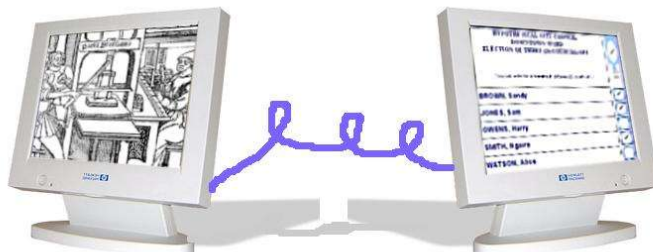


A Virtual Private Network for Internet Voting



January 2004
Everyone Counts PL
contact@e1c.net
Suite 1 207 Lygon St
Carlton VIC 3053
Australia
+61 3 9347 2199
www.everyonecounts.com

Summary : We describe our contribution to the field of Internet voting since 1997. We cover our most recent public Internet election in which we introduced two technical innovations to the field. The new work creates a virtual private network from the voter to the Electoral Returning Officer using a single public key infrastructure channel. This service includes a voter-verified inclusion service. These technologies were deployed in May 2003 for a local government election in Stratford-upon-Avon, United Kingdom, for an electorate of 100,000 voters.

1. Introduction

As many Western countries prepare to modernise their electoral systems from paper or Direct Recording and Enumeration (DRE or lever-voting) machines to electronic voting, the process of postal or absentee voting has been brought into the spotlight. The increasing maturity and acceptance of the World Wide Web as a communication medium makes it a good starting point for remote voting. Unlike the new touch-screen voting or ballot scanning machines being introduced in polling places, our approach to remote Internet voting is voter-verifiable, and open to public scrutiny.

Internet voting as a replacement for postal (or

absentee) voting introduces three distinct benefits: the vote cannot be observed in transit nor in storage before it is counted; the election is available to the voter wherever there is World Wide Web (web) access in the world and the process is familiar to users of the web; and the web is accessible via necessary compliance to the World Wide Web Consortium (W3C) standards^[1] which govern how the non-able bodied can use the web. The first point being the most important as Internet voting introduces the protection of cryptography to anyone who wants to vote.

The Internet also brings many other benefits which facilitate the education of voters, expands the reach of candidates and establishes efficient two-way communication between campaigners and the electorate. Actual vote casting on the Internet is

very quick and easy; almost effortless. What the web really introduces is a richer, more interactive political environment for voters to explore. We are seeing this in the large for the first time in the Howard Dean campaign. It follows naturally that the voters engaged by Dean's campaign will be likely to attend the Michigan Caucus ballot which can be reached via the Internet for the first time in early 2004.

Everyone Counts PL (E1C) has deployed more than 160 Internet ballots in a wide variety of configurations; either on behalf of Electoral Returning Officers (EROs) or by training EROs to use E1C tools themselves. Within this document we discuss some of the most important aspects of Internet voting and the respective challenges. We then describe in detail the ERO and voter experiences of our most recent and most publicised Internet election for a local government authority in the United Kingdom.

1.1 A brief history of Everyone Counts PL and Internet Voting.

The first legally binding web ballot is attributed to the United States Reform Party in 1996^[2]. It followed other Internet-enabled voting systems which pre-dated the web and succeeded computerised voting, starting as far back as 1972. This kind of web ballot (which we will refer to as Internet voting henceforth) is a basic web page which requires a login procedure from the visitor. The login requires a unique piece of information such as a membership number so that attempted multiple voting can be detected and prevented. This basic Internet ballot “form” consists of a list of candidates with “check boxes” next to them such that the choice of one or more candidates was possible.

<input type="checkbox"/> Dave Brown	<input type="checkbox"/> Rob Smith
<input checked="" type="checkbox"/> Derek Flatley	<input type="checkbox"/> Waldorf Lastly
<input type="checkbox"/> Saleena Patra	<input type="checkbox"/> Tran Ngong
<input type="checkbox"/> Soozie Waters	

[Click Here to Submit](#)

A basic web ballot

Internet ballots can also be “smart”, in that the system might offer a voter the appropriate ballots for their electorate out of a larger list of ballots.

One of the most useful features of this kind of automated ballot is that it is much harder to accidentally vote for the wrong people or to submit a vote that is informal or spoiled.

Most Internet elections run today are served as “secure websites” and this provides the same level of security as an Internet banking application. However Internet voting is quite different from Internet banking and so other security and privacy measures are needed. Also required of Internet voting is some form of *verifiability* so that voters can confirm their vote arrived unmodified and unobserved to the ERO. It is the ability of Internet software to meet this particular criterion which makes Internet voting a real contender as a replacement for postal or absentee voting.

Everyone Counts (formerly the Online Assessment Company) is responsible for the world's first on-line ballot in the Proportional Representation style^[3]. Since 1997, E1C has executed elections over the Internet for a total electorate of more than a million people who were eligible to vote one or more of 200 ballots in Australia, the USA, Canada, Spain and the UK. Voters attended on-line from all continents and most major cities in the world. E1C has also established polling places where Internet terminals are supervised by electoral staff and voters were marked off registers in the traditional way before being given access to the on-line ballots. Many of E1C's on-line elections have provided for voters requesting paper ballots; it has rarely been the case that an Internet ballot is executed to the exclusion of traditional channels such as attendance/paper voting or postal voting.



Postal votes are counted in Stratford-on-Avon

In summary, the advantages of Internet voting are

1. It has great reach : voters may be located anywhere and can access ballots at any time of day.
2. It is fast : a voter can vote in a few minutes, once

the session is complete, the vote will be received immediately by the Electoral Returning Officers.

3. The ballot is helpful : being a computer program, the ballot can warn voters if they have not entered enough choices or if they have entered too many. It can offer multiple languages.
4. The ballot is accessible : the Internet ballot is accessible to users of screen magnification software and speech software; the ballot can be made accessible via personal data assistants and other devices
5. The ballot is encrypted : unlike a paper mail ballot, the voted Internet ballot travels in an encrypted format that cannot be read or changed in transit.

Some of the remaining challenges for Internet voting are

1. It is difficult to determine voter identity : Internet voters have to be identified in special ways so that only the right people can vote, and vote only once. Currently this is managed by issuing Internet voters with sets of one-off voting credentials via paper mail. Ultimately, voters might reuse a set of credentials for all voting or they may be issued a device such as a smart card or biometric token.
2. Remote voters are not supervised : generally true of absentee voting – voters are currently still vulnerable to coercion and can sell their votes. The success of this manipulation can be made less reliable if voters were allowed to vote more than once, overriding their previous vote. In this way, a vote seller or a coerced voter would be able to vote again and only their final vote would be tallied.
3. Voters need web literacy : the minimum requirements for Internet voters are computer skills and web access. Regardless, the web has been a huge success because it is not hard to use.
4. The Internet voting server system is vulnerable to denial of service attacks : this means that a large coordinated effort can swamp the systems with fake requests for ballots such that real voters cannot vote. Although this has only been reported to have happened once, it is an ongoing concern. This is not unique to Internet voting and there are several research projects looking at ways to hide servers and distribute traffic such as Freenet^[4], MUTE^[5] and Freehaven^[6]. A sustained denial of service attack on an Internet election may require the ERO to extend the polling period.

We now cover some of the more detailed reasons

why Internet voting is unlike other Internet activities such as Internet banking or web surfing. The reasons lie in the special requirements of the electoral process itself.

2. Why Internet voting is special

Internet voting is unlike web surfing and Internet banking in at least three ways : firstly, while an Internet banking customer has to be identified to allow them access to their account, a voter has to be identified as eligible to vote, but their vote cannot be recorded with any kind of identifying information. It should not be possible to look at a collected ballot and then be able to work out who voted it.

Secondly, the voter must not be allowed to submit multiple votes. There are some rare exceptions to this, such as in Sweden and Denmark where voters can cast a pre-poll ballot but then change their mind and cast another ballot in the actual poll - but the majority of democracies do not allow more than one vote. With banking, there is obviously no limit to customer transactions and these include “undoing” transactions by reversing them. The voter gets one chance to vote and so this must also be straightforward and not prone to voter or system error.

Sometimes an Internet ballot is run in conjunction with a paper ballot. In this case, the submission of a paper ballot usually takes precedence over any submission by the same person over the Internet.

The third requirement is that the voter should be able to confirm that their submission over the Internet has arrived at the other end and that it was recorded as the voter sent it – not changed in any way and not having been observed while in transit. This is complicated by the requirement that the voter cannot be able to see how they voted since this would let them potentially sell their vote. With Internet banking, all transactions can be confirmed on regular bank statements for customers.

Part of this third requirement is the necessity for the ERO to see a full audit trail of the Internet election so that any detected anomalies can be reviewed. The voter themselves also must be able to independently verify that their vote was received.

Hidden under these requirements are other technical conditions such as the Internet ballot being available at all times. These are further controls over the availability, reliability and security of the Internet election server and the underlying Internet. Since

the Internet was originally designed as “the universal network for information exchange” (hence UNIX) and was to promote communications and publications, security was less important. Since the advent of e-commerce, security is now the focus for planned roll outs of the software that drives the Internet.

Because of all these requirements, reliable and secure Internet voting is difficult to implement. It can be deployed for small, private elections with quite a simple set-up, but for large public elections, considerable work is required. Some of the complicating factors are:

1. Consistency of the ballot : The ballot has to appear the same to all voters or else some candidates may be disadvantaged : if a ballot appears too large for the voter's screen, then some candidates may be obscured; the voter's configuration of their browser must not rearrange the online ballot
2. Plurality of voter machines : Web users access the web from a large variety of computers, operating systems and browsers : the most common is Internet Explorer on Windows for PC, but there are 140+ browsers, each with possibly tens of versions. There are also many versions of Windows as well as MacOS, Linux, Solaris and the many kinds of computers underneath. Each web browser may thus present the ballot differently.
3. Bandwidth limitations : The Internet slows down when there is a lot of traffic or if there is a fault : the Internet never completely “stops” which is its greatest strength, however, it can be slow. The majority of Internet voters access the Internet via modem. This slows the traffic further for those users.
4. High peak voting times : Voters tend to vote at regular times (such as between 8 and 10pm), and sometimes very many may vote at the last possible moment before the ballot closes. This places extra demands on the availability of computer systems which support elections.
5. System must serve multiple ballots : While voters may access the systems from anywhere, we still need to provide a jurisdiction ballot which is correct for them. In the US Primary elections, there are more than 100,000 such ballots. All these ballots then need to be created and made available centrally for the Internet system.
6. Secure login : Voters need to be identified more reliably than via presentation of, say, their DOB, drivers' license number or electoral register

number. All these credentials are potentially known by many other people.

7. Security of the voting systems : The location of the voting systems (that is, the voting servers) needs to be very secure and the integrity of the voting systems cannot be entirely reliant on one- or a few- technical people or the ERO. This would expose such staff to coercion or bribery.
8. Security of the voter's PC : If the voter uses a common operating system and browser, there may be viruses which attack this software or observe the voter's screen and keyboard.
9. Votes must stay in the country : The voting system may need to be in the country where the election is taking place. While the Internet lets one vote from “from anywhere”, electoral law may require the server system to be near the voting jurisdiction.
10. Software must be certified : The voting software has to be able to be changed so that it is kept up to date with Internet technology. This makes it hard to certify the software in the traditional sense.
11. Additional voting channels : Sites that want to trial Internet voting generally also run a parallel paper process to support the most voters possible. This means that personnel resources are often stretched when the new technology is being introduced.
12. Varying electorates : No two electorates are the same as each voting region has different levels of web access for citizens, literacy, perception of civic duty, disenchantment with the current voting methods and so on. Different regions also have varying numbers of voters or non-voters who may benefit from Internet voting and engaging those people requires different voter education programmes.
13. Limited ERO resources : Procedural requirements and any software learning curves for administrative staff must not require a huge time investment nor radical change in the way the democratic process works as electoral staff are typically already occupied with traditional voting channels.

Our next section introduces the EIC system in some detail as well as the general approach to establishing and systems and services for new Internet voting institutions. We explain how all of the above problems can be solved or ameliorated with procedural and technological processes. Our Discussion addresses each of the 13 points.

3. E1C and eLect

E1C has built an Internet voting system called *eLect* which we will describe as part of illustrating the electoral experiences for both the ERO and the voter in a recent election for Stratford-on-Avon District Council^[7]. Elect is a unique tool and has been written to ameliorate several of what we have described as the difficulties of Internet voting. To illustrate how this tool works and what human processes are required, we use a series of steps which follow the election process for Stratford-on-Avon, which used eLect. The steps cover the stages leading up to the election, the process of certifying the on-line election, sending voters their ballot access information, voting, counting and notification of results.

Stratford-on-Avon is a fairly wealthy district with house prices on average 40% above the national average and with a higher aged population density. This may account for 60% of its citizens having web access. Still, web access is usually associated with the young and so Stratford presented an unusual trial group. The District has roughly 200,000 registered voters and all 65,000 citizens in contested areas were subsequently given access to vote via the Internet (excluding registered postal voters).

Prior to the use of eLect, potential clients need to consider whether their constitution allows electronic voting. If this is not specified or if it is allowed, the institution can employ Internet voting in a legally binding outcome. Otherwise, Internet voting can be used for opinion polling but the outcomes have no official value.

The Internet ballot in Stratford-on-Avon required changes to UK electoral law for the local jurisdiction. This was a lengthy process and required the expertise of the Stratford-on-Avon legal counsel.

As part of the eLect service E1C has helped clients understand and even change their constitutions or corporate law to allow for this new voting channel. E1C has a strong network of qualified electoral advisers available to them. Also at our disposal are experts in proportional representation, which is a fairer ballot style than first-past-post and can be employed in many kinds of elections.

3.1 Installation of the systems

If the election requires the E1C systems to collect votes close to the jurisdiction of the elections, E1C installs its system at an approved, secure data centre nearby. The data centre can be at any major centre in the country of the election and the network access for voters will likely be the same. A number of international elections have been run from our installation in Australia.

Elect can be used as a web service from one of our established installations, it can be used as part of a consultation where E1C staff manage the work, or it can be purchased and installed.

All E1C installations include establishment of a reporting hierarchy for data centre staff and the configuration of remote computers which monitor the installation. In this way, system failures or problems are reported both internally (by data centre staff) as well as by remote computers which continuously check that the service is available. If anything seems wrong, either the data centre or the remote monitors contact E1C. Voters report issues via email or a free-call number.

In all installations, E1C coordinates with the data centre staff (during the course of the election) such that the data centre staff “lock out” E1C staff. In addition, the data centre staff themselves have no access to the software running on the voting system. In this way, access to the computers requires coordination of several parties. Finally, when we establish a new system, the computers are “load tested” to determine that they will be able to service the anticipated voting traffic peaks.

Installation takes about two weeks, but if the ballots can be run from one of our existing systems in London or Melbourne, some ballots can be opened almost immediately.

Another aspect of installation is the establishment of a call centre facility if required. In the Stratford-on-Avon election, a call centre was established on a national toll-free number for 24 hours a day during the Early Voting period (there was an International call number as well but this was not free). Call centre agents were trained in tackling both Internet and traditional election issues. This took some load off Stratford-on-Avon Council as electoral staff usually field all enquiries. The number of calls received pertaining to the Internet service was roughly 5% of the votes recorded.

3.2 Training

An election on the EIC system can be run by people with no programming or web authoring skills. If the ERO prefers to have control over all systems, then the appropriate staff are trained to design, launch, count and declare the election with eLect. EIC provides both on-site training as well as manuals for the system and a support line.

Training takes into consideration the fact that most electoral staff are already committed to supporting existing paper voting channels (most Internet deployments provide an additional channel to paper balloting). Training is not classroom-style but is provided on-line with a live installation of eLect. An on-site EIC trainer adds the essential support to make sure that client staff really understand the system and are comfortable with it.

For new Internet voting deployments, some clients want the election to be created and run by EIC staff - the responsibility then rests on EIC who reports at regular meetings on the progress of the run.

Training includes the management of voter education and publicity. In Stratford-on-Avon this involved a broad campaign that reached half of all voters on a very limited government controlled budget. The campaign involved local press articles, a radio advertisement campaign, visits to old age pensioner groups, establishment of demo systems in local council offices, posters and banners around the district and press kits for regional and national media. In addition, EIC provided a website which ran a demo ballot, a survey, a quiz and a long FAQ.

In addition to this, EIC can also create curriculum material for local colleges and schools. This introduces Internet voting to new voters and to those students who will be of voting age in time for the next elections.

3.3 Ballot design

eLect provides a friendly, graphical “wizard” for creating ballots. eLect helps administrative staff progress the ballot design and publication by providing stages of authoring similar to a paper ballot. These are “draft” - during which time any changes can be made, “released” - which is when the ballot is “locked down” and ready to be published, “open” - when the ballot can be voted by voters and “closed” - when late voters are told they cannot log in to the ballot to vote any more.

Once the ballot is released, it provides interactivity via the web from a unique Internet address. The ballot can be “recalled” from being “released” and changes can be made, but this results in entries in the security audit log (covered below).

eLect has created ballots in a wide variety of formats via its authoring tool. These include first-past-post, single transferable vote (STV) ballots, above- and below- line voting, run-off voting, preferential and exhaustive preferential, and referenda.

If the authoring tool does not meet the requirements of the election in terms of the layout or behaviour of the ballot, a “higher level” editing system called eScript is used. eScript is a “mark-up” ballot language like a very simplified HTML. It is intended to be human-readable and gives the administrator the ability to change just about everything eLect does for their ballot.



An image of the graphical system for creating ballots. This is one stage of a “wizard” which guides the administrator through creating the election on-line

```
.title Election
.type %election
.open 10/4/2006:09:00
.timezone Europe/London
.who %group NewUsers

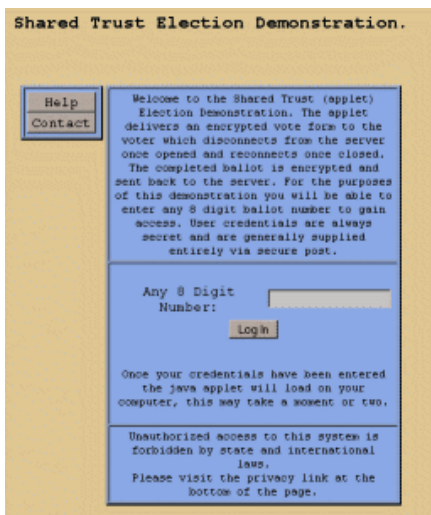
.ballot %cleaner fpp
.ballot %elect 1
.ballot %limit 1
.ballot %counter fpp
.ballot %type checkbox
.ballot %title Prime Minister

.info Please choose no more than
one candidate
```

Equivalent eScript for creating the same ballot. eScript can be used to control almost all aspects of the eLect system.

Some eLect users make up a draft ballot with the graphical tool, then convert the project to eScript to make modifications if needed. eScript allows the embedding of HTML so that existing content (such as candidate speeches) can be reused in the eLect ballot.

A single Internet election may in fact have several ballots built in to it. When the voter accesses the Internet system and logs in, the system offers them the right ballots based on the electoral enrolment of the voter. This makes running multiple elections much easier as the voter is guided through all ballots in one voting session.

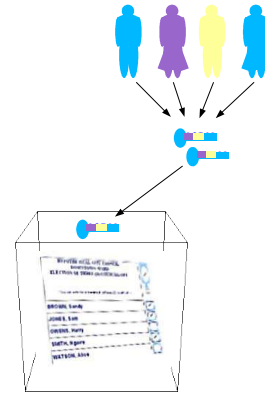


This is an on-line demonstration ballot, showing login and ballot types.

One of the most critical aspects of creating the Internet ballots is the creation of cryptographic keys which will then “lock” the voter's submitted ballots so that they cannot be changed before they are counted.

This is achieved by using a common technique called Public Key Cryptography (PKC)^[9]. One or many officials and observers contribute passwords which together combine to give access to the created keys. One key, the public key, is sent to the voters to encrypt their ballots; it cannot be used to decrypt ballots. A second key, the private key, is kept by the ERO to decrypt the votes; it cannot be used to

encrypt them. The decryption key can only perform this task if all the passwords created are provided correctly in order by all official observers.



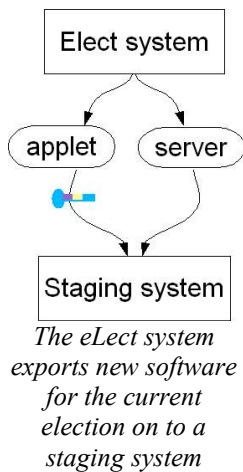
One or more official observers are required to create cryptography keys which protect ballots

3.4 Release of the ballot and sign off of the ballot images

When the administrative staff have finished drafting the ballots, the configuration can be tested. A test might involve enlisting the help of other staff. eLect facilitates this by sending out links to the ballot via email to a (possibly) large list of staff email addresses. In this way, everyone gets a link to the ballot, gets to test the login, votes, and then the ERO can declare a test outcome or compare with a manual count.

If the test is satisfactory then the ballot is given a formal “open” time. This is the time the ballot is to open for voters to vote on it. Any voter who visits the address of the ballot before it opens is told they are early. The system will then refresh the page each minute so that if the voter accesses the site just a few minutes before the polls open, they need only wait for the ballot to become accessible rather than having to “keep trying”.

When the ballot is released, eLect creates separate, new software which will run the election. The eLect authoring system itself cannot affect the running ballot and can even be shut down. The software that runs the actual election is a very small, simple pair of programs. One part which we refer to as the “Server” stays on the “staging” system while the other part is served out to the voter and executes in the voter's browser. We refer to this as the “Applet”.



The Applet is machine-written in Java1.1. It can be exported from eLect so that a third-party auditor can examine the software and then digitally sign it. This provides considerable assurance that the software is free from errors and is not biased in any way. The third-part digital signature then prevents anyone from changing this critical piece of software before, during or even after the election event.

Because the Applet controls the appearance of the ballots, administration staff can print screen grabs of the ballot pages. This is a way of having more traditional sign-off executed. If the ballot is not “recalled” from being released, then the ballots will be served to voters exactly as they are shown in the screen grabs.

The Applet is the most important part of the system. Only the Applet can modify voter's votes. The Applet encrypts votes so that they cannot be changed in transit across the Internet, nor while in storage at the voting system, nor at any other time before the ERO receives and decrypts them. This is performed by using the public key created by the ERO and the observers.

Making the computer code for the Applet software available to the general public is possible because none of the security the Applet uses is hidden in the software itself. This is similar to the way in which the design of most door locks is well known but this does not make the locks easy to break.

Making the Applet software available to the public is also very important because it demonstrates that the system is not a “black box” and helps build the voter trust in the electoral outcome. eLect itself is a very large program and would be very difficult to audit and certify. By producing the minimal Server

and Applet software which run in isolation from eLect, it is much easier to prove exactly what software is “inside the box” running the election.

Another advantage of the Applet is that the voter can disconnect from the web while they vote. They then re-connect when they want to submit the vote. This makes it harder to remotely affect an Internet voter while they vote.

The Server software is an application that manages the storage of votes and manages voters authentication requests. This script too can be made available for audit, but because only the Applet has the ability to create votes, the Server is less critical.

Neither the Server or the Applet are used again for another election; they are archived with the declaration of the election so that there is an exact record of the software that was used to run the election. New elections on eLect result in the creation of more new Applets and Servers. “Used” Applet and Servers are deleted from the EIC system.

3.5 Management of voter authentication

Voters must provide proof of who they are in order to demonstrate that they are eligible to vote and to allow the system to determine that they have not already voted. eLect supports a wide variety of ways in which this can be done. They range from “unique user name and password login” as used by many computer systems, “unique VIN and PIN login” which has been become the standard for Internet voting or “web crossing” which allows a voter to be authenticated elsewhere then “passed” to eLect. In addition, eLect will allow any number of arbitrary credentials to be required for the voter to gain access to the ballot; these could be social security number, drivers license number, password and so on; as many as required.

If the ERO has private information about voters (such as passwords from some existing system), then these can be imported into eLect in an encrypted form so that they cannot be used to vote except by a voter who knows the original password. Failing this, login to the ballot can require a combination of non-private information such as suggested above : e.g. social security number, DOB, electoral roll number, in combination.

Alternatively, if the ERO wishes to send voters

“one-off” credentials, then eLect can create them. In this case, eLect generates random data which are hard to guess (by being many bytes long). The ERO can then export these from eLect and have them overprinted on to electoral information which is posted to voters via paper mail.

In Stratford-on-Avon, 65,000 voter records were extracted from the Pickwick voter roll computer program. The data was cleaned using EIC software; duplicates were removed and some missing fields were reported. All records included the voter registration number (RN), voter name, address, and voting precinct for contested parishes and wards.

The voter register number (which is a publicly known datum) was modified by having an extra digit added to the end. This extra digit is a checksum digit. It allows the Java applet to validate the RN without having to request a remote check back at the voting server.

EIC created unique 11-digit ballot numbers (or BNs, which are usually marked on the paper ballot) and 5-digit PINs. Being 11 digits long for a field of 65,000 voters meant there was only a one-in-769,230 chance of being able to guess a legal BN. The PIN also included a sixth digit which was again a check sum value, for the same reason as the RN. In fact, the PIN was not unique and functioned more as a kind of password and did not identify the voter.

In addition to the 65,000 sets of credentials, EIC created an additional 1% as spare to distribute to voters who did not receive a polling card by mail. Since a set of credentials identifies a specific jurisdiction, EIC created spare credentials across all jurisdictions so that the live voting system did not need its records to be updated in case of spares being issued.

To determine if any poll card fraud had taken place, EIC ran an outbound telephone survey which contacted 750 people to find 100 voters. There were no instances discovered where a polling place voter was denied a vote because of a previous, fraudulent Internet vote, and similarly, there were no recorded cases where Internet voters were not marked as having voted in the polling place register.

The Internet voting was not run at the same time as polling place voting and so EIC coordinated the printing of polling place registers for voting day which were already marked for voters who had voted on-line. In this way, it was not possible to vote by both methods. Postal voters were not

permitted to vote on-line.

Two secret credentials (PIN and BN) instead of just one were specifically created for Internet security reasons: when the voter requested the ballot, their BN was sent over the Internet. The RN and PIN were not – they were “self-checked” against their checksums by the applet.

The use of checksums is a common practice in the credit card industry. The technique is called a LUHN checksum^[10]. It works as follows : the original letters and numbers are converted to values (A is 10, B is 11 etc. and numbers 0 to 9 stay as these values). These converted values are totalled up such that the same list of numbers and letters produces the same single-digit total. If one letter or number is entered incorrectly by the voter, then the checksum digit will not match the total of the entered letters and numbers. The LUHN technique is specifically designed so that “transpositions” or accidental re-orderings of the entered voter credentials trip up the checksum.

In this way, only one of the two secret credentials, the BN, can be considered as compromised as it has to leave the voter's computer. The RN and PIN are checked at the voter's PC. The disadvantage is that there is a 1 in 10 chance a voter enters the wrong PIN or RN and the checksum test still passes. In this case, the vote is recorded but it will ultimately be unauthorised and were not counted.

3.6 Notification of election

EIC has variously notified electors of an upcoming election by using paper mail, email or by advising the electoral authority on the use of local media or other publications. If the electoral authority has email contact with its voters (such as might be already established in a union or other organisation with a fixed membership), then this is by far the best way to both notify voters and deliver the voting web address. “Email notification” has seen three-fold attendance improvements for some EIC clients along with very rapid response from the electorate.

For public elections, email notification is less effective as most local government authorities do not have established email interactions with citizens. In this case, paper mail is used as the local government database of street addresses for citizens is typically updated regularly, in-line with rates and mortgage records. One advantage of Internet voting in public elections is that the process might require the voters to register an email address that can be

used in an ongoing fashion for other on-line ballots.

For Stratford-on-Avon, every voter in the contested jurisdictions was sent voting information which included Internet voting access credentials. In addition, E1C helped Stratford-on-Avon to create local radio advertisements, parish newspaper advertisements, posters for the local railway station, banners, press kits, and interactive mock-ups of the system in the lead-up to polling. E1C also attended local community meetings to demonstrate the system and collect feedback. E1C helped create a website for Stratford-on-Avon which included a mock-up of the ballot, a quiz, a survey and a large list about the system. Voters could also click a link and request the software code for the Java Applet itself. The website collected email addresses for use in an automated notification and subsequent automated reminder emails.

The polling card included the details of the voter's local voting station so that they had the choice of attending on the 1st of May or voting early via the Internet up to a day before May 1st. The voter was given their voting credentials – the RN, BN and PIN as well as the WWW address of the voting system. This address had not been published prior to voters receiving polling cards. Information on the Stratford-on-Avon Council website was modified so that there was also a link to the ballot from this location as well. If the Stratford-on-Avon website was not available at any time, the voter could key-in the address of the voting system from their polling card. This address had a simple format which was tied to the Stratford-on-Avon web address : vote.stratford.gov.uk. While this address appeared to be part of the Stratford-on-Avon website, the E1C system was actually a completely separate system not reliant on the Stratford-on-Avon system at all.

3.7 Polls open

eLect opens the ballot automatically at a pre-configured time. Voters who visit the address early (but after the ballot is “released” by the ERO) are told they are early and are given the exact remaining duration in days, hours and minutes until the ballot will open. If they arrive close to the time the ballot is due to open, then the page they are given will count down for them and bring up the ballot automatically.

Once the Stratford-on-Avon ballot was open, the voter was asked for their BN. This was used to identify if the voter had a legal BN as well as

whether the voter had voted already or not. If the voter entered a correct BN and if the BN had not already been recorded for the ballot, the voter was served the voting applet client.

Because the applet did not allow the voter to increase the text size, we created a link on the ballot page above the applet which was “Click here if the ballot does not appear below or if you would like the Large Print ballot”. This sent the authenticated voter to a “secure site” version of the ballot which did not use an applet client. This additional “fail over” mechanism meant that users of text browsers could also access the ballot and users with systems that could not execute the Java client would still be able to vote on-line. The “secure site” system is not ideal as it does not encrypt the votes, it only uses the encrypted-channel protection of the secure site connection.

To make sure all candidates appear on the screen without scrolling, the applet automatically creates two columns when needed.

Thirty percent of Stratford-on-Avon voters used the “Large Print” link even though at least 95% of the browsers and systems used can run the applet. We believe that this is attributable to Stratford-on-Avon's large aged population and that the “Large Print” link would have attracted more voters familiar with large print documents. Ideally, we would only offer the “Large Print” link if we could not remotely determine the voter's browser compatibility.

3.8 During polling

During polling, E1C staff support local administration officers and provide answers to technical questions or issues that are reported by voters or voting staff. On a daily basis, certain collected information can be reviewed by the ERO. Some information collected by eLect can be given to political agents such as a marked register (the list of who has voted or a list of all voters with marks). The local laws governing elections define what information can be made available at any time.

In simple ballots such as polls, voters may vote more than once. In this case, we count the collected votes and announce results, possibly several times during a set duration. Supporting a more traditional ballot requires that no count of the election can be performed until the close of polls.

During polling, the computer system creates an

election event log. This is a file of events recorded for voters. It does not expose the voters' identities. This log file captures events such as attempted logins, failed logins, timed-out voting sessions and successful submissions. This lets the ERO monitor the voters' general ease with the procedure. If it appears voters are making many attempts to log in, extra instructions can be added to the website the voters visit to get the ballot, for example.

Some of the more common requests for support during voting are due to lost polling cards. It is obviously important not to give a voter fresh credentials to access the ballot without strong identification. In this case, a fresh printed voting instruction form was issued to the voter and the original credentials that failed are tested against the system and may result in a ballot being marked unauthorised.

A ballot can be made unauthorised by the manual removal of a voter BN from the eLect list of voters. This does not destroy their ballot but marks it so that it is not counted at the close of polls. These ballots and other unauthorised ballots can be included in a test count if required.

The Applet checks the RN and PIN via their checksum values and the voter is offered the appropriate ballots for their jurisdiction. In Stratford this was at most two ballots – one for Parish and one for District. Some voters received only one ballot if either their Parish or District was not contested.

The pages of the applet appear instantly and the session can be very quick regardless of the voter's connection to the Internet. This is because the applet downloads in its entirety (128K in size), executes on the voter's computer and does not communicate with the server until the ballot submission. It presents the ballots exactly as they were viewed by the ERO, regardless of the browser or computer system the voter is using.

The applet warns the voter if they have chosen too many candidates. They are not allowed to choose too few. This can be set to vary with the local election rules. The applet offers a summary page showing the choices the voter has made and if the voter wants to make changes, they can go “back” and makes as many changes as desired. When voters are finished, they are prompted for a password (which we called a “keyword”). This password is used to create a receipt only they will know. If they proceed, the vote is encrypted and

submitted over the Internet.

If the voter is in the process of voting but loses their connection (such as if their modem times out) they can connect again and submit the ballot. If they abandon the session, they can log in again provided they have not successfully submitted before. In fact, the applet allows the voter to purposefully disconnect completely from the web and then reconnect when they are ready to submit the vote. This thwarts common “remote observation tools” used in many workplaces such as PCAnywhere and VNC.

The Applet presents considerable defence against viruses which potentially can affect the way a ballot appears or behaves in a web browser. A common fear among specialists is of a potential “Internet voting virus” that attempts to change votes on their machine. In general, the risk to the remote voter from viruses is ameliorated by the following:

1. a “voting virus” specifically aimed at remote voters has to find them without itself, being detected. Since virus propagation is a kind of broadcast, it is more likely that a more prolific virus would be detected. That is, probability of detecting a virus increases with the breadth of its spread as it will inevitably hit systems scattered across the Internet which are put there to detect new viruses.
2. On the Internet, it is hard to find PCs which are going to be used for Internet voting as this can take place on any kind of machine. For this reason, it is harder to “set up” any kind of attack in advance
3. An attack on remote voters is a more attractive activity to attackers if it affects more voters. The voting Applet could potentially be observed remotely if the voting machine has already been infected with a particular virus such as Back Orifice. However, effecting, say, a change in the voter's preferences is very hard as this would require an attacker to see and understand what the remote voter is doing. This makes it hard to automate. Automating such a process would also make it much harder to conceal as the remote voter can see choices being taken for them.
4. A successful “voting virus” would have to be a new virus as many known viruses are already detected by common PC virus software. In addition, many new PCs are sold with virus software subscriptions and “personal firewalls” which block remote access.
5. The majority of viruses act when the user opens an email attachment. Voter education in the lead up to the election can improve voter's vigilance

to viruses and other potential Internet ploys. The attacker does not have this educator access to voters.

Once the voter is happy with their preferences, they can submit the ballot. If the submission is successful, the voter is informed of this and issued their receipt. They are advised to write down the receipt as this can be used to prove that their vote was received by the ERO without having been decrypted or otherwise modified or observed in transit or storage. This is made possible via the Public Key Cryptography^[9] preparations described above.

If they wish, the voter can visit the “vote checker”(VC) website during the election to confirm that their submission was received. This is advertised on submission of the ballot as well as in the polling card. The VC website cannot yet prove that their vote was received intact as this requires the votes to be decrypted. This is described next.

3.9 Close of polls

The on-line ballot closes automatically at a fixed time. For any voters who logged in before this time, the system observes a grace period so that they can submit their votes. For those who arrive after the close of the ballot, a friendly “closed” message is given.

In the specific example of Stratford-on-Avon, the Early Voting resulted in an interim result that was not made public at the close of the Internet ballot, but was combined with the rest of the election to give total outcomes. In this case, the ballots are counted but the results are “exported” so that they may be either automatically or manually incorporated into other systems.

Either way, the results are counted and the ERO declares the outcomes. If the Internet votes are part of a larger election employing paper and other channels, then the Internet voting result is merely combined as an interim total with the totals of the other channels. If the election is an STV or other proportional type ballot then all ballot data need to be combined together to allow a count. In this case, the other channels are either fed into the eLect counter or the Internet votes are printed out as a list for hand-counting.

The eLect vote counter can provide various reports at the close of polls. These include full count sheets

for STV ballots, including quotas, exclusions, vote carries and other statistics. For FPP ballots it gives the raw totals for candidates, the winner(s) and number of unauthorised ballots, and number of informal, invalid (or spoiled) ballots. In this latter group, the report includes a summary of reasons why the votes were spoiled : these include over-, under-, and blank- voted ballots. For STV ballots the reasons can be much more elaborate.

Your receipt is:

f73f 35da 1144 66cd 8158

This should match the receipt you were given when you cast your vote. If the receipts do not match, you may have entered your Ballot Number or keyword incorrectly. Please carefully check them and try again. If you are sure that you have entered your Ballot Number and keyword exactly as you did when you voted, and the receipt you see here is different to the one you received then, please contact the Helpline on 0800 052 2481 or +44 (0) 2392 899 224.

Type your Ballot Number in this box:

Type your Receipt Keyword in this box:

The voter verification service can prove that the vote has not been changed or observed in transit or storage

After ballots are decrypted, they are checked for consistency. The voter can check that their vote was indeed received intact for the BN, RN, PIN and personal password of the voter. This is done by again visiting the Vote Checker site (as above) and entering the BN and receipt password. A simple mathematical operation then attempts to calculate the receipt the voter would have seen based on the collected RN and PIN (encrypted with the ballot) and the password and BN (entered by the voter). Only the voter can know if the resulting recreated receipt is in fact the one they were issued.

The ERO can publish the outcome of the election over the Internet to voters. This is possible either by replacing the content on the voting website or by having eLect replace the original link to the ballot with a link to the counted results of the ballots. In this way, voters need only check back shortly after the close of polls to get an instant result.

Depending on the arrangement for the use of the eLect systems, the client may then have ongoing access to run as many ballots and surveys as they please.

3.10 Reporting

E1C writes a report for clients that contains the

following information and includes a compact disk of collected data.

The written sections are

1. Summary of the particulars of the election
2. Summary of events and anomalies
3. Summary of call centre events
4. Graphs and statistics on voting participation, including geography, time, etc.

The data files are

1. A file of all election events recorded by the system
2. The software which ran the ballots; server and client
3. The decrypted ballot data
4. Declaration created by eLect

4. Discussion

The Stratford-on-Avon pilot was possible because each of the Internet voting challenges introduced in a previous section were met or ameliorated as follows :

1. Consistency of the ballot : the appearance of the ballot is controlled not by the voter's browser but by the Java card layout system. The ballot appears the same to all voters.
2. Plurality of voter machines : Using a JDK1.1 Java applet as the basis of the ballot function places its execution in the Java Virtual Machine, not the actual browser, operating system or machine underneath. A fail over mechanism was provided for text browsers which was a standard SSL voting channel.
3. Bandwidth limitations : The Java Applet downloaded at the initiation of the voting session. Interactivity with the ballot was then immediate regardless of Internet traffic.
4. High peak voting times : The voting servers were rated against estimated peaks, not mean traffic.
5. System must serve multiple ballots : The Applet served one or two of 26 ballots to each voter. It can serve many more as required.
6. Secure login : All voters were delivered a Ballot Number and PIN via second class mail. A telephone survey of 100 Internet voters in the highest use voting areas found no evidence of fraud.
7. Security of the voting systems : The voting servers were not located at a shared-use facility

but were managed by an e-voting consortium, Anite, who were responsible for a number of other e-voting pilots. To remove the dependence of the system on one- or a few-people, coordinated access was required to access voting servers. More than one password is required to decrypt votes and the eLect system itself does not require an EIC consultant to operate it on behalf of the ERO.

8. Security of the voter's PC : the voting Applet is hard to break directly from the operating system : it also allows the voter to disconnect while they vote to thwart remote observation.
9. Votes must stay in the country : The servers were located roughly 1 hour from the voting district.
10. Software must be certified : The only software which can modify votes, the Applet, was examined and signed by a software company who declared it free of bugs and free of software which could manipulate the voters' ballots.
11. Additional voting channels : Internet voting in Stratford-on-Avon did not occur in tandem with polling-place voting. Other Internet voting executed by EIC has allowed for the potential removal of Internet ballots from the count.
12. Varying electorates : EIC executed a broad voter education programme and media campaign which reached half of all voters and which was directed at everyone from new voters to old age pensioners. Follow-up surveys received submissions which included praise from non-voters, the disabled, the aged and many others.
13. Limited ERO resources : An EIC staff member was on-site for the whole Stratford-on-Avon Internet election.

5. Conclusion

The EIC deployment of Internet voting for Stratford-on-Avon District Council was one of the first of its kind in the world. This adds to the fairly long history EIC has enjoyed in the field; more than 160 Internet elections since 1997. The success of Stratford-on-Avon and the learning experiences gained demonstrate the valuable process of Internet vote pilots.

EIC has taken a novel route in providing for institutions that want to use this electronic channel for voting. EIC has one of the most secure solutions even trialled; the provision of public key cryptography from the ERO to the voter's remote PC. The solution is transparent to the voter and does not require any software installation. Creation of the election is greatly facilitated by the EIC tools

which enable non-technical staff to create and run the election themselves.

E1C has also successfully deployed a voter-verifiable audit trail so that voters can know their vote was received and decrypted from them, intact.

E1C will continue to innovate and provide even better solutions in this field. In 2004, E1C will provide a telephone voting system which uses the Applet system of voting.

References

- [1] WCAG, the W3C Access Guidelines
<http://www.w3.org/TR/WAI-WEBCONTENT/>
- [2] An history of e-voting
http://www.eucybervote.org/Reports/KUL-WP2-D4V1-v1.0-01.htm#P323_14632
- [3] Proportional representation voting example
<http://www.fairvote.org/irv/muppets/index.html>
- [4] Freenet, an anonymous network development at
<http://freenet.sourceforge.net/papers/freenet-ieee.pdf>
- [5] MUTE, an optimised anonymous network
<http://mute-net.sourceforge.net/howAnts.shtml>
- [6] Freehaven distributed data storage
<http://www.freehaven.net>
- [7] Stratford Evaluation .pdf is available at
<http://www.everyonecounts.co.uk/downloads/StratfordEvaluation.pdf>
- [9] Public Key Infrastructure and Public Key Cryptography
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214299,00.html
- [10] LUHN checksum algorithm
<http://www.ee.unb.ca/tervo/ee4253/luhn.html>