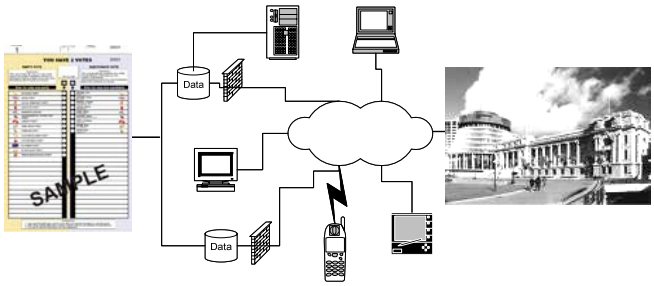
Chief Electoral Office

Ministry of Justice
Tahu o te Ture
Wellington
New Zealand

Draft Long Term Strategy for Voting Technology



Version 1.1

TABLE OF CONTENTS

Draft Long Term Strategy for Voting Technology

1 Executive summary

1.1 Summary of Draft Strategy

PRINCIPLES

This draft strategy examines the desirability and technical feasibility of electronic voting (e-voting), and considers how it could be implemented for general elections and referenda. The proposed approach is cautious, and aimed at ensuring that high levels of public and political confidence in the electoral system are maintained.

Voting methods currently in use are working well for most people and enjoy high levels of public confidence. However, there is an existing demand for e-voting from sections of the community for whom paper-based ballots or the need to attend polling places result in accessibility difficulties or an unsatisfactory voting experience, for example a lack of independence and privacy.

Looking to the future, there are indications that the demand for e-voting is likely to grow. There is a risk that voters with a strong preference for e-voting may not vote at all if the choice is unavailable to them. It is important to note, however, that e-voting is only part of the solution to diminishing voter turnout. The introduction of e-voting would be a highly visible demonstration of the viability of electronic delivery of government services. Its introduction would support Government and state sector priorities for the next decade, including the Digital Strategy and the Disability Strategy.

E-voting will not suit all voters. It will be inaccessible for some. There should be no pressure on voters to change. Current methods of voting should be maintained for the foreseeable future, and e-voting should only be an additional and optional means of casting a ballot.

The costs of e-voting will exceed savings until the volume of e-voters builds up. Under a cautious step-by-step approach, this is not expected until several cycles of elections have been completed. A wide range of non-financial benefits have been identified however

PROPOSAL

The draft strategy suggests that e-voting should not be made widely available until three or more cycles of pilots at elections have been completed. This enables a prudent step-by-step path of learning and development to be followed. In this way, increasing demand for a wider range of methods to cast a ballot can be met while maintaining democratic principles and a trustworthy electoral system, and ensuring the integrity of individual votes.

Small scale, carefully controlled pilots that would test specific elements of e-voting solutions in real electoral environments, is proposed. The greatest benefits would be gained by enabling electronic voting from unsupervised locations such as home, work, or public Internet facilities. Telephone and Internet voting methods are favoured for pilots, and both could be piloted at the same time.

Unsupervised remote voting raises particular challenges for: voter privacy and the secrecy of the vote; the exposure of the voter to undue influence or coercion; system security and integrity; and the ability of voters to be confident that their vote has been received and counted as intended. These challenges can be met, with the proposed solutions to be tested in trials and pilots.

Online voting also requires a higher level of authentication of voters' identity compared to in-person voting as a different level of risk applies. E-voting could potentially be susceptible to large scale electoral fraud or attempts to disrupt elections. Such crime may originate from outside New Zealand.

Use of the Internet for voting raises a number of risks which are particular to the nature of the Internet and personal computers (such as security weaknesses and highly coordinated 'denial of service' attacks which result in web sites becoming unavailable to users). These problems have been well documented in other e-voting analyses and are likely to affect public trust. The draft strategy takes account of these risks, with a package of mitigations suggested.

To gain maximum value, it is suggested that the initial pilots be designed to improve the accessibility of voting to voters who are currently disadvantaged by the paper-based system, such as blind and vision-impaired voters, and voters with other disabilities; and to test the various aspects of an e-voting system that would enable its secure and reliable extension in the future. After evaluation and subject to satisfactory outcomes, the scale and scope of pilots would increase over the course of three or four elections, thereby: facilitating access to voting; enabling cost efficiencies in the electoral system; and, as scale increases, improving choice and convenience to a wider base of voters. The approach should be as open to scrutiny as possible, including publication of system details and the outcomes of pilots. It is suggested that independent e-voting observers be appointed.

The option of electronic voting in polling places (such as the 'kiosks' used widely in the USA and parts of Europe) is not favoured. The costs would be high and the benefits, compared to the well-functioning paper-based system, would be minimal.

Ongoing assessment of the risks to the secrecy of the vote, undue influence or coercion, transparency of process, and resistance to electoral fraud or disruption, is required so that appropriate levels of response can be built into the pilots at each election. The high level system architecture 'straw men'[1], discussed in this strategy, incorporate high levels of protection and transparency. Actual implementations should apply specific controls and restrictions flexibly, according to the assessed risks and the

[1] A 'straw man' in this document is an illustrative and partially 'fleshed-out' example to assist discussion, not a fully developed proposal.

objectives of the pilots. The draft strategy takes into account other risks such as possible loss of sovereignty or control over election data and processes.

The Chief Electoral Officer must have the authority to suspend or cancel e-voting pilots at any time if the integrity of the election is threatened or if public confidence in election outcomes could be lost.

Two important features of the proposed e-voting system are designed to mitigate key risks. The first is that e-voting be undertaken in the advance voting period – usually about 17 days ending on the day before polling day. This would ensure e-voters are not under time pressure and can choose an opportunity convenient to them when they are likely to be in private. Advance e-voting also provides administrators opportunities to manage any technical, security or process issues that may arise, with minimal impact on e-voters. It is unlikely that an e-voter would inadvertently be deprived of their vote in the event of any problem with the e-voting system because advance voting would allow them to vote conventionally on election day.

The second feature is the ability to re-vote, either electronically during the advance vote period or at a polling place on election day. This is a powerful safeguard against the risk inherent in unsupervised voting of e-voters being more exposed to coercion or undue influence, and can reassure an e-voter who may be unsure that their e-ballot was correctly cast. Only the last vote counts if an e-voter votes again.

If an e-voter is not satisfied that they can cast a secret electronic vote of their own free choice, they can cast a traditional ballot at a polling place, and that vote would over-ride any previous e-vote. The democratic principle of everyone having the same number of votes is maintained in that everyone has the same number of votes *counted*.

The usability of e-voting systems is just as important to the success of e-voting as other challenges, and must be balanced carefully against the complexity that can arise from risk management measures. Pilots should include assessments of user-friendliness, e-voter satisfaction, and wider public attitudes. E-voting on a moderate to large scale should not proceed until there is well justified public confidence in all aspects of the system.

IMPLEMENTATION

E-voting will not be possible for the 2008 election, and there are significant risks with implementation in 2011. Further legal and policy work (including public consultation) and enabling legislation are required in advance of the introduction of e-voting. The preparation of a detailed business case and cost estimates is also advocated.

Two implementation timelines are included, commencing either in 2011 or 2014. The 2014 timeline would enable the successful implementation of e-voting, without compromising the delivery of high quality election services in 2008, when the general election must be held. The 2011 timeline has been included in the draft strategy to illustrate the operational risks to the Chief Electoral Office. These would be exacerbated if a by-election or a citizens initiated referendum were also to be held in 2008/early 2009.

2 Vision and goals

The draft strategy shares the vision of the Chief Electoral Office.

Chief Electoral Office Vision: Widespread public and political confidence in the administration of the parliamentary electoral process.

The e-voting contribution to this vision is:

An electronic voting system for New Zealand capable of delivering user-friendly and convenient voting services of high integrity to those voters who choose to use it.

There are two proposed goals for e-voting technology which must both be satisfied:

2.1 Goal 1: Improve access to voting

There are three component parts to this goal, which have been ranked in order of importance:

a) *To utilise e-voting technology to reduce barriers to participation in voting*. This is the prime objective because it addresses those who are currently unable to vote, or who face particular obstacles to voting.

b) *To utilise e-voting technology to improve the quality of the voting experience*. Not all voters have the same experience of voting. This objective targets improvement in key characteristics of the vote:

- privacy – the opportunity to cast a secret ballot;
- self-sufficiency – the opportunity to cast a vote with the least possible aid from others; and
- user-friendliness – reducing physical difficulty, the complexity of the voting process, and the likelihood of errors (which could invalidate the vote).

c) *To utilise e-voting technology to increase choice and convenience for voters*. Voting methods should be relevant to the communities they serve and recognise that preferences and priorities change over time, but also that the established practices can be highly valued and contribute to a sense of community. Responsiveness to voter preferences and social change is likely to influence future levels of participation.

2.2 Goal 2: Maintain or enhance the trust and confidence of voters, candidates and politicians in the electoral system

There are five component parts of this goal:

a) *To ensure e-voting technology incorporates appropriate high levels of accuracy, security and reliability*. It is essential that the application of technology does not enable or facilitate votes being removed,

changed, diverted or inserted, or result in the opportunity to vote being denied.

b) *To ensure e-voting technology and associated processes are transparent and verifiable, both to the voter and to audit or scrutiny by other parties.* Acceptance of new technology will be assisted by the ability of voters to assure themselves that their vote has been received and counted as they intended. The technology should also facilitate measurement that enables accountability for electoral administration.

c) *To ensure e-voting technology balances individual voter needs with the concerns and requirements of citizens overall*. The technology should reflect a balance between 'customer' requirements, democratic principles, and consensus about what constitutes good public service in electoral administration. (A number of trade-offs or balances can be envisaged: ease of voting versus voter authentication requirements; convenience of voting versus security; secrecy of the vote versus ability of a voter to check that an e-vote was correctly lodged; and so on).

d) *To ensure e-voting technology is cost-effective and meets real needs*. Initiatives that appear wasteful or do not bring real benefits (as perceived by stakeholders) will result in a loss of confidence in the electoral system.

e) *To ensure e-voting technology is integrated and efficient*. In particular the technology should, where practicable:

- use common standards;
- use common tools and networks; and
- provide for collaboration and multi-use.

Timeframe: The proposed strategy looks forward ten years to 2017. This period covers four general election cycles: 2008 (at which electronic voting technology will not be in use), 2011, 2014 and 2017.

3 Introduction

This draft strategy is the principal deliverable of the e-voting technology strategy project.

The draft strategy is supported by a series of working papers which set out the underlying research and justification for the positions and options proposed. For more detailed discussion, the working papers should be consulted – noting that the working papers are just that, and do not represent the draft strategy.

The draft strategy proposes a possible way forward for consideration by Ministers and senior managers, and does not represent Government policy.

3.1 Sources for this draft strategy

The draft strategy draws upon all the working papers in this series and the related steering group discussions.

The working papers are:

1. Strategic Context and Value;
2. Chief Electoral Office Voting Processes;
3. Technology Options and Opportunities;
4. Guiding Principles;
5. Legislative Analysis;
6. Future Business Model, Chief Electoral Office;
7. E-voting Issues; and
8. System Architecture, Integration & Requirements.

3.2 Glossary of common terms

Phrases used in this document have the following meanings:

Table 1, Glossary of common terms

Advance vote	A means of voting in the two and a half weeks before polling day if: the voter will be outside the electorate or overseas on election day; or is prevented by illness from going to a polling place; or their religion does not allow voting on a Saturday; or the voter can satisfy the Returning Officer or Issuing Officer that going to a polling place would cause hardship or serious inconvenience. An advance vote is a special vote. The voter shows in the declaration the grounds that apply.
Assistive technology	Hardware and/or software that helps people with disabilities to use information and communications technologies, e.g. by magnifying computer images, 'reading' aloud the material on a computer screen, or providing an alternative to keyboards.
Electronic counting	Vote counting using electronic means. Electronic counting of conventional paper ballots does not constitute e-voting for the purposes of this paper.
Electronic voting, e-voting	Voting at a general election or referendum that involves the use of electronic means in at least the casting of the vote.
Pilot	A small scale use of new methods and policies to cast real votes. Distinct from a 'test' or 'trial' which does not involve real votes in a genuine election.

Remote voting	Voting which takes place away from a supervised voting location.
Special declaration vote, special vote	A means of voting when the voter is outside their own electorate on election day, cannot get to a polling place, or is not found on the main or supplementary rolls. Overseas votes are a form of special vote. The voter shows in a declaration the grounds that apply.
Supervised voting	Under the direct management and oversight of electoral officials or election day workers.
Voting channel, channel	Method of casting and transmitting votes to ballot box (or e-ballot storage).

3.3 Glossary of Abbreviations and Acronyms

Abbreviations and Acronyms used in this document have the following meanings:

Table 2, Glossary of Abbreviations and Acronyms	
ACT	Australian Capital Territory
CEO	Chief Electoral Office
EEC	Electoral Enrolment Centre
EMS	Election management system
CESG	Communications-Electronics Security Group
GLS	Government Logon System
ICT	Information and communication technologies
IT	Information Technology
IVS	Identity Verification Service
ODIHR	Office for Democratic Institutions and Human Rights
OSCE	Organisation for Security and Co-operation in Europe
PCIN	Personal Candidate Identification Number
PIN	Personal Identification Number

RID	Response Identification
SMS TXT	Short message service text
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UK	United Kingdom
USA	United States of America
VEC	Victorian Electoral Commission
VVPAT	Voter Verified Paper Audit Trails
WORM	Write Once Read Many

4 Why consider electronic voting options?

There are a number of reasons why e-voting technologies could be considered for introduction in New Zealand.

