to vote via another channel, he or she can then override that vote by visiting the polling booths where coercion cannot occur.

- SMS voting was marred by difficulties with the ordering of the number, PIN and vote in the message. This could theoretically be simplified by making the PIN the last 4 digits of the voter card number so that voters simply enter one long number instead of two in a particular order. In the UK that would require a 12 digit voter card number, which is 4 digits shorter than a credit card number, which e-shoppers seem to be able to enter into websites with ease. Unfortunately card numbers are public and the PIN is required in order to ensure that the card holder, and only the card holder, can vote using that card number.

- One problem was confirmed: that of vote selling. Voters can sell their vote and the published lists allow them to prove that they voted as requested. Unfortunately a system that provides verifiability will always suffer from this flaw. Anonymity and verifiability appear to be mutually exclusive properties.

Handivote Critique

The Rowntree Reform Trust's report *Purity of Elections in the UK: Causes for Concern* (Wilks-Heeg, 2008) stated that: "e-voting pilots have proved extremely expensive and there is no evidence to suggest that e-voting offers any significant scope for turnout to be increased by this means. At the same time, serious concerns persist about the security and transparency of e-voting systems and their vulnerability to organised fraud"

Concerns were particularly raised about e-counting: "Not only has e-counting frequently failed to improve on the estimated time required for a manual count, it has also highlighted the lack of transparency in such a system". Furthermore, they point out that there were 42 convictions for electoral fraud between 2000 and 2007. Moreover, every English police force except the City of London has investigated electoral malpractice allegations since the year 2000. Finally, there were concerns about the credibility of the voters roll, with many voters not being registered and postal voting has been shown to be open to wide-spread abuse.

Does our proposal offer a viable alternative to existing systems? We believe that it does. Let us consider each problem highlighted by this report in turn.

Increasing turnout was identified as important in countries where voting is not compulsory. Handivote offers voters an opportunity to vote from their phone, mobile phone or public phone, we lower the bar. It makes voting as convenient as placing a phone call, and removes the need for voters to visit polling stations.

It is also important for the process to be as transparent as possible. The verification phase allows voters to verify that their vote was recorded correctly, from the comfort of their own homes — either on the TV or via the Web.

In terms of expense, our scheme requires simple voters' cards to be produced. Since the card does not have an embedded chip the cost should not be excessive. The voter can place a free calls to the voting line in order to register a vote.

Coercion is a risk that goes hand in hand with electronic voting. If a voter is coerced to

place a vote which was not intended, he or she can simply visit the polling stations and vote there. This vote replaces the earlier vote and therefore the system offers some measure of resistance to coercion.

Vulnerability to organised fraud is a concern. Our system is able to provide some resistance by using a combination of an increasing delay and the privileged status of the polling booth vote.

Problems in the Scottish elections of 2007 occurred because votes were recorded manually and then scanned into a system to be electronically counted. This was bound to be a problem since people became confused and recorded their votes incorrectly. Furthermore, handwriting variety led to the software being unable to recognise numerals. HandiVote uses familiar technology and existing tried and tested infrastructures and does not rely on an error-prone technology such as handwriting recognition.

Conclusion

Our aim has been to suggest a technology and set of procedures by which a major democratic deficit of modern society (Wolin, 1994; Frey, 2005) can be addressed. E-voting is in the news regularly, and many articles claim that anonymity and auditability cannot co-exist (Press Association News, 2007).

In this paper we suggest a mechanism which, whilst it makes limited use of cryptographic techniques in the background, is based around objects and procedures with which voters are currently familiar and which does provide an environment for happy co-existence of anonymity and auditability.

We believe that systems like this hold considerable potential for the extension of democratic participation and control.

We have reported on a simulation of the proposal for electronic plebiscites. The simulation was successful since it showed that the procedure was viable. We did make some changes where it became clear that the procedure needed to be fine-tuned and we now have a tried and tested

procedure which could be used on a larger scale to improve participation, lower boundaries, engender trust in the electoral process and prove a valuable tool in the hands of electoral officials.

References

- Aristotle. (1984). *The Athenian Constitution*. Penguin.
- Bannet, J., Price, D. W., Rudys, A., Singer, J., & Wallach, D. S. (2004). Hack-a-vote: Security issues with electronic voting systems. *IEEE Security & Privacy*, 2(1), 32–37.
- Barnes, S. J. (2002). The mobile commerce value chain: analysis and future developments. *International Journal of Information Management*, 22(2), 91-108.
- BBC. (2000, Sept). *The blockade that grew*. BBC Website.
(<http://news.bbc.co.uk/1/hi/uk/919852.stm>)
- BBC. (2008, 30 March). *BBC Monitors warn on Zimbabwe delay*. (BBC Website)
- Bradley, J. T., Gilmore, A. T., & Thomas, N. (2006). What proof do we prefer? Variants of verifiability in voting. In *Workshop on e-voting and e-government in the uk* (p. 58-65). Edinburgh.
- Braun, N. (2004). E-voting: Switzerland's projects and their legal framework. In A. Prosser & R. Krimmer (Eds.), *Electronic voting in europe- technology, law, politics and society, gesellschaft fur informatik* (p. 43-52). Bregenz, Austria.
- Brücher, H., & Baumberger, P. (2003). Using Mobile Technology to Support eDemocracy. *Hawaii International Conference on System Sciences*, 5, 144b.
- Caltech/MIT Voting Technology Project. (July 2001). *Voting - what is, what could be* (Tech. Rep.). Caltech/MIT Voting Technology Project.

- Cetinkaya, O., & Doganaksoy, A. (2007). Pseudo-voter identity (PVID) scheme for e-voting protocols. In *Ares 07*. IEEE Press.
- Cranor, L.-F. (1996). Electronic voting: computerized polls may save money, protect privacy. *Crossroads*, 2(4), 12-16.
- Deloitte. (2008, July). *Personal computer - the Digital index*.
(<http://www.deloitte.com/dtt/article/0,1002,cid%253D205161,00.html>)
- Dill, D. L., Schneier, B., & Simons, B. (2003). Voting and technology: Who gets your vote? *CACM*, 46(8), 29-31.
- Drane, C., Macnaughtan, M., & Scott, C. (1998). Positioning GSM telephones. *Communications Magazine, IEEE*, 36(4), 46-54, 59.
- Drechsler, W. (2004). The estonian e-voting laws discourse: Paradigmatic benchmarking for central and eastern europe. *NISPAcee Occasional Papers in Public Administration and Public Policy*, 5(2), 11-17.
- Evans, D., & Paul, N. (2004). Election security: Perception and reality. *IEEE Security & Privacy*, 2(1), 24-31.
- Finley, M. I. (1985). *Democracy ancient and modern*. Rutgers University Press.
- Frey, B. S. (2005, April). *Direct democracy for a living constitution*. (Walter Eucken Institut, Freiburg Discussion papers on Constitutional Economics , 04/5.)
- Gibson, R. K. (2006). Internet elections: The voters viagra? In *Workshop on e-voting and e-government in the uk*. Edinburgh.
- Green, T. C. (2004, 10 May). *E-voting promises UK election tragicomedy*. (The Register)
- Greenwald, A. G., Carnot, C. G., Beach, R., & Young, B. (1987). Increasing voting behavior by asking people if they expect to vote. *Journal of Applied Psychology*, 72(2), 315-318.

- Hadfield, W. (2007, 2 May). *Scottish election results delayed by e-voting problems*. (Computer Weekly)
- Hermanns, H. (2008). Mobile democracy: Mobile phones as democratic tools. *Politics*, 28(2), 74-82.
- Ibrahim, S., Kamat, M., Salleh, M., & Aziz, S. R. A. (2003). Secure e-voting with blind signature. In *4th national conference on telecommunication technology proceedings*. Shah Alam, Malaysia.
- Juang, W. S., & Lei, C. L. (1997). A secure and practical electronic voting scheme for real world environments. *IEICE Trans Fundam*, E80-A(1), 64-71.
- Katz, J. E., & Aakhus, M. (2008). *Perpetual contact*. Cambridge University Press.
- Klonowski, M., Kutylowski, M., Lauks, A., & Zagórski, F. (2005). A practical voting scheme with receipts. In *International conference on information security and cryptology*. Incs 3935 (p. 490497). Seoul, Korea.
- Kohno, T., Stubblefield, A., & Rubin, A. D. (2004). Analysis of an electronic voting system. In *IEEE symposium on security & privacy* (p. 27- 40). Berkeley, California: IEEE Computer Society Press.
- Lauer, T. W. (2005). The risk of e-voting. *Electronic Journal of e-Government*, 3(2), 177-186.
- Liaw, H.-T. (2004). A secure electronic voting protocol for general elections. *Computers & Security*, 23, 107-119.
- Lin, L.-C., Hwang, M.-S., & Chang, C.-C. (2003). Security enhancement for anonymous secure e-voting over a network. *Comput. Stand. Interfaces*, 25(2), 131–139.
- Ling, R. (2004). *The mobile connection: The cell phone's impact on society (interactive technologies)* (3rd ed.). Morgan Kaufmann.

- Maaten, E. (2004). Towards remote e-voting: Estonian case. In A. Prosser & R. Krimmer (Eds.), *Electronic voting in europe- technology, law, politics and society, gesellschaft fur informatik* (p. 83-90). Bregenz, Austria.
- Nightingale, V., & Dwyer, T. (2006). The audience politics of 'enhanced' television formats. *International Journal of Media and Cultural Politics*, 2(1), 25-42.
- Oostveen, A.-M., & Besselaar, P. van den. (2004). Ask no questions and be told no lies. In U. E. Gattiker (Ed.), *13th worldwide 13th annual european institute for computer antivirus research (eicar 2004)*. Grand-Duche de Luxembourg.
(www.social-informatics.net/EICAR2004.pdf.)
- Pfadenhauer, M. (2006). Crisis or decline? problems of legitimation and loss of trust in modern professionalism. *Current Sociology*, 54(4), 565-578.
- Pieters, W. (2006). What proof do we prefer? variants of verifiability in voting. In *Workshop on e-voting and e-government in the uk* (p. 33-41). Edinburgh.
- Press Association News. (2007, 19 April). *Fears over e-counting system*.
(http://www.channel4.com/news/articles/science_technology/fears+over+ecounting+system/446082)
- Rannu, R. (2003). *Mobile Services in Estonia*. PRAXIS Working Paper no 8.
(http://pdc.ceu.hu/archive/00003208/01/mobile_services_in_Estonia.pdf)
- Ryan, P. Y. A. (2004). *A variant of the chaum voter-verifiable scheme* (Tech. Rep.). School of Computing Science.
- Ryan, P. Y. A., & Schneider, S. A. (2006). Prêt á voter with re-encryption mixes. In D. Gollmann, J. Meier, & A. Sabelfeld (Eds.), *Computer Security - ESORICS 2006. 11th European*

- Symposium on Research in Computer Security. Lecture Notes in Computer Science, 4189* (p. 313-326). Hamburg, Germany: Springer.
- Srivastava, L. (2005). Mobile phones and the evolution of social behaviour. *Behaviour & Information Technology, 24*(2), 111-129.
- Storer, T., & Duncan, I. (2004). Practical remote electronic elections for the UK. In *Second annual conference on privacy, security and trust. pst2004* (pp. 41–45). Wu Centre, University of New Brunswick. Canada.
- Storer, T., & Duncan, S. (2005). Electronic Voting in the UK: Current Trends in Deployment, Requirements and Technologies. In A. Ghorbani & S. Marsh (Eds.), *Proceedings of the third annual conference on privacy, security and trust* (p. 249-252). St Andrews, New Brunswick, Canada.
- Storer, T., Little, L., & Duncan, S. (2006). An exploratory study of voter attitudes towards a pollsterless remote voting system. In D. Chaum, R. Rivest, & P. Ryan (Eds.), *Iavoss workshop on trustworthy elections (wote 06) pre-proceedings* (p. 77-86). Robinson College, University of Cambridge, England.
- Suárez, S. L. (2006). Mobile Democracy: Text Messages, Voter Turnout and the 2004 Spanish General Election. *Representation, 42*(2), 117-128.
- Valcourt, E., Robert, J.-M., & Beaulieu, F. (2005). Investigating mobile payment: Supporting technologies, methods, and use. *Wireless And Mobile Computing, Networking And Communications, 2005. (WiMob'2005), IEEE International Conference on, 4*, 29-36 Vol. 4.
- Wallace, B. (2006). *30 countries passed 100% mobile phone penetration in Q1*. Telecommunications Online.
(http://www.telecommagazine.com/newsglobe/article.asp?HH_ID=AR_2148)

Wildermuth, J. (2007, 2 Dec). *Secretary of state casts doubt on future of electronic voting*. (San Fransisco Chronicle)

Wilks-Heeg, S. (2008). *Purity of elections in the uk. report commissioned by the joseph rowntree reform trust*.

Wolin, S. (1994). Fugitive democracy. *Constellations*, 1(1).

Footnotes

¹Our original proposal included the use of ATM machines. It was pointed out to us by reviewers that banks can hardly be considered neutral when it comes to plebiscites, so we removed this option.

Figure Captions

Figure 1. Facsimile Voter Card

Figure 2. Voting Process

Figure 3. HandiVote

Figure 4. Facsimile Voter Card

Figure 5. Simulation Voter Card

Figure 6. Simulation Voting

Figure 7. Simulation Verification



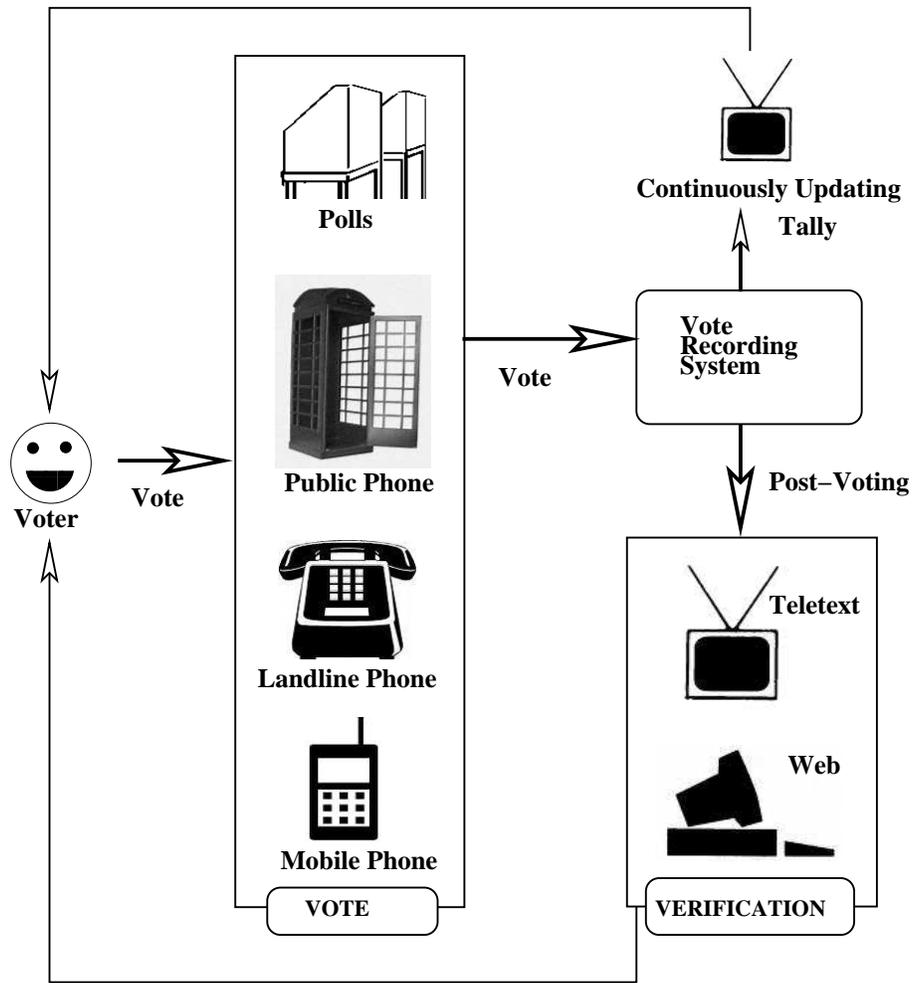
Voter Card

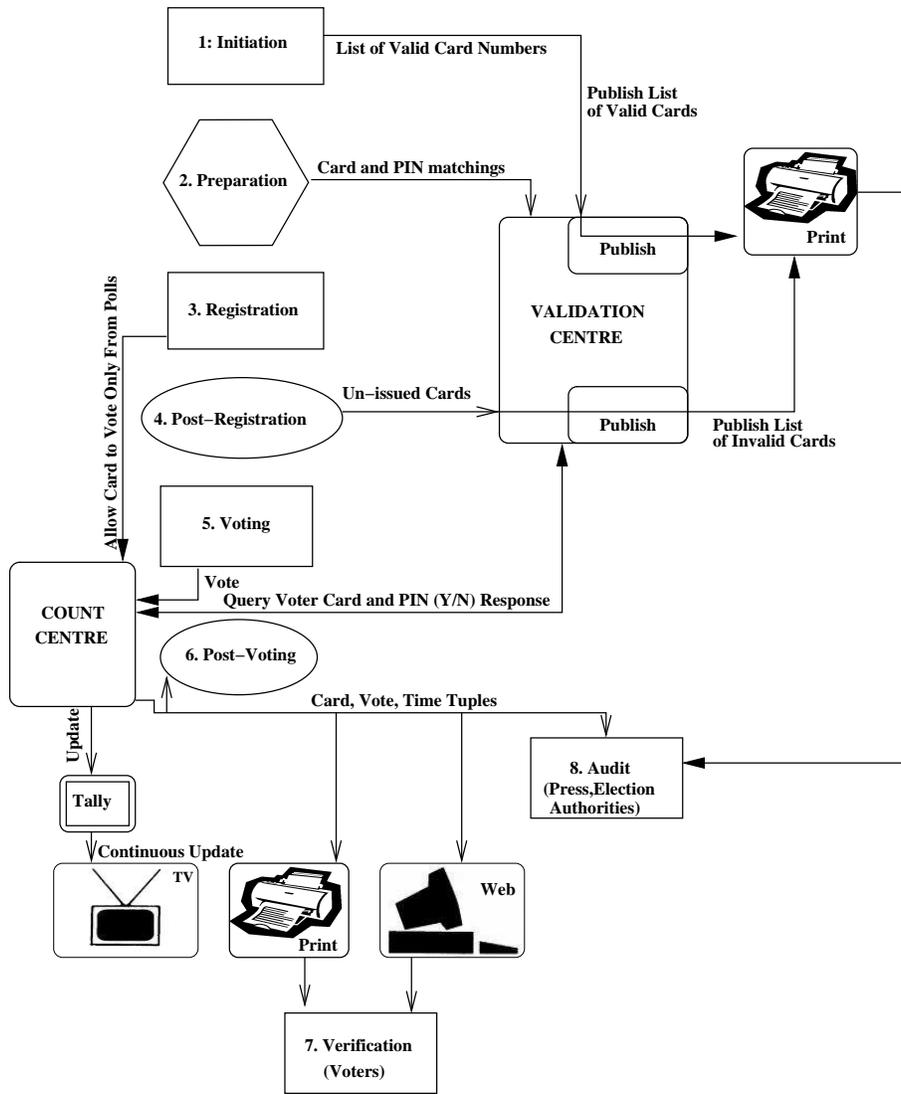
Valid Until: 09/09



1234 5678 9012

See Reverse for Telephone Numbers







← Real Time Count of Votes Cast



TV Camera

ePlebiscites



VOTING CARD

Card Number **123 456 789**

PIN Number **8765** Valid Until **04/2008**
See reverse for voting instructions

How to cast your vote

To take part in the ePlebiscites evaluation, visit:
<http://duke.dcs.gla.ac.uk:8080>



Then there are a number of different ways you can vote:

- By phone. Dial 0800 800 0000, and listen for instructions
- By SMS. Send a text message to 8888 with your card number, followed by a space, then your pin, another space, then either Yes or No. e.g. 1234567890 1234 yes
- Via a cash machine (ATM). Follow the on screen instructions.

For assistance, contact mccreada@dcs.gla.ac.uk

ePlebiscites



ePlebiscites - Telephone Voting



ePlebiscites - SMS Voting

Reminder: Send your message (in the format: CardNumber PinNumber Yes/No) to 8888

The plebiscite question is: Should Scotland be a fully independent nation?



ePlebiscites - View Vote List

This page allows you to view the Yes and No votes for a plebsite.

Votes are voided when two *different* votes are received using the same card number and PIN.

Plebiscite (P1) : Do you believe Scotland should be a fully independent nation?

List of Yes votes

Card number
0505125027
3611988357
4861141713
5156531300
5810352583
8324720917
8522235262
9111829981
9496668799
Total votes: 9