From a democratic perspective there is potential to:

- Improve access to elections;
- Improve the quality of the voting experience for those voters who have difficulties with paper-based and polling place located services;
- Maintain or enhance trust and confidence by responding to societal changes (e.g., demands for choice and convenience), meeting expectations for electronic service delivery, and at the same time retaining traditional channels and electoral culture; and
- Reduce the likelihood that human error will invalidate a vote.

From an efficiency and effectiveness perspective, the introduction of e-voting technologies could:

- Continue the progression of electoral process and system enhancements and integration, through information and communication technologies (ICT);
- Enable long-term cost savings;
- Improve the accuracy of vote counting;
- Increase the speed of vote counting and the announcement of election results; and
- Build organisational knowledge and capability for electronic service delivery.

E-voting has the potential to contribute to Government goals[2]:

- The introduction of e-voting technologies would contribute (via the Ministry of Justice outcome of a fairer, more credible and more effective justice system) to each of the Government's priorities for the next decade:
  Economic transformation: supporting e-government and the Digital Strategy and using the associated all-of-government systems;
  Families young and old: enhancing opportunities for participation, access, and choice; and
  National identity: electoral processes that reflect and support New Zealand's democracy and society.

- The introduction of e-voting technologies would be consistent with, and support, the Digital Strategy. The introduction of e-voting technologies would enable for voting services the E-government 2020 milestone of: "people's engagement with the government will have been transformed, as increasingly innovative use is made of the opportunities offered by network technologies". The draft strategy reflects the characteristics of successful e-government: convenience and satisfaction; integration and efficiency; and trust and participation.

- The introduction of e-voting technologies could make a direct contribution to the development goals of the state sector, in particular: networked state services; co-ordinated state services; accessible state services; and trusted state services.

4.1 Why develop a Strategy to guide the introduction of e-voting technologies?

A strategy is required to guide the introduction of e-voting technologies in order to:

- Make the future direction visible to the public and all stakeholders;

- Provide direction to the electoral agencies who must be involved in investment, development, and integration;

- Ensure each short and medium term step makes a meaningful contribution to the achievement of long term goals;

- Reduce the risk of investment in options that may not add value in the longer term; and

- Identify measures that reduce the risk that a change to voting methods: disenfranchises voters; makes electoral fraud easier; disrupts an election; or leads to a loss of sovereignty[3].

4.2 E-voting when?

The draft strategy makes it clear that the implementation of trustworthy and trusted e-voting will take time. A cautious approach to the introduction of e-voting technology, based on carefully controlled pilots

[2] See the discussion in working paper 1, *Strategic context and value.*
[3] For example, by making New Zealand election outcomes susceptible to interference from outside New Zealand.

accompanied by review and decision steps, is proposed. Before the pilots can commence, there will need to be a period of extensive public consultation, and policy and legal work in support of new legislation.

E-voting pilots in real electoral environments must adhere to the three-year electoral cycle. The reality is that several cycles would be required before technical and procedural robustness was fully demonstrated and public trust established. The latter point may be the slower process. It would be a high risk approach to attempt to make up time by taking bigger steps over fewer electoral cycles.

Implementation timeframes are discussed further in a later section.

5 Current electoral and e-voting environment

Working paper 1, *Strategic Context & Value*, summarises the current situation in New Zealand and internationally. It concludes that the existing processes of the Chief Electoral Office are in fundamentally good shape. There is no crisis in the current voting system requiring urgent or radical change, but there are likely to be opportunities available to enhance access and participation. There is a very high level of public confidence that New Zealand general elections are administered fairly and vote counting is accurate. Most voters face no delays and the election night count of votes proceeds quickly.

Technology holds considerable promise to improve the achievement of voter goals, as well as public service goals for electoral administration. In many countries, considerable effort has been put into reviews and experiments to determine or confirm the feasibility and desirability of various options. New electronic technologies and processes have already been applied to other aspects of the electoral system, and their extension into voting, in the long term, is probably inevitable.

ICT applications to voting processes in New Zealand include:

- The register of electors is held on an electronic database, and a certain amount of data matching with other major public registers, as allowed by law, takes place;
- Members of the public can check their enrolment details online at the elections.org.nz website (though the process requires a signed paper document to finalise a change);
- The most popular means of requesting an enrolment pack prior to the last election was by short message service text (SMS TXT) message[4];
- The Chief Electoral Office uses an election management system (EMS) to assist the administration of elections. Details of parties, candidates, electoral districts, polling places, election staff, and results are collated and statistics are held on this system. It facilitates quick information to the media on election night;

[4] *Promoting participation: can a personalised message to the newly enrolled have an impact on turn-out?* Dr Helena Catt & Peter Northcote, NZ Electoral Commission, September 2006, http://www.elections.org.nz/uploads/voter_motivation_trial.pdf .

- www.elections.org.nz provides a large amount of information about the electoral process and New Zealand's parliamentary democracy;

- Ballot papers can be downloaded from www.elections.org.nz by overseas voters. In 2005, there were 20,931 individual downloads of New Zealand ballot papers by New Zealand electors in 150 countries;

- Political party secretaries can lodge their candidate details with the Chief Electoral Office via the Internet; and

- The work of the Representation Commission in reviewing electoral districts following the 2006 census was heavily supported by ICT.

Internationally, many electronic voting implementations of varying scales are already in place, addressing a variety of electoral problems or opportunities. A number of these are described in Appendix 6 to this paper.

Non-voting is an established and growing trend internationally, and while New Zealand turn-out is good by international comparison, the trend is nevertheless evident here. Poor turnout is considered to affect the legitimacy of democratic governments. Actions to counter or slow the trend have been common in developed countries in recent years.

It would be unwise, however, to expect the introduction of e-voting to result, by itself, in a lasting and significant improvement in turnout. Other factors, such as interest in politics, the habit of voting or not voting, and the closeness of a given election, can be expected to be more influential. Surveys indicate that specific groups within the electorate, such as youth voters, may respond positively to e-voting opportunities. E-voting should be regarded, however, as just one element of a preventative strategy to discourage further loss of turnout in future years.

Internationally, the introduction of e-voting technologies has not been "plain sailing". Ambitious plans for e-voting implementation have been scaled back or delayed in the United Kingdom (UK), following comprehensive pilots which have raised matters for further consideration, including the ability of local government bodies to implement change successfully. Reviews by a number of other Governments have resulted in a cautious approach and, in some cases, a decision not to proceed further at the present time.

The large scale, federally funded, push for change in the United States of America (USA) – mainly towards kiosk-style voting machines in polling places - has run up against growing public concern over transparency and auditability. Security analyses of popular commercial voting machines and Internet-based remote voting options have created a generally negative perception, at least in the USA and parts of Europe, of the security of systems dependent on electronic 'black boxes', the Internet, and home personal computers.

The prevailing international environment includes a significant element of mistrust and scepticism. This would need to be considered when designing communications and education policies and practices in advance of the commencement of any pilots. In introducing any forms of e-voting into

New Zealand, the risk of both genuine fraud and mischievous allegations of non-existent fraud would have to be carefully managed.

The 'bottom up' demand for Government services to be available on line is growing rapidly, as the public's access to Internet connections and mobile phones with Internet capability expands. New Zealanders appear willing to utilise the Internet for transactions with the Government sector. This is being encouraged and enabled by Government agencies. There is good reason to think that the growth trends evident in commercial Internet transactions will be echoed by the volumes of Government service transactions, and that public demands for access to Government services via the Internet will continue to climb.

"E-democracy' and 'e-participation' are concepts increasingly promoted by the United Nations and many Governments, including New Zealand's. The concepts are helping to shape the future relationship between citizens and their Governments. E-voting is recognised as an important means of implementing these concepts. Accordingly, Governments need to strive to move up the 'electronic participation' ladder, and at a relatively early point address e-voting options. For e-voting to be successful, however, high levels of trust must be extended by the electorate to the administrators of the electoral system.

6 Public attitudes

A public survey, conducted by the Electoral Commission as part of the development of this draft strategy, confirmed that a significant number of New Zealand voters (46 percent) would choose to vote online rather than at a polling place. However, a significant number of voters (39 percent) would not.

The survey results are attached as Appendix 1 to this draft strategy. The public attitudes expressed in this survey have been taken into account in developing the draft strategy – not least in respect of the proposal that e-voting should be only an optional and additional means of voting.

As a concept, voting over the Internet and the telephone is generally well received by the public. This support has been borne out in practice through experiments in the Netherlands, Switzerland, and the UK where such e-voting technologies had been introduced in addition to traditional voting methods. Convenience and simplicity are high rating reasons for voter support.

7 Guiding principles

7.1 Democratic principles

It is essential that any adoption of e-voting technologies respects all the principles of democratic elections and referenda.

International authorities tend to agree on four principles which give elections their democratic status and are equally applicable to traditional and electronically enabled elections and referendums. The principles and their meanings have been summarised as follows[5]:

- **Universal suffrage** – all human beings have the right to vote and to stand for election subject to certain conditions, for example: age and nationality;

- **Equal suffrage** – each voter has the same number of votes;

- **Free suffrage** – the voter has the right to form and to express his or her opinion in a free manner, without any coercion or undue influence; and

- **Secret suffrage** – the voter has the right to vote secretly as an individual, and the state has the duty to protect that right.

It is understood that there are trade-offs or balances to be struck between some of these principles. For example, it is acceptable for the secrecy of the ballot to be breached to a limited extent if a voter is unable to cast a vote without assistance; and the heightened potential for undue influence (for example, when voting from home) may be accepted if a voter would otherwise be unable to vote at all. The principles are therefore not absolute.

The greatest risks to these principles posed by e-voting are:

- Universal suffrage would not be achieved if certain forms of e-voting, for example, Internet voting, were the only means of voting available. Many voters would not want to use electronic voting, and others would not have ready access to, or the knowledge and confidence to use, e-voting channels;

- The secrecy of the ballot is subject to greater risk where the voter casts their vote in an unsupervised location. The voter's choice may be observed by others, or the ballot may be observable during transmission to the electronic ballot box; and

- Freedom from coercion or undue influence is difficult to guarantee when the voter casts their vote in an unsupervised location. The voter may be exposed to pressure from family members or others.

The draft strategy deals with these risks, because it is proposed that the voter should be able to use the Internet or the telephone from remote (i.e. unsupervised) locations of the voter's choice. Ways of dealing with these issues have been identified and are discussed in this draft strategy and the more detailed working papers[6]. The risks and mitigations are summarised briefly in Table 3 below

[5] Explanatory memorandum to the *Legal, Operational and Technical Standards for E-Voting*, Recommendation Rec (2004) 11, adopted by the Committee of Ministers of the Council of Europe, 30 September 2004, Council of Europe Publishing.
[6] See in particular working papers 7, *E-voting Issues* ,and 8, *System Architecture, Integration and Requirements.*

Table 3, Summary of e-voting system mitigations of issues affecting democratic principles		
Democratic principle	**Issue**	**Mitigations in draft e-voting strategy**
Universal suffrage	E-voting could be less accessible overall than conventional voting, and some voters would be less willing and/or less able to vote electronically.	E-voting would be optional.
		E-voting from location of choice enhances access for e-voters.
		Existing voting methods are maintained – no reduction in access to conventional voting.
Free suffrage	E-voters voting away from supervised polling places may be subject to coercion or undue influence.	E-voter can re-vote if the first has been cast under coercion or undue influence.
		Ability to choose the time and place to vote in order to avoid exposure to coercion or undue influence.
		Ability to vote in a supervised polling place (overriding any previous e-vote).
		Coercion and undue influence of an e-voter would be an offence.
Equal suffrage	E-voters may legitimately vote more than once (i.e. re-voting to redress coercion).	E-voting system would identify all votes by the same voter and ensure only one vote was counted.
	A voter might cast an e-vote and a conventional vote.	Paper votes and e-votes would be reconciled to identify multiple votes from the same voter, and ensure only one is counted.
	E-voters may have their votes changed or deleted before they are counted.	E-voters would be able to confirm that their votes had been received and stored, and were unaltered.
		Interference with e-votes would be an offence.
Secret suffrage	E-voters voting away from supervised polling places may be exposed to	E-voters have the ability to choose the time and place to vote – over several days - to avoid exposure to direct observation.
		E-voters would be instructed to vote alone

	greater risk of a breach of vote secrecy.	and secretly.
		Looking at or interfering with an e-vote would be an offence.
	The state has a duty to protect the secrecy of each voter's choice.	Supervised polling places and procedures to protect paper-based ballots would remain in place and available as at present. Potential e-voters would exercise personal responsibility to make a choice of voting method that protects secrecy and meets their needs and preferences.
	E-votes in transit may be intercepted.	Candidate and party lists would be randomly ordered on e-ballots, and all names removed in transit.
		Encryption for voter identity and ballot content. Transmission via the Internet using HTTPS[7].
		Intercepting e-votes would be an offence.
	E-ballots and voter identity might be electronically matched for other than lawful purposes.	Voter identity and vote content would be cryptographically scrambled. Separate cryptographic keys would be required to unscramble each set of data. The two keys would be held by different electoral officials to prevent potential matching by a single corrupt official.
		Each cryptographic key can be further divided between two or more officials to prevent unauthorised decoding by an individual.
		Matching ballots with voter identities for other than lawful purposes would be an offence.

The draft strategy suggests that e-voting as one channel in a suite of voting methods maintains democratic principles. The Chief Electoral Office can meet its democratic obligations by providing remote e-voting services *in addition to* supervised voting facilities. Use of e-voting would be optional. This would require the voter to take responsibility for deciding which channel to use in order to cast a vote that is convenient to them, private, and free from undue influence or coercion.

7.2 Electoral administration principles

The New Zealand Justice and Electoral Committee's *Report on its Inquiry into the 1999 General Election* (I.7C, 2001, pages 18-20) recommended that the Government encourage all electoral agencies and officials to

[7] HTTPS is an encryption protocol for exchanges over the Internet to prevent eavesdropping, tampering and message forgery. It is considered acceptable for commercial purposes.

observe the five electoral principles of: independence; neutrality; service to voters; candidates and parties; professionalism; and responsibility and accountability.

E-voting, including remote voting, can meet each of those principles. Consideration of electronic options would make a particular contribution to meeting the Committee's guidelines in relation to:

Table 4, E-voting contributions to good electoral administration

Principles	Select Committee Guidance	E-voting
Service to voters, candidates and parties	Electoral agencies: ▪ Provide the highest quality electoral services to all voters, candidates, and political parties in accordance with the law ▪ Provide electoral services to voters, candidates, and political parties in ways which are: as simple as possible; consistent with the law; and minimise compliance costs ▪ Ensure that all sections of the community have ready access to the electoral process in accordance with their needs	  
Professionalism	Electoral agencies: ▪ Continually evaluate their provision of electoral services and their internal and external procedures to ensure they: are in accordance with the law; are meeting users' needs; are as simple, efficient and effective as possible; and use appropriate information technology ▪ Keep up to date with best international democratic electoral practice	 
Responsibility and accountability	Electoral agencies: ▪ Make efficient and effective use of financial and other resources to carry out their statutory functions	

7.3 Standards

An e-voting system would adhere to the NZ E-government interoperability framework and authentication standards.

7.4 Adding value

An e-voting system should add value for:

- voters and the community;
- democracy and government; and
- electoral administration.

7.5 Balancing customer service and public values

The delivery of voting services is not simply a matter of meeting 'customer' demands. Because of the importance of the underlying democratic principles and the need to ensure the integrity of the electoral process, a balance must be sought between purely customer oriented values and the public values that citizens would expect from the electoral system.

The potential for improved access, service, convenience, and efficiency through e-voting must therefore be moderated by the need for security, reliability, accuracy, and integrity of the voting system.

8 What are the key characteristics of an e-voting system?

Any electoral system must be accessible to voters, whilst maintaining both their individual privacy and overall public confidence in the process. Electoral systems must be secure and should prevent such activities as: vote buying; voter intimidation; the altering, removal or insertion of votes; and the casting of multiple votes by a single voter. Electoral systems should also provide the means to produce reliable results, audit the election process, and to conduct a recount should a result be challenged.

Voting systems can be broken down into those where the act of voting occurs in a supervised or controlled environment (such as a polling booth) and those that occur in remote or uncontrolled environments (such as postal, telephone or Internet based voting). Both types of voting systems have their own technical and logistical challenges.

The main issues that must be addressed by any e-voting solution fall into the following categories:

- Verification of voter identity;
- The possibility of the e-voting device being compromised;
- Vulnerabilities in the ballot transmission channel, or network;
- Attacks on the e-voting infrastructure; and
- Trustworthy verification of the counted results.

In the case of e-voting, especially remote e-voting, the ability of modern technological devices to conduct millions of operations per second, or to exist unseen across hundreds or even thousands of computers, potentially opens the door for an individual to submit many thousands of fraudulent votes. This makes the verification of voter identity more important for a remote e-voting system than for other types of voting.

Electoral systems can be architected in such a way however, that it is possible to have a high degree of confidence in the results produced and at the very least to be able to detect widespread fraud or attacks upon the system, should these occur.

The e-voting infrastructure must be protected from attacks originating from the inside as well as the outside. Also, whilst voting and ballot

transmission processes must place an emphasis on voter privacy and preserving the integrity of the ballot, ballot receipt and processing systems should emphasise transparency, in order to build and maintain public confidence in these processes.

The draft strategy suggests that an e-voting system can be designed to meet these requirements, but must be subject to carefully managed implementation in order to demonstrate effectiveness and usability in real environments.

9 What would an e-voting service look like?

9.1 Sample voting architectures

Two e-voting systems with the ability to meet the challenges of remote electronic voting are described in Appendix 2. More detail is contained in working paper 8, *System Architecture, Integration and Requirements.*

The schemes are intended to illustrate possible approaches and are not complete solution designs. The architectures assume that e-voting takes place during a defined period in advance of election day. They are set out to follow the e-voting process through the main stages:

- Pre-registration for e-voters – confirming that the e-voter is on the electoral roll, generating an identifier for the voter within the electronic roll, and establishing appropriate log on credentials;
- Authentication of the voter, which assumes the use of the Government Logon System (GLS) – the GLS may not be appropriate for smaller or lower risk pilots;
- Casting the vote – the e-voter's correct electorate is determined from the roll and a randomised ballot is presented to the voter. The e-voter can print or save a receipt with a serial number but without parties or candidates identified;
- Ballot verification – the e-voter can contact the ballot verification system (in this example, the voter sends a text on their mobile phone or compares their ballot serial number to a copy on a public website) and checks that the vote stored in their name is correct; and
- Ballot count – a tamperproof 'write once read many' drive containing the encrypted ballots is disconnected from all networks in a controlled environment and unscrambling of the data takes place under scrutiny.

The architectures also describe the fault tolerance characteristics of the possible solutions.

9.2 Are the proposed architectures as reliable and secure as conventional voting?

A comparison of the two sample architectures against a reference architecture (in this case postal voting) helps establish whether each is as reliable and secure as elections that do not use electronic means. The comparison of architectures is attached as Appendix 3.

An e-voting system with the checks and balances described in this draft strategy and the accompanying working papers is capable of appropriate levels of reliability and security.

10 E-voting Issues

The main issues associated with the introduction of e-voting are set out in Working paper 7, *E-voting Issues*, as well as a number of the other working papers. These are summarised here.

10.1 Remote e-voting security risks and challenges

It would be inappropriate to be complacent about threat levels in New Zealand. It should be assumed that any New Zealand e-voting solution will be a target (whether of 'recreational' hackers or those with political, economic or criminal intentions) and it therefore needs to incorporate, from the outset, relatively sophisticated security measures. The system would also need to adapt to the changing security threat environment each time it was deployed, changed or expanded. New Zealand e-voting solutions should therefore be designed to produce results at least as free from electoral fraud and manipulation as conventional forms of voting at general elections. The opportunities for motivated parties, including crime syndicates, foreign governments, and overseas corporations (for example, technology suppliers), to improperly influence e-voting is however much greater than with paper based elections, and detection could potentially be more difficult.

As a result, security measures (along with other design requirements) could make an e-voting solution relatively complex for users. It would be necessary to confirm at key points in development, particularly in early tests and trials, that this has not resulted in barriers and costs that outweigh the original objectives and benefits - especially the goal of improving access to voting. Identification of a satisfactory balance between security and accessibility should be an objective of the development and pilot phases.

A 'life cycle' model of security should be adopted, covering information technology (IT), operational, and physical security. It should include security and privacy reviews or audits at key points. Security measures must recognise the risks of insider attacks during development and operation.

The draft strategy suggests that the implementation of remote e-voting should proceed initially through small and cautious steps, with thorough monitoring and evaluation. This would make the impact of any breaches small, and the likelihood of them being detected high.

Progress of the all-of-government GLS should be monitored, as it would provide many of the attributes required of a secure remote e-voting channel for larger numbers of voters.

10.2 The culture and significance of Election Day

A significant proportion of the voting population is likely to have a strong attachment to the community-based nature of current voting methods, and to place a high value on that aspect of electoral behaviour. Voting at

local polling places may also make a valuable contribution to social cohesion and the perceived value and significance of voting and democratic society. At the same time, new forms of community and social networks, such as online communities, are growing. While these may not currently have the same attributes or provide equivalent benefits for society, these too are likely to be highly valued by a certain segment of society.

The draft strategy does not actively promote a shift away from polling place voting. It would steadily build a platform for multi-channel voting in the future, so that the different voting preferences of most citizens can be catered for.

10.3 Is an e-vote a second-class vote?

Some commentators have suggested that, because it does not take place in the symbolic public space of the polling place and is relatively quick and easy, an e-vote may be debased compared to other votes, or cast without reflection. The popularity of text voting TV shows such as *New Zealand Idol* and *Dancing with the Stars* may enhance this perception.

The draft strategy takes the view that, if a person is sufficiently motivated and interested to vote, and is eligible, then access to the polls should be facilitated without presumptions about the supposed quality of the voter's choice. The suggested processes for e-voting would not result in voting that can be completed in a precipitate manner or on a whim.

10.4 Elections are increasingly on-line events

Elections in the future will have an increasing on-line presence. It would be a simple matter for e-voting services to be electronically linked with other services that add value for voters (such as enrolment processes or electoral information) in a 'one stop shop' approach.

It would be equally easy to provide electronic links to the web sites of political parties, pundits and candidates. However, an extremely cautious approach to the prospect of linking with other on-line sites and services is appropriate. Individuals, groups or organisations wishing to provide an electronic link to e-voting facilities should only be able to provide a link to Elections New Zealand (elections.org.nz); the site shared by the Chief Electoral Office, the Electoral Commission and the Electoral Enrolment Centre. From that point, re-direction to the voting service would follow the same steps for all e-voters.

The draft strategy suggests that an e-voting web site (or telephone voting service) should remain free from political or electioneering material in the same way that polling places currently do. Legislation to effect this may be appropriate.

10.5 Impact of advance e-voting

There are several reasons why the draft strategy suggests that e-voting should take place in the period prior to polling day. However, this is not ideal from the point of view that voters should be as well informed as possible prior to making their choices. Political campaigns are geared around maximising the impact of messages to voters close to polling day when most voting takes place. A shift in the number of voters who vote

before polling day would, if the number became sufficiently large, begin to change the dynamics of campaigns and political strategies.

The probable increase over time in advance voting is not an issue that arises solely because of e-voting – 8.5% of votes are already cast in the advance voting period – but the trend might be emphasised over time by the availability of e-voting channels. Voters currently have to have grounds to vote in advance. An advance e-voting option may increase pressure for the general availability of advance voting.

If advance e-voting was to cause concern because e-voters were unable to take into account all campaign developments up to election day, those concerns would be balanced by the proposal to allow e-voters to re-vote for any reason (with only the last vote counting).

10.6 Usability and accessibility

Usability has a big impact on the degree to which voters are confident that every vote counts. The e-voting experience should be as simple, easy, and error-proof as reasonably possible, for voters and administrators.

A single new voting channel would be unable to enhance access and usability across the full range of disadvantaged voters. The draft strategy therefore proposes two options: one computer based (Internet access), and the other telephone based. These options could be piloted at the same time (see Implementation Streams 1 and 2 in section 16.4). Experience in the UK suggests that there may be less demand for the telephone based option over time. However, it is the preferred option for many blind and vision impaired voters for the medium term, in the absence of widespread access to the Internet by that segment of the community.

A key objective of the proposed implementation strategy is to enable e-voting from remote locations in the first round of pilots. This is driven by access and usability considerations. Voters with disabilities would be able to use the telephone or computer set-up with which they were familiar, and in an environment in which they would be well-placed to assess and manage any threats to privacy or undue influence.

Prior to any detailed system design work relevant to usability and access, the draft strategy suggests focus groups to inform user-centred design of e-voting systems and interfaces. Field tests and trials are essential to properly identify and de-bug usability and access problems, and should be a feature of the implementation strategy. Good usability for people with disabilities will usually translate to good usability for all.

Any new e-voting system should allow for assistive technologies to be applied, especially those in common use in New Zealand (such as JAWS, the screen-reading/Braille programme often used by the blind and visually impaired). The e-census option in 2006 demonstrated that a high level of compatibility with home computers and Internet browsers can be achieved. The e-census did not attempt to deliver Te Reo in conjunction with assistive technology, but the potential demand for this feature among e-voting pilot users should be re-assessed in the design stage.

The metrics described in working paper 7, *E-voting Issues,* should be used to assess usability during trials and pilots.

Good usability will reduce the incidence of inadvertent invalid votes by all voters. Early investment in usability will be amply repaid, if e-voting is rolled out to larger numbers of users in the longer term.

10.7 Transparency

A feature of the current paper-based system is that key voting, vote storage, and counting processes are readily observable and there is tangible evidence of each vote, (see working paper 2, *Chief Electoral Office Voting Processes,* for a description). Election officials and scrutineers can see and understand what is happening at each step. Indeed, most of the administration is performed by temporary election workers who are peers of the voters. Courts can readily examine ballot papers and conduct recounts. The directly observable nature of the key voting steps encourages and supports a high degree of trust.

The same is not true of e-voting. For example, checking that each ballot box is empty to start with, and allowing each voter to physically place their vote into a sealed ballot box, are impossible with electronic votes. Other mechanisms must be used to underpin confidence and trust in the system. It becomes necessary to put considerable weight on aspects of system design and technology, and on the assessments of technical experts who can perform certifications and audits on behalf of the authorities and the public.

Features of an e-voting system that can enhance trust in the absence of direct transparency are listed in working paper 7, *E-voting Issues*. These include:

- Confirmation of the eligibility of an e-voter to a high degree of confidence;
- The ability of each e-voter to confirm that their vote has been placed in the e-ballot box, and is unchanged from the original intent;
- IT security practices and cryptography;
- As much openness as possible in system design and software code (to the extent conducive with good security);
- Physical security, independent audit, and observation (where relevant);
- Printing e-votes so that they can be incorporated into conventional post-election processes (scrutiny, counting etc) – at least in small scale pilots;
- Independent certification of software and systems to give assurance that they do what, and only what, they are intended to do; and
- The retention of overall judicial oversight.

An unavoidable outcome is that election administration (like many other facets of modern society) would become increasingly the province of specialists and technicians, and the conduct of elections would at least in

part be given over to Government agencies and businesses in ways that cannot be easily subject to scrutiny by the citizenry. Scrutiny and transparency mechanisms would of necessity also become more complex, but never-the-less capable of providing justified confidence. These could include independent certification and audit, and good quality statistical comparative analysis of sets of traditional and e-votes.

10.8 E-ballots and candidate/party order

The Electoral Act 1993 sets the order of the lists and the style of the paper ballots. The alphabetical approach and the layout are familiar to voters. However, there are at least two reasons why the current format might be changed.

First, an important security feature of the suggested e-voting architecture is the randomly ordered presentation of candidates. Rather than the current alphabetical presentation of candidates on the ballot paper (with the adjoining party list corresponding to the candidate on the same line), each e-voter would receive an e-ballot with an unpredictable order of candidates.

Second, while there would be benefits in maintaining a similar 'look' for paper and online ballots, good usability and error-proofing in the electronic context might suggest changes to layout. For example, keeping the paper ballot layout, which has the candidate selection boxes and the party selection boxes near each other down the centre of the ballot might induce errors when translated to an electronic context, with selection by 'pointing and clicking'.

Candidates and parties would be understandably interested in the resolution of these matters. Early development and testing of e-ballot format options (and the equivalent for telephone voters) with appropriate advice on usability would assist in setting the protocols for piloting. High levels of e-voter awareness and the ability to practice e-voting would be important implementation objectives.

10.9 The digital divide and e-voting

Certain groups in society, including people with disabilities, tend to be socially excluded. This means they may not have had opportunities to use the latest technology or to develop the confidence to learn new technology related skills. Other segments of the community make less use of network technologies for a variety of reasons. Age, location, education, and employment factors can all have a bearing.

The over-riding principle of the draft strategy is that existing voting methods should be maintained for the foreseeable future – no one will have reduced access to voting as a result of the introduction of e-voting. This position is taken in recognition of the high levels of accessibility provided by the current voting channels, and the uneven levels of access across the population to computers and the Internet.

An e-voting system which required all intending voters to have access to and confidence in using computers and the Internet, would result in a significant number of voters being disenfranchised. Various sections of the community with less access to network technologies have been identified in New Zealand studies (see working paper 7, *E-voting Issues*). Telephone

voting is therefore proposed for early pilots because standard touch tone telephones are widely distributed and accessible at this time. The impressive growth of mobile phones in New Zealand is noted in the working papers. However, in the view of representatives spoken to in the course of this project, this is not a particularly usable option at this time for many blind, vision-impaired or other people with disabilities.

It is suggested that pilots could also be conducted of Internet voting for those voters with disabilities with access to the Internet. These would be aimed at determining the technical fitness and usability of internet voting for people with disabilities, and act as a basis for extending the use of computer based voting to the wider population.

Piloting of moderate to large scale Internet voting, beginning with supervised e-voting in advance voting facilities, is signalled in 'stream 3' of the indicative implementation options (described later). Public Internet facilities, such as those at public libraries, may also be considered. The use of such facilities would overcome to some extent the problem of limited access to the Internet, while allowing computer-based e-voting for those who would prefer it to telephone or paper ballots.

Reliance on supervised access at dedicated facilities would provide a low risk environment for introducing the Internet voting option to a wider range of voters. It would also allow the Chief Electoral Office to review the economics and popularity of supervised Internet voting at selected locations. E-voting at all polling places is not favoured in this draft strategy on the grounds of high cost and limited benefits (see the discussion of 'voting machine' costs in an Appendix to working paper 1, *Strategic Context and Value*).

10.10 E-voting and trust

The draft strategy takes as its starting position that voting and vote counting processes at general elections in New Zealand are currently trusted by the public and other stakeholders. However, there is no room for complacency. Voter and stakeholder trust in the voting and vote-counting system can be influenced by other issues (unrelated to voting) affecting the trust of the wider community. A decline in public trust of the Government or its agencies for any reason, or a significant computer/Internet incident, could affect confidence in the voting process.

The draft strategy has been designed to ensure that each of the following questions, influential in establishing trust, can be answered in the affirmative:

- Are there valid reasons for making a change? Would e-voting create public value? Would voters be able to exercise their personal preference in this matter?

- Would all valid votes, and only valid votes, be counted accurately and fairly?

- Would potential risks and issues be properly mitigated and managed? Is the proposed system at least as trustworthy as the current system? Would reported problems be taken seriously and assistance provided?

- Is provision made for interested parties, including targeted users, to be involved in policy and design? Is there widespread understanding and acceptance among all stakeholders? Would there be ongoing monitoring, analysis and public reporting - especially prior to decisions to expand e-voting?

- Will the draft strategy be responsive to changing societal preferences and expectations?

10.11 Protection for secrecy and freedom from coercion/undue influence

The Bill of Rights Act 1993 expresses the electoral rights of New Zealand citizens, which include equal suffrage and secret ballots.

Traditionally the state has enabled secret ballots by providing supervised polling places with screened voting booths. Polling places are carefully laid out to protect privacy and prevent a voter's choice from being seen by others (for example, through windows behind the voter). The supervised environment also allows election officials to ensure that voters are not subjected to undue influence or coercion while in the act of voting. The Electoral Act 1993 describes a range of prohibited activities and creates offences to support the authorities in preventing undue influence and breaches of secrecy.

Protection of the privacy of the voter and the secrecy of the ballot, and the insulation of the voter from undue influence, cannot be provided by the state in the same way when voting takes place in an unsupervised location. It is suggested that the state's obligations can be met by:

- Ensuring that supervised voting continues to be provided;

- Allowing e-voters to cast another e-vote, or a vote in a polling place, if they feel they have been subject to coercion or undue influence while casting an e-ballot;

- Making it easy for e-voters to report incidents to the electoral authority;

- Creating offences applicable to e-voting circumstances; and

- Taking into account relevant balances or trade-offs.

A balance of risks and benefits is present when voters use the existing remote voting channels such as postal voting or facsimile voting. These forms of voting are exposed to the risk of loss of secrecy or undue influence in similar ways to remote e-voting, but the alternative of in-person polling place voting may create considerable inconvenience or hardship in voting, or result in loss of the opportunity to vote altogether.

The draft strategy suggests that voters with disabilities be the first to pilot e-voting services. This group is more likely to have degraded privacy and independence while voting conventionally, and the risks associated with e-voting must be considered relative to their current experience.

The experiences of this group in e-voting pilots and the risk/benefit trade-offs can be considered before a decision is made to maintain restricted access to e-voting or to widen its availability. The draft strategy allows a

cautious approach to be taken to establishing appropriate points of balance. Review and decision points are incorporated into the indicative implementation strategy.

10.12 The roles of the state and the voter in protecting rights

The draft strategy suggests a balance of responsibilities between the state and the electronic voter, which is similar to that for postal or facsimile voting. The remote voter must take responsibility for deciding when it is an appropriate time and place to vote to minimise the risk of their choices being observed or them being subject to undue influence by others. If the current advance voting period (17 days) is retained for e-voting, they will have ample opportunity to choose a suitable time.

The e-voter must also decide if the circumstances are such that it is more appropriate to use a conventional supervised polling place or advance voting facility.

In principle, e-voters would be no worse off, and are likely to be better off. They can have the benefits of increased choice and convenience, in which case they must exercise additional personal responsibility to guard their electoral rights; or they may use the conventional voting system where the authorities provide a high level of protection for those rights.

In practice, it would be inappropriate to be complacent about the potential risks. The survey attached at Appendix 1 specifically sought the views of the voting public regarding these matters, as there is little international or New Zealand research on the subject.

In response to the statement "*I would be confident that I could vote online without anyone seeing who I was voting for*", there was a strong split in views. 58% of respondents agreed, including 33% who strongly agreed. 13% were neutral. 27% disagreed, including 16% who strongly disagreed.

In response to the statement "*I would be confident that I could vote online without anyone else unduly influencing my vote*", a similar pattern emerged. 62% of respondents agreed, including 39% who strongly agreed. 12% were neutral. 24% disagreed, including 14% who strongly disagreed.

These results suggest the draft strategy is correct in placing weight on retaining existing supervised voting channels, where voters can have confidence that their choice is secret and the authorities provide protections from undue influence while voting. The strong expressions of confidence that online voters could maintain their rights of privacy and freedom from undue influence also support the concept that online voters could satisfactorily manage these aspects of e-voting.

Ensuring public awareness and understanding of this issue and of the mitigating features of the final strategy would be an important function of e-voting communications programmes.

10.13 Re-voting

Conventional supervised voting channels deal effectively with the risks of potential voter coercion and lack of privacy or secrecy. Remote voting channels need to solve the problem in another way, and an effective and

simple solution is to allow an e-voter the opportunity to vote again, either electronically or in person. This solution was used in the 2007 Internet voting system for the Estonia general election, and was recommended in the 2006 Norwegian Government electronic voting report[8].

The suggested practice does not breach the intent of the democratic principle that all voters should have the same number of votes (equal suffrage). A second or subsequent electronic vote would overrule any previous e-vote, and a polling place vote on election day would overrule any electronic vote(s). The design of the e-voting system would ensure only one vote, the last, is counted (the e-voting system would identify the vote *cast* last, as it may be possible for e-votes to be delayed in transit and arrive in the e-ballot storage in the wrong order).

The Estonian experience of re-voting in 2007 was that of the 31,064 votes cast over the Internet 789 were repeated votes (2.5%) and just 32 e-votes were subsequently cancelled by a paper ballot.[9]

Conventional voters might wonder whether re-voting should be available to them also. However, they are not subject to the same risk, and have no need to replace a vote made in a supervised polling place where they are free from coercion or undue influence. If a voter in a polling place makes an error while voting they can have a new ballot paper issued to them.

A remote electronic voter could be effectively disenfranchised if their vote was coerced. In the event this occurred, the voter should be free to vote again to ensure their true choice is recorded. If the risk of coercion remained in the e-voting location, the voter should be able to vote conventionally at a polling place. This would be possible because e-voting is proposed to take place in advance of election day.

An unusual pattern of re-voting might be investigated by the authorities if it appeared to be an attempt to lodge multiple votes.

Remote voters casting postal or facsimile votes are exposed to the same risk of coercion as e-voters, but paper based systems do not have the efficiency and accuracy to allow the same solution, i.e. identifying re-votes and determining which was cast last. It would be appropriate for voters using paper based remote votes to have an early opportunity to transition to e-voting systems.

10.14 Sovereignty and control

The self-determination and independence of New Zealand as a nation could conceivably be influenced through the manipulation of election results or the disruption of an election. Providers of goods and services for the e-voting system would be in an advantageous position to attempt this. It is therefore important that genuine control of any e-voting system should be in the hands of the Chief Electoral Office, with high levels of transparency and the capability to make thorough independent checks. In the event that system development, operation or hosting of the e-voting

[8] *Electronic voting – challenges and opportunities,* Norwegian Ministry of Local Government and Regional Development, February 2006.
[9] *Parliamentary elections 2007: Statistics of e-voting,* Estonian National Electoral Committee, Tallinn, 2007, available at http://www.vvk.ee/english/Ivoting_stat_eng.pdf.

system is undertaken by commercial parties for the Chief Electoral Office (which is likely in some degree), governance, control and understanding must be retained.

Overseas experience suggests that e-voting projects can become vendor-led if there are unreasonable time or resource constraints or a lack of management and oversight capacity in the electoral authority. This should be avoided.

Control would be more difficult to maintain, and may be beyond the reach of the Chief Electoral Office and New Zealand law if election data processing (for example, counting) or storage were to occur outside New Zealand. Outsourcing of election data processing to an organisation abroad would probably have the effect of making that data subject to the laws of the overseas country[10]. This would raise questions about the ability of the Chief Electoral Office to maintain the strict legal and procedural controls over the secrecy of votes and the matching of votes with voters. The transparency to the New Zealand public of voting and counting processes would also be affected.

Any personal information held in an e-voting system and the link between voter identity and the content of their vote must be thoroughly protected and remain within the ambit of New Zealand law. The draft strategy therefore suggests that providers of goods and services to develop or support the operation of an e-voting system: must be subject to New Zealand law; must hold or process election-related data only in New Zealand; and must not transfer any such data offshore. This may require legislative backing. Privacy impact assessments should form part of the development and ongoing operation of an e-voting system.

10.15 Open access to advance e-voting

E-votes are proposed to be cast in a defined period prior to election day. The Electoral Regulations currently provide for advance voting where a voter would otherwise face hardship or serious inconvenience. If e-voting is to be extended at some future point to voters who simply prefer to use the electronic channel and are not facing hardship or serious inconvenience, a change of policy would be required.

11 Policy and legislation

Voting in general elections and referenda by electronic means is not authorised by the Electoral Act 1993 or the Citizens Initiated Referenda Act 1993. Citizens initiated referenda can be conducted using remote postal voting because of the relatively lower risk attaching to referenda, compared to general elections and by-elections.

[10] The United States 'Patriot Act' 2001, in an effort to curb terrorism threats to the USA, requires companies served with a search warrant to disclose certain information (including computer data). The fact of disclosure of such information must not be disclosed. Potentially, New Zealand election data held by a company subject to the Patriot Act (i.e. with offices in the USA) would be at risk of disclosure to the American Government.

A number of challenging policy issues would need to be resolved prior to drafting legislation to enable electronic voting. These include:

- The operation of voting system pilots of an experimental nature in real elections;
- Whether e-voters should have the ability to re-vote, either electronically or conventionally at a polling place (with only the e-vote cast last, or the vote cast at a polling place, counting);
- The use of new ballot formats for electronic media, with random ordering of candidate and party lists on e-ballots;
- How to ensure sovereignty and control of electoral data and processing;
- Whether the ability to cast the electronic equivalents of advance and special declaration votes would remain subject to grounds such as being outside the electorate on polling day, hardship or serious inconvenience;
- The development of a formal framework for 'observers' of e-voting; and
- The introduction of a range of new offences.

It is possible that proposals for legislative change may include amendments to entrenched provisions in the Electoral Act 1993. These provisions can only be amended with a 75% majority of the House of the Representatives.

A two step approach to legislative change is suggested: firstly, making those amendments required to authorise the development and implementation of e-voting pilots on an explicitly small scale and experimental level; and secondly, making those amendments required to extend e-voting on a 'fully fledged' basis (including for use in citizens initiated referenda). Whether these latter amendments would be undertaken would be determined after consideration of the outcomes of the first step. By separating the two steps, it would not be possible for e-voting to evolve into a large scale voting method without explicit consideration and authorisation by Parliament. The lessons learned in the pilots would enable policy to be fine-tuned before more broadly applicable legislative amendments were put forward.

An analysis of a number of the relevant sections of the Electoral Act 1993 has been undertaken. This is found in working paper 5, *E-voting Legislative Analysis.* The analysis does not include the Electoral Regulations 1996, and does not extend to the new matters that would need to be provided for legislatively. This would be a significant body of work.

12 What would it cost to implement an e-voting system?

12.1 Estimates

- Withheld: sections 9(2)(f)(iv) and 9(2)(i) Official Information Act 1982

12.2 Cost reasonableness check

- Withheld: sections 9(2)(f)(iv) and 9(2)(i) Official Information Act 1982

13 Non-financial benefits from e-voting

A wide range of non-financial but valuable benefits are available from the introduction of e-voting technologies.

Voter and community benefits:

- Access, privacy and independence can be enhanced for blind and vision-impaired voters – this is a suggested top priority. This facility also enhances access for voters with reading difficulties;
- Access, privacy and independence can be enhanced for other voters with disabilities – this is a suggested top priority;
- Access can be improved for voters with restricted mobility, difficulty using a pen, or difficulties in attending polling places or voting on election day (including care-givers);
- Ease of voting and convenience can be enhanced for voters who would otherwise have to use special declaration voting procedures – this is a suggested second priority;
- A choice of channels can be provided to reflect modern lifestyles, preferences and time pressures, and recognise voters who relate to online communities. This is expected to be a growing segment of voters. This is a possible long term outcome;
- Access can be enhanced for voters who are not proficient in the official languages;
- Voter errors or omissions on ballots or special declarations that could invalidate votes can be reduced; and
- Access and convenience can be improved for overseas voters and participation might be improved for a potentially large group of overseas non-voters.

Benefits to democracy and Government:

- Ensuring that a limited range of voting methods does not become a future contributor to decreasing participation in general elections in an increasingly technological society, and supporting efforts to promote greater participation;
- Supporting the Digital Strategy by "connecting people to things that matter to them", bringing isolated groups into the political life of the nation, and closing the growing gap to leading nations in applying technology to electoral processes;
- Supporting the NZ Disability Strategy by underpinning voting rights for people with disabilities, fostering responsive services, and promoting participation;

- Providing a highly visible example of e-Government and transformational change, using technology to provide user-centred services;

- Improving public trust in general elections by a combination of improved accessibility, responsiveness to shifting public preferences, and the availability of multiple channels providing choice and increased convenience for voters. Conversely public trust could be negatively affected if widespread voter preferences are not responded to in a timely way;

- Improving the certainty of election outcomes by enabling speedy counting of special declaration votes;

- Using the all-of-government GLS for larger scale e-voting implementations; and

- Contributing to the state sector development goals, particularly accessible state services, trusted state services, coordinated state agencies, and networked state services.

Operational benefits:

- Step-by-step development and pilots allow new policies and processes to be tested and tuned in an environment of low operational, financial, and political risk;

- Resources can be released for other priority programmes such as improved electoral participation by hard-to-reach groups;

- Enabling a logical progression of technology from other electoral processes (ICT solutions are already in place for voter registration, the roll, 'download and fax' voting, the administration of the election, media and public access to election results, public access to election agency information, etc.);

- Enhanced integration of systems across electoral agencies and improved leverage of existing investments (for example, electronic roll, www.elections.org.nz web site);

- Quicker and more accurate vote counting;

- Improved security and voter authentication compared to existing remote voting methods (postal, facsimile);

- Increased depth and robustness of Chief Electoral Office capabilities (for example, ICT) to deliver future electoral services and respond to new technologies;

- New Chief Electoral Office capabilities (for example, usability of electronic voting interfaces) developed in a low risk organic manner;

- Potential future efficiencies facilitated (for example, electronic counting of paper ballots);

- Pre-registration for e-voting would provide an additional opportunity to update voter contact details and assist enrolment and communication activities; and

- Building a knowledge base for future technology implementations.

14 Savings accruing from the implementation of an e-voting system

The application of technology (with the associated investments in development and implementation) will unlock future fiscal savings in the delivery of elections. However, savings will not be achieved in the smaller scale pilots suggested as first steps.

As the implementation of an e-voting system progresses, savings can be accessed by facilitating the transfer from high-cost special declaration votes[11] to e-votes. The expenditure that could be reduced (i.e., the variable field cost) by the elimination of one special vote is three times that of an ordinary vote. Special votes are therefore a potential priority target for cost efficiencies related to e-voting.

The estimated total (three year) cost of special vote services at the 2005 election was $4.95 million. However, there are practical constraints on the levels of cost saving achievable by e-voting:

- Personnel cost reductions do not become achievable until certain trigger points are reached in the reduction of special vote volumes (a special vote issuing officer position cannot be eliminated unless a reduction of about 70 special votes is achieved at a given polling place);

- Paper-based special vote services must be retained for those who do not wish to vote electronically, or do not have ready access to the Internet; and

- A large proportion of polling places have low levels of staffing[12] and further personnel reductions are not achievable (over half of all special votes are cast at smaller polling places).

Levels of realisable savings based on 2005 costs are estimated below, assuming that the full variable field cost of special votes can be saved at larger polling places ($11.89 per special vote), and only the variable cost of field supplies - ballot papers etc – ($3.41 per special vote) can be saved at smaller polling places.

[11] The cost structure of the Chief Electoral Office and the main types of paper-based ballot are discussed in working paper 6, *Future Business Model, Chief Electoral Office.*
[12] Chief Electoral Office statistics record that in 2005 there were 1522 polling places with only two or three staff.

Table 5, Estimate of realisable savings – special votes	
Reduction in the volume of special declaration votes	**Estimated cost saving per election (2005 values)**
20 percent reduction	$370,000
40 percent reduction	$740,000
60 percent reduction	$1.1 million

If e-voting becomes generally available, future savings would also accrue from the transfer of ordinary votes to e-votes. The variable field cost of an ordinary vote is estimated at $3.84 per vote (2005). Such savings would be cumulative with special vote savings. (While advance ordinary votes would also transfer to e-votes, available savings would be limited for reasons similar to those noted above for special votes in small polling places).

Table 5, Estimate of realisable savings – ordinary votes	
Reduction in the volume of ordinary votes	**Estimated cost saving per election (2005 values)**
10 percent reduction	$787,000
20 percent reduction	$1.57 million
40 percent reduction	$3.15 million
Assumes 2.05 million ordinary votes (2005 election) @ $3.84 per vote	

Thus an e-voting implementation that resulted in – for example - a 40 percent reduction in special votes and a 20 percent reduction in ordinary votes would save $2.31 million per election, and if 60 percent of special votes and 40 percent of ordinary votes transferred to e-votes the estimated saving would be $4.25 million per election (based on 2005 data).

These high level estimates do not replace the need for a more detailed assessment of costs and benefits prior to any specific investment in e-voting.

15 Impacts of not proceeding

The impacts of not proceeding with the introduction of e-voting technologies would include:

- A perception that the Chief Electoral Office is not implementing certain Ministry of Justice and Government strategies;
- Opportunities to enhance services to voters being delayed or lost;
- Opportunities to increase access or improve the voting experience for blind/vision impaired people and people with other disabilities being delayed or lost;
- Opportunities for developing possible technological responses to declining voter turnout being delayed or lost;
- The process of capability building within the Chief Electoral Office being delayed, affecting future implementation of new technologies and increasing operational risk;
- The process of legislative change not being commenced in a timely manner, affecting future implementation timeframes; and
- Opportunities for future cost savings and efficiency improvements being delayed or lost.

16 Implementation strategy

16.1 A flexible approach based on risk management and proportionality

The draft strategy incorporates the principles of ongoing risk management and proportionality. There are a range of mechanisms available to respond to e-voting risks and issues and, in some cases, they can be applied to different degrees. The extent to which the various mechanisms are applied during implementation should reflect the objectives and the risks of the specific implementation. For example, a small scale implementation with a known group of volunteer e-voters in a closely monitored pilot would not require the same level of voter online identity authentication as a larger scale implementation open to many voters. Solutions could range from a user name and password in a low risk pilot, to a user name and password plus a one-time password supplied by SMS TXT message to the voter's mobile phone for a 'higher strength' authentication.

A lower security version of the telephone voting infrastructure is outlined in the final section of Appendix 2.

A cautious step-by-step approach should be adopted for implementation. Technical features, procedures, usability, and public attitudes should be carefully tested through small scale pilots in low risk environments and carefully reviewed, before being applied on a larger scale. A 'big bang' approach to new voting methods should be avoided.

16.2 E-voting pilots

Pilots should form an important part of the development process. They allow the impacts of new policies and delivery mechanisms to be tested in a carefully controlled and monitored manner, and in a spirit of experimentation. Each pilot should have clear technical objectives. There should be no pressure to deliver specific outcomes, but pilots should bring out any weaknesses and areas for further work. A decision to discontinue with remote e-voting would be a valid possible outcome of a pilot programme.

E-voting technologies would be relevant to referenda, but their infrequency and relatively short notice for preparation would make it difficult to use referenda for pilots.

16.3 Adding value

Even a small scale pilot can add value in its own right – for example improving access to elections for a specific group of voters (or non-voters). It is therefore suggested that a value-based approach should be applied to the selection and priority of pilots. The first pilots would therefore focus on blind and vision impaired voters, and other voters with disabilities. The next phase would focus on reducing the volume of high-cost special declaration votes and the third phase would build on earlier learning to make e-voting generally available.

16.4 Indicative implementation approach

The following three diagrams illustrate a possible implementation approach. The approach is indicative only. Three development streams are outlined – telephone voting for voters with disabilities, Internet voting for a similar target group, and Internet voting for special declaration voters – and key features of the programme of pilots set out. Indicative development paths are shown, up to the point that a significant number of special declaration voters and advance voters could be involved.

In the diagrams, the 'impact objective' described for each development stream is the intended effect for the target voters, and the 'process objective' is the intended learning relating to the method of delivery and the technology.

The diagrams follow a pattern of tightly defined, small scale, e-voting pilots, followed by an expanded pilot or a limited roll-out, and finally a larger roll out. There is a review and decision point after each step. This ensures risks and problem areas are identified and fixed before any further expansion of the e-voting system. It would also be possible to accelerate implementation or increase/decrease the scale of the next step, as a result of the reviews.

The suggested implementation approach contributes to electoral goals at each step. Stream 1, the telephone based 'limited pilot', (see the following diagrams), delivers improved access to voting for a volunteer sample of blind voters. It is also a demonstrable response to specific requests for e-voting from representatives of blind and vision impaired persons. The roll-out stage allows other voters with disabilities access to the (now proven) system. Similar steps would also be followed in respect of the

implementation of an Internet based system targeting the same users. This is Stream 2, which again starts from a small scale.

Stream 3 targets a different user group. It would focus on high cost special declaration vote services, with the two objectives of firstly, reducing the compliance burden on voters (the additional witnessed declaration) and administrators; and secondly, enabling savings in later elections. It is suggested that Stream 3 start one election cycle after Stream 2, building on the results of that development stream. However, there is flexibility around this point.

Stream 3 reflects the cautious view that a more widely available e-voting system (compared to the targeted user groups in Streams 1 and 2) should commence in supervised environments – probably a limited number of advance voting facilities which could utilise a private telecommunications network (rather than the Internet). This would have the benefits of: firstly, introducing the system to the general public in a low risk environment, and secondly, familiarising the general public (through communications programmes) with the concept of e-voting before moving, in later election cycles, to unsupervised voting via the Internet.

The key assumption underpinning Stream 3 is that public acceptance will lag behind technical capability. Whether Stream 3 is overly cautious in its design would be tested in reviews and user/public surveys undertaken in association with the pilots. It is noted in the accompanying text to the Stream 3 diagram that the second election cycle could move to unsupervised voting via the Internet, if that was in keeping with public demand and acceptance. By this time, Stream 2 would have tested key Internet based remote voting concepts and systems, and the GLS would be well-established.

A future full roll-out (unrestricted access to e-voting) is considered to be beyond the timeframe of this draft strategy, i.e. 2020 or later. It would be dependent on a policy decision that the electronic equivalent of advance and/or special votes would no longer be restricted to special circumstances such as voter hardship or being outside the electorate on polling day. This decision need not be made until the impact and implications of smaller scale e-voting have been considered.

The following diagrams are for illustrative purposes and do not represent detailed designs or the full range of possible implementation options. There is flexibility in, and between, possible e-voting development streams depending on the circumstances, for example: available funding; the outcomes of any public discussion prior to pilots commencing; and the results of ongoing evaluation as the pilots progress.

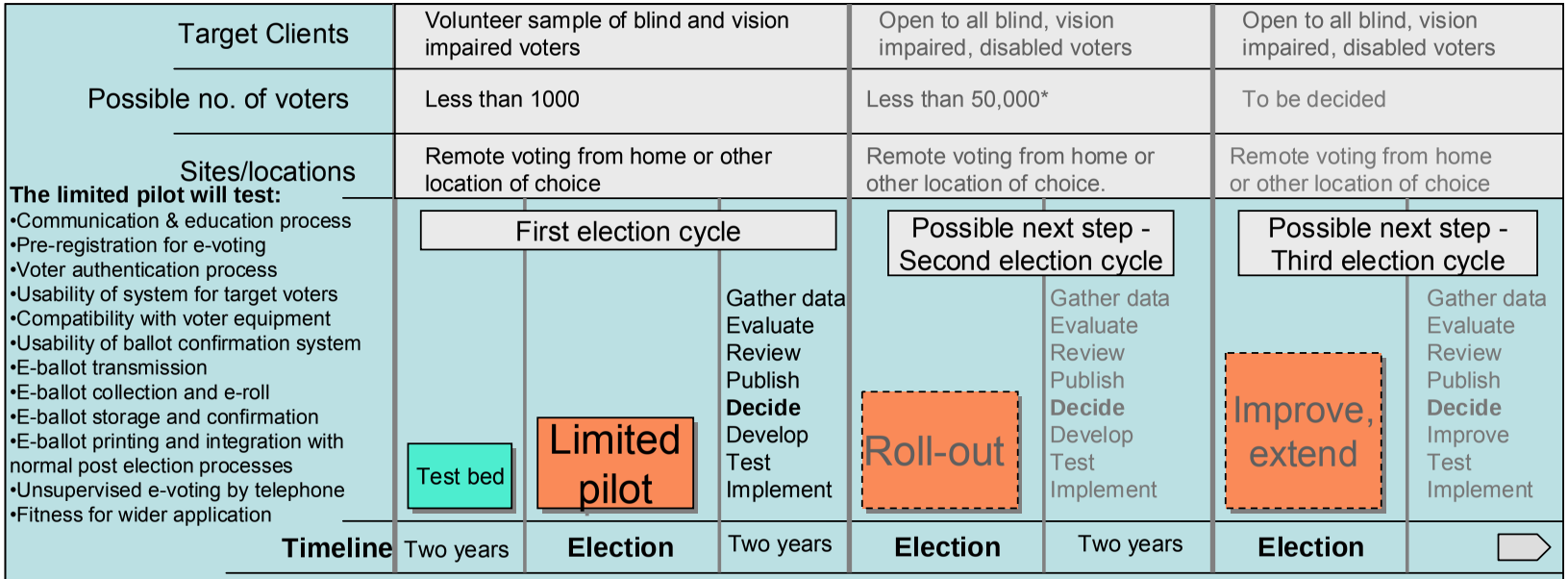
Draft E-Voting Technology Strategy – Indicative Implementation Approach

STREAM: 1 Telephone-based

Impact objective: Enhanced independence and access for blind and vision-impaired voters without internet access.

Process objective: Determine technical fitness and usability of telephone-based voting for blind and vision impaired voters

Development path: Extension to all voters with disabilities who prefer the telephone option; consider availability to all voters.



Discussion

It is suggested that the limited pilot of telephone voting commence with remote voting rather than supervised voting (at an official location) so that voters can use familiar telephone equipment in a location that is accessible to them. The number of pilot voters in the first cycle would be restricted to reduce risk and allow enhanced support and monitoring.

Telephone voting would take place in the advance voting period, giving plenty of opportunities for voters to choose a time when they can vote privately. In the event that a voter felt they were subject to undue influence or coercion, or their vote may not be secret, they would be able to vote (paper ballot) in a supervised advance vote facility or polling place. A small number of e-voters could be asked to re-vote to test that function.

An identity risk analysis would determine the level of online authentication required. Care would be needed to ensure the authentication requirements (password etc) remained user-friendly for the target clients. Explanatory material and instructions would need to be provided in the form preferred by the voters. E-ballots may be printed for integration with normal post-election scrutiny and counting processes.

System design and development should include representative users, and the test period should include practice opportunities.

Subject to satisfactory assessment the telephone voting option could be made more widely available to voters with disabilities in the second election cycle. In the assessment of the second cycle, a decision could be made on whether telephone voting should be made available to voters generally.

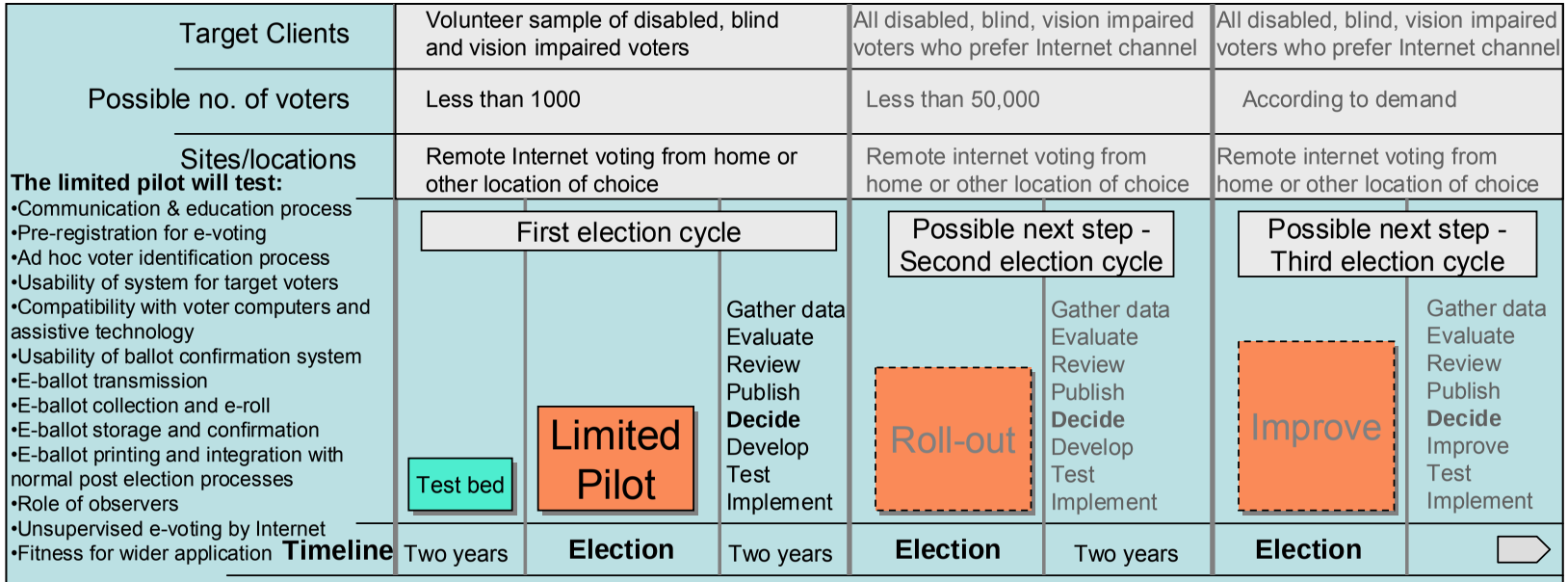
* The estimate of possible voter numbers in cycle 2 represents about 50 percent of the number of adults recorded as blind or vision impaired in the 2001 census.

STREAM: 2 Internet-based, small scale

Impact objective: Enhanced independence, access and choice for blind, vision-impaired and disabled voters with internet access.

Process objective: Determine technical fitness and usability of internet-based voting for blind, vision impaired and disabled voters.

Development path: Extension to all disabled voters who prefer the Internet option; foundation for Stream 3 – see following.



Discussion

It is suggested that the limited pilot of Internet voting commence with remote voting rather than supervised (at an official location) so that voters can use familiar computer equipment, including assistive technology such as screen readers, in an accessible location. The number of pilot voters in the first cycle would be restricted to reduce risk and allow enhanced support and monitoring.

Pre-registration would be required. Internet voting would take place in the advance voting period, giving plenty of opportunities for voters to choose a time when they can vote privately. In the event that a voter felt they were subject to undue influence or coercion, or would have difficulty keeping their vote secret, they would be able to vote in a supervised advance vote facility or polling place. A small number of e-voters could be asked to re-vote to test that function. E-ballots may be printed for integration with normal post-election scrutiny and counting processes.

An identity risk analysis would determine the level of online authentication required. Care would be needed to ensure the authentication requirements (password etc) remained user-friendly for the target clients. Explanatory material and instructions would need to be provided in the form preferred by the voters. System design and development should include representative users, and the test period should include practice opportunities. Subject to satisfactory assessment, the Internet voting option could be made openly available to all voters with disabilities in the second election cycle.

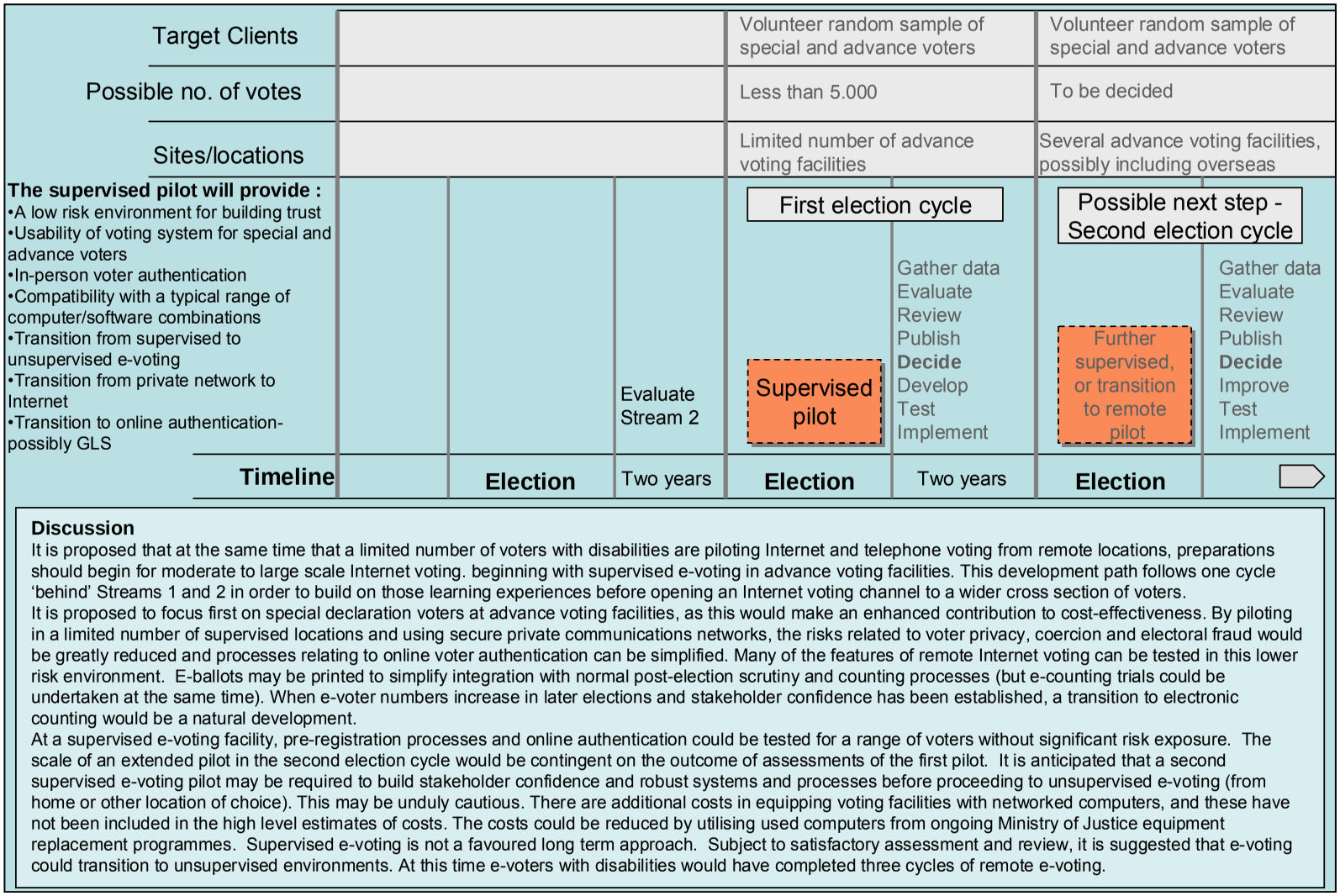
Experience with this Stream would provide the foundation for other potential Internet voters - see Stream 3.

STREAM: 3 E-voting, supervised, exposure to wider public

Impact objective: Easier and quicker voting for special declaration voters; build wider stakeholder confidence; enable future cost-efficiency gains.

Process objective: Building on Stream 2, usability of e-voting for a general audience, and transition from supervised to unsupervised e-voting.

Development path: Extension to all special and advance voters who prefer the Internet voting option, allowing consideration of future 'open' access.



Discussion

It is proposed that at the same time that a limited number of voters with disabilities are piloting Internet and telephone voting from remote locations, preparations should begin for moderate to large scale Internet voting. beginning with supervised e-voting in advance voting facilities. This development path follows one cycle 'behind' Streams 1 and 2 in order to build on those learning experiences before opening an Internet voting channel to a wider cross section of voters.

It is proposed to focus first on special declaration voters at advance voting facilities, as this would make an enhanced contribution to cost-effectiveness. By piloting in a limited number of supervised locations and using secure private communications networks, the risks related to voter privacy, coercion and electoral fraud would be greatly reduced and processes relating to online voter authentication can be simplified. Many of the features of remote Internet voting can be tested in this lower risk environment. E-ballots may be printed to simplify integration with normal post-election scrutiny and counting processes (but e-counting trials could be undertaken at the same time). When e-voter numbers increase in later elections and stakeholder confidence has been established, a transition to electronic counting would be a natural development.

At a supervised e-voting facility, pre-registration processes and online authentication could be tested for a range of voters without significant risk exposure. The scale of an extended pilot in the second election cycle would be contingent on the outcome of assessments of the first pilot. It is anticipated that a second supervised e-voting pilot may be required to build stakeholder confidence and robust systems and processes before proceeding to unsupervised e-voting (from home or other location of choice). This may be unduly cautious. There are additional costs in equipping voting facilities with networked computers, and these have not been included in the high level estimates of costs. The costs could be reduced by utilising used computers from ongoing Ministry of Justice equipment replacement programmes. Supervised e-voting is not a favoured long term approach. Subject to satisfactory assessment and review, it is suggested that e-voting could transition to unsupervised environments. At this time e-voters with disabilities would have completed three cycles of remote e-voting.

16.5 Evaluation of the implementation strategy

Working paper 4, *Guiding Principles,* discusses evaluation and identifies appropriate evaluation criteria for e-voting pilots, based on UK experience and the requirements of the UK Electoral Commission's statute.

Table 7, Evaluation criteria for e-voting pilots
The scheme's success or otherwise in facilitating access to voting and participation in elections
Whether the turnout of voters was higher than it would have been if the scheme had not applied
Whether voters found the procedures provided for their assistance by the scheme easy to use
Whether the procedures provided for by the scheme led to any increase in personation or other electoral offences, or in any other malpractice in connection with elections
Whether those procedures led to any increase in expenditure, or to any savings, by electoral agencies
The extent to which the scheme facilitated or otherwise encouraged participation among particular communities, including young people, Maori and minority ethnic groups, and people with disabilities
Overall levels of user awareness and comprehension of the voting method being tested, including an assessment of the effectiveness of any literature or other materials used in the promotion of the pilot
The attitudes and opinions of key stakeholders, including voters, with a view to determining overall levels of confidence in the voting method being tested
Whether the pilot resulted in measurable improvements, or had any adverse impact, with respect to the provision of more efficient and effective service delivery to voters.
Whether the pilot resulted in measurable improvements to, or had any adverse impact on, the existing system of electoral administration.
Whether the pilot represented good value for money.

16.6 Communications

Consultation with the general public on the implementation strategy would be desirable. Public acceptance of e-voting as a credible, reliable and secure addition to the New Zealand electoral system will be critical for achieving successful implementation.

The challenge is to build a constituency, set expectations, and maintain public confidence, without creating unreasonable expectations or

demands, or undermining the credibility of the current electoral system. It will be important to develop communications and public education activities appropriate to the different stages of the three development streams.

Communications activity to support the implementation strategy would need to include a balance of:

- Strategic positioning of e-voting:
    - Providing benefits to voters
    - Enabling future voter demands to be met
    - As an evolution of the electoral process
    - As part of the Government's E-Government Strategy;
- Explaining why there would be no immediate large scale implementation of e-voting, in a manner that builds confidence in the proposed system and any future developments;
- Building a constituency of support from experts, commentators, interest groups and the public. This will help with informed debate and discussion about the implementation strategy;
- General awareness raising amongst the wider community; and
- Specific education and communications activity for the target groups who will use e-voting.

Key audiences will include:

- Targeted disability groups, individuals and caregivers – i.e., those who would experience e-voting in the first pilots;
- Political parties and politicians;
- Policy makers, commentators and political scientists;
- IT experts;
- Political media, disability media, IT media; and
- The general public.

Regular engagement with these groups – whether formally through a working group or informally through regular updates - would be needed. It may be effective to run e-voting seminars to engage these groups and keep them aware of the process. Regular updates to the public and media pitched at the right level and frequency would support an open and evolutionary approach to e-voting.

A major communications and public education exercise would support the implementation of e-voting. This would focus on ensuring that those targeted for using the particular e-voting system are fully informed of its existence and how to access it. Wider general communications activity would also support the roll out. This general communication could include expert analysis from technical and electoral experts, and draw on overseas experience as appropriate.

16.7 Implementation timeframe issues

Appendix 5 shows two indicative implementation timeframes. The first shows a possible timeline for a pilot implementation at the 2011 general election, and the second shows a possible timeline for a pilot in 2014.

The timelines both assume the e-voting pilot – though small in scale – would be relatively fully featured to enable testing and learning in relation to many of the elements of a larger future service. A minimum 18 months development time (including tendering and certification processes) is assumed, but there would be more certainty after system tenders had been received.

16.7.1 Scenario: pilot in 2011

The timelines reveal a period of high demands on the Chief Electoral Office from late 2007 to early 2009. To achieve a pilot in 2011, it would be necessary to obtain Government approval for further legal analysis, policy development (including public consultation), and legislative drafting work to take place during 2008. This would enable Parliament to consider and pass enabling legislation during 2009. Budget approval for expenditure associated with this work would be required. In this scenario, technical work on the pilot would commence in parallel with the passage of legislation in order to be complete by the time electoral systems are frozen[13] in late 2010. Budget approval would be required in 2009 for expenditure associated with this work. This timeline assumes policy continuity into the term of the next Parliament.

In this scenario, there is a period commencing late 2007 and going through until early 2009 of intense policy-related demands on the Chief Electoral Office. This coincides with the mission-critical delivery of the 2008 general election. To manage this risk and deliver good quality policy development for e-voting, it would be necessary to provide sufficient resource and management capability for the project to proceed without impinging unduly on the other work streams of the Office. This would not be possible at current (2007) staff levels. Unforeseen electoral events such as by-elections or referenda in 2008 and 2009 would increase project and operational risks.

This scenario would reduce the risk that public demand for electronic voting channels would get well ahead of readiness, and enable early benefits to be gained. Potential e-voters are likely to expect a 2011 pilot to be easily achievable. The Chief Electoral Office would be perceived to be supporting e-Government initiatives and the state sector development goals.

16.7.2 Scenario: pilot in 2014

To achieve an e-voting pilot in 2014, Government policy approval would not be required until 2009. Further legal analysis, policy development (including public consultation), and legislative drafting work would take

[13] Development and improvement work on electoral systems ceases at the end of the calendar year before a general election. This is a good business practice to ensure systems and procedures are stable and documented, the field structure can be rolled out, and election worker training refers to the correct procedures. This planning assumes the election could be held from July onward in election year.

place during 2009, which would enable Parliament to consider and pass enabling legislation during 2010. Budget approval for expenditure associated with this work would be required. Technical work on the pilot would commence after the passage of the enabling legislation, finishing in 2012. Budget approval would be required in 2010 for expenditure associated with this work. In 2013, the Chief Electoral Office's procedures could be integrated and amended. This timeline leaves key policy decisions till after the 2008 election.

In this scenario, the development of e-voting policy and legislative options does not coincide with the late 2007 – early 2009 period of intense demands on the Chief Electoral Office or the delivery of the 2008 general election.

E-voting work streams through 2009 to 2013 should allow a 2014 pilot to be prepared with low project risk. Compared to the 2011 scenario, the additional resource and management requirements for the project would be reduced, but would still exceed current (2007) levels. There would be an increased risk that voter demands for electronic channels would get well ahead of readiness. Opportunities to accelerate subsequent development would be limited by the 3 year electoral cycle and the need to retain a cautious step-by-step approach. The Chief Electoral Office's support for e-Government initiatives could be perceived to be low.

16.8 Implementation Strategy - risks

The greatest risks to the successful implementation of e-voting are:

- The negative sentiments and scepticism associated with some overseas implementations could gain early hold in public debate, affecting public trust and confidence in the electoral system;
- An e-voting development stream is insufficiently funded, or is not properly structured, and becomes a threat to Chief Electoral Office mission-critical election services;
- Implementation proceeds faster than public acceptance, and confidence and trust in the electoral system is reduced;
- Users are not involved in design and testing, and poor usability affects system credibility;
- Early pilots are perceived as failures, and the overall concept loses credibility;
- There is insufficient openness in the development, operation and review of pilots, limiting public discussion and creating mistrust; and
- There are delays to implementation, with public expectations and voter demand moving substantially ahead of the Chief Electoral Office's ability to deliver e-voting.

These risks have been taken into account in the development of the implementation strategy, which tends towards caution.

17 Conclusions

It is suggested in the draft e-voting strategy that multi-channel voting be adopted for New Zealand general elections and referenda. The draft strategy documents a cautious step-by-step approach towards the introduction of e-voting as an additional and optional voting method. Existing voting methods would remain available for the foreseeable future.

The long-term objective of e-voting would be determined through a process of piloting and evaluation. E-voting could become a specialised voting channel for defined groups of users (such as blind and vision impaired voters, other voters with disabilities, and voters currently using special declaration votes); or a general channel available to all voters. It could even be discontinued. The choice can remain open while pilots are assessed. This would include consideration of voter experiences and public attitudes.

The draft strategy suggests that remote unsupervised e-voting be targeted from the outset as the key to future accessibility, convenience and voter choice. This pathway poses special challenges to democratic principles (in particular, the secrecy of the vote and freedom from coercion) that must be met with a high degree of assurance.

The risks associated with electronic forms of voting are real, and must be balanced with thorough mitigations and careful monitoring. Solutions are relatively complex and costly, and must be carefully tested for user-friendliness and transparency.

A clear implementation strategy using a stepped approach is suggested. It incorporates public awareness and information programmes, aimed at enabling the public to reach informed views and maintain high levels of confidence in the administration of elections.

The implementation strategy consists of three development streams, featuring e-voting pilots in real electoral environments. This is the best means of making progress, while managing the challenges involved in developing e-voting technologies. Users would be involved from the outset to ensure that a high degree of usability is designed into each pilot. Each pilot would be followed by a careful and open evaluation, review and decision phase. The components of each development stream and the rate of progress are flexible, thereby being capable of adjustment to reflect the results of each pilot, including the level of acceptance by the public. At any point the Chief Electoral Office must be able to suspend or halt e-voting pilots if the integrity of electoral processes is at risk.

Before the first pilot commences, a detailed business case and comprehensive cost estimates will be required. Further legal analysis and policy development (including public consultation) in support of legislative reform will also be necessary. It is possible that entrenched provisions in the Electoral Act 1993 may need amending.

The Chief Electoral Office is a small business unit of the Ministry of Justice and fully occupied throughout the three year election cycle. Two indicative timelines are suggested for implementation, commencing in 2011 and 2014. The 2014 timeline will minimise the possibility of the administration of the 2008 General Election being compromised.

18 Appendix 1, Internet use and e-voting public attitudes survey June 2007

Survey conducted for the Electoral Commission by UMR Research in June 2007.[14]

Results are based upon questions asked in the UMR Research nation-wide omnibus survey. This is a telephone survey of a nationally representative sample of 750 New Zealanders 18 years of age and over.

Fieldwork was conducted from the 8th to 11th June 2007 and from the 21st to 26th June 2007 at UMR Research's national interview facility in Auckland.

The total sample size from the two surveys is n=1500.

The margin of error for a 50% figure at the '95% confidence level' based on a sample of n=1500 is ± 2.5%.

USE OF THE INTERNET FOR BANKING OR PURCHASING

How often do you use the internet for online banking or making online purchases?

	JUN 07 %
Once a week or more	41
1 to 3 times a month	13
Less than once a month	11
Never	34
Unsure	-
TOTAL	**100**

Base: All, n=1500
Note: Table will not sum to 100 percent due to multiple rounding.

[14] For further information regarding this survey and results, refer to Dr Helena Catt, Chief Executive, Electoral Commission

REASONS FOR NOT USING THE INTERNET MORE OFTEN

[Asked of those who use online banking or make online purchases less than once a month:]

Why don't you use the internet for online banking or making online purchases more often? What are your reasons?

	JUN 07 (n=169) %
Don't think it is very safe/ secure	37.3
Things restricting internet use Do not have internet access (10.1%), Internet too slow (5.9%), Not familiar with technology (4.7%), Do not have credit card (1.8%), Set-up costs (1.8%), Have to remember password (1.2%), Have old personal computer (0.6%), Have not heard good things about it (0.6%)	26.7
No need for it	14.2
Prefer other methods More convenient going to bank/shop (4.7%), Prefer tele-banking (3.6%), Prefer other methods (3.0%)	11.3
Prefer personal interaction Prefer to see person when making transactions (6.5%), Like to see what I am buying (3.0%)	9.5
Current purchasing habits My partner takes care of it (4.1%), Only use to purchase from overseas (1.8%)	5.9
Unsure	6.5

Base: 11% of respondents - those who said they use the internet for online banking and making online purchases less than once a month, n=169.
Note: Table will not sum to 100 percent due to multiple responses.

REASONS FOR NEVER USING THE INTERNET

[Asked of those who never use the internet for online banking or making online purchases:]

Why don't you use the internet for online banking or making online purchases? What are your reasons?

	JUN 07 (n=511) %
Do not have internet access	35.4
Things restricting internet use Not familiar with technology (17.4%), No need for it (5.5%), Internet too slow (2.0%), Do not have credit card (1.8%), Do not have personal computer (1.6%), Have not heard good things about it (1.6%), Set-up costs (0.8%), Have old personal computer (0.6%), Do not like using computer (0.4%), Internet unreliable (0.4%)	32.1
Do not think it is very safe/ secure	25.4
Prefer personal interaction Prefer to see person when making transactions (4.9%), Like to see what I am buying (1.0%)	5.9
Current purchasing habits My partner takes care of this (5.1%)	5.1
Prefer other methods More convenient to go to bank/shop (1.8%), Prefer other methods (2.6%)	4.4
Unsure	2.0

Base: 34% of respondents - those who said they never use the internet for online banking and making online purchases, n=511.
Note: Table will not sum to 100 percent due to multiple responses.

CONFIDENCE IN MANAGEMENT AND ACCURACY OF GENERAL ELECTIONS

Using a 0 to 10 scale, where 0 means not at all confident and 10 means very confident, how confident are you that general elections in New Zealand are managed fairly and that vote counting is accurate.

	JUN 07 %
0 – Not at all confident	1
1	1
2	1
3	2
TOTAL NOT CONFIDENT (0-3)	**5**
4	2
5	8
6	3
TOTAL NEUTRAL (4-6)	**13**
7	6
8	20
9	16
10 – Very confident	38
TOTAL CONFIDENT (7-10)	**80**
Unsure	1

Base: 91% of respondents - those who expressed a voting preference, i.e. did not say 'unsure', 'refused' or 'won't vote' when asked which party they would vote for if an election were held today, n=1371
Note: Table may not sum to 100 percent due to multiple rounding.

E-VOTING STATEMENT TESTING – I WOULD VOTE ONLINE

The possibility of online voting is being explored for New Zealand general elections. On election day you could choose to vote at a polling place as people do now, or do it from anywhere else as long as you had access to a computer connected to the internet.
Using a 0 to 10 scale, where 0 means strongly disagree and 10 means strongly agree, how strongly do you agree or disagree with the following statements about online voting in New Zealand general elections, assuming that it would use security systems similar to internet banking and reputable online retailers?

I would choose to vote online instead of visiting a polling place

	JUN 07 %
0 – Totally disagree	24
1	8
2	4
3	3
TOTAL DISAGREE (0-3)	**39**
4	2
5	9
6	3
TOTAL NEUTRAL (4-6)	**14**
7	4
8	7
9	4
10 – Totally agree	31
TOTAL AGREE (7-10)	**46**
Unsure	1

Base: 91% of respondents - those who expressed a voting preference, i.e. did not say 'unsure', 'refused' or 'won't vote' when asked which party they would vote for if an election were held today, n=1371
Note: Table may not sum to 100 percent due to multiple rounding.

E-VOTING STATEMENT TESTING – COMFORTABLE VOTING ONLINE

The possibility of online voting is being explored for New Zealand general elections. On election day you could choose to vote at a polling place as people do now, or do it from anywhere else as long as you had access to a computer connected to the internet.
Using a 0 to 10 scale, where 0 means strongly disagree and 10 means strongly agree, how strongly do you agree or disagree with the following statements about online voting in New Zealand general elections, assuming that it would use security systems similar to internet banking and reputable online retailers?

I would be comfortable with voting online

	JUN 07 %
0 – Totally disagree	22
1	5
2	3
3	3
TOTAL DISAGREE (0-3)	**33**
4	1
5	7
6	2
TOTAL NEUTRAL (4-6)	**10**
7	5
8	9
9	7
10 – Totally agree	34
TOTAL AGREE (7-10)	**55**
Unsure	1

Base: 91% of respondents - those who expressed a voting preference, i.e. did not say 'unsure', 'refused' or 'won't vote' when asked which party they would vote for if an election were held today, n=1371
Note: Table may not sum to 100 percent due to multiple rounding.

E-VOTING STATEMENT TESTING – CONFIDENT OF PRIVACY

The possibility of online voting is being explored for New Zealand general elections. On election day you could choose to vote at a polling place as people do now, or do it from anywhere else as long as you had access to a computer connected to the internet.
Using a 0 to 10 scale, where 0 means strongly disagree and 10 means strongly agree, how strongly do you agree or disagree with the following statements about online voting in New Zealand general elections, assuming that it would use security systems similar to internet banking and reputable online retailers?

I would be confident that I could vote online without anyone seeing who I was voting for

	JUN 07 %
0 – Totally disagree	16
1	5
2	3
3	3
TOTAL DISAGREE (0-3)	**27**
4	2
5	8
6	3
TOTAL NEUTRAL (4-6)	**13**
7	5
8	12
9	8
10 – Totally agree	33
TOTAL AGREE (7-10)	**58**
Unsure	2

Base: 91% of respondents - those who expressed a voting preference, i.e. did not say 'unsure', 'refused' or 'won't vote' when asked which party they would vote for if an election were held today, n=1371
Note: Table may not sum to 100 percent due to multiple rounding.

E-VOTING STATEMENT TESTING – CONFIDENT OF NO UNDULY VOTE INFLUENCE

The possibility of online voting is being explored for New Zealand general elections. On election day you could choose to vote at a polling place as people do now, or do it from anywhere else as long as you had access to a computer connected to the internet.
Using a 0 to 10 scale, where 0 means strongly disagree and 10 means strongly agree, how strongly do you agree or disagree with the following statements about online voting in New Zealand general elections, assuming that it would use security systems similar to internet banking and reputable online retailers?

I would be confident that I could vote online without anyone else unduly influencing my vote

	JUN 07 %
0 – Totally disagree	14
1	3
2	4
3	3
TOTAL DISAGREE (0-3)	**24**
4	2
5	8
6	2
TOTAL NEUTRAL (4-6)	**12**
7	4
8	10
9	9
10 – Totally agree	39
TOTAL AGREE (7-10)	**62**
Unsure	2

Base: 91% of respondents - those who expressed a voting preference, i.e. did not say 'unsure', 'refused' or 'won't vote' when asked which party they would vote for if an election were held today, n=1371
Note: Table may not sum to 100 percent due to multiple rounding.

ESSENTIAL SECURITY FEATURES

If you were to vote online, would you regard the following security features as essential, nice to have or not important?

	JUN 07 %			
	Essential	Nice to have	Not important	Unsure
A screen which would ask you to confirm who you were voting for before it was made final.	76	11	11	2
Being able to revisit the voting website to confirm that your vote has been received but not who you have voted for.	54	29	16	2
Being able to revisit the voting website to confirm that your vote has been received and who you have voted for.	50	27	21	2
Being able to request confirmation using a different means of communication, such as text	25	34	38	3

Base: 66% of respondents - those who said they use the internet for online banking or making online purchases at least once a month, n=985
Note: Table may not sum to 100 percent due to multiple rounding.

19 Appendix 2 , E-voting system 'straw men'

This section is taken from Working Paper 8, *System Architecture, Integration and Requirements.* Numbering of figures has been retained from that paper.

19.1 Sample Architecture - Internet Based Dual Channel Scheme

The following sample architecture is provided as a high level example of an unsupervised e-voting system. It should be noted that this is not a complete solution design, having not undergone a detailed design process, peer or academic review. Low level details of cryptographic and encrypted ballot generation operations required to undertake this architecture have not been included.

This sample architecture borrows somewhat from the *Prêt à Voter* system[15], but is not intended to represent a complete implementation of that scheme. In some other respects (such as allowing the voter to cast multiple ballots, only the last of which is counted), it resembles the Internet based voting system used in the Estonian general election of March 2007.

The scheme is intended to illustrate one possible approach to unsupervised e-voting. Implicit within this architecture are the following assumptions:

- That completely preventing all violations of voter privacy[16] in an unsupervised election is very difficult to accomplish without introducing excessive complexity to the voting process;
- That if introduced, remote Internet based voting would remain an optional facility, with conventional polling stations remaining available for those who preferred traditional voting methods; and
- That due to its optional nature, along with other privacy related mitigations outlined below, such a system adequately provides for the democratic principles of secret suffrage and freedom from undue influence.

The architecture itself places an emphasis on voter verification of ballots, detection of irregularities at all stages of the electoral process, and allowing the voter to re-vote, either conventionally or electronically, should they feel they have been subject to intimidation, or violation of privacy.

[15] *Pret a Voter: a Systems Perspective,* Peter Y. A. Ryan and Thea Peacock, September 2005, available from http://www.cs.ncl.ac.uk/research/pubs/trs/papers/929.pdf

[16] Privacy violations can be by either direct observation (e.g. a person in the room with the voter) or indirect observation (e.g. by way of software installed on the voter's voting device). Lack of electoral supervision of voting can also enable voter coercion, vote buying or other corrupt practices, unless these risks are in some way mitigated

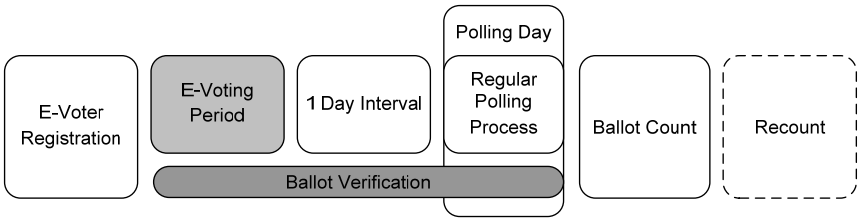


Figure 11

This sample architecture is dual channel, making use of the Internet for actual e-voting, and the voter's choice of either mobile phone MMS (PXT) text message or a public Web site as channels for verification of ballot content.

Figure 12 below shows a simplified view of communications between the voter and the e-voting infrastructure[17].

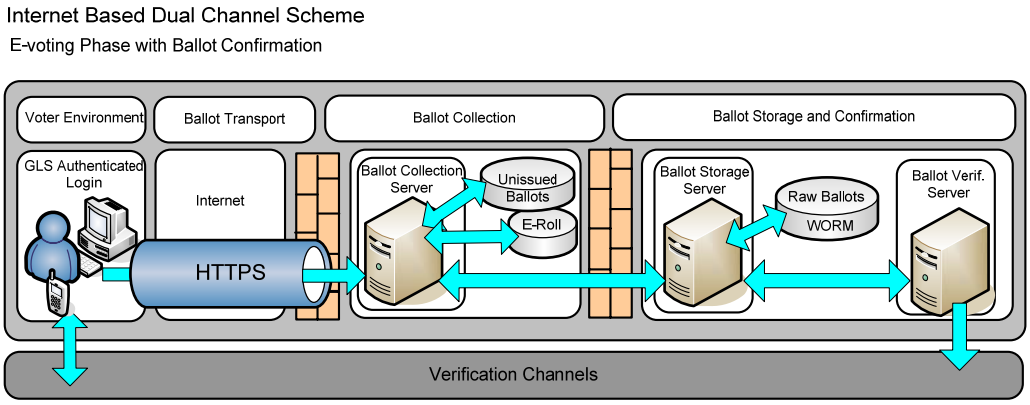


Figure 12

E-voting occurs during a discrete period in advance of polling day. Voters may submit as many e-votes as they wish, with only the last ballot cast being counted in the final result. If implemented in a medium or large scale, this system would very likely make use of the Government Logon Service (GLS)[18] operated by the State Services Commission for authentication services. Secure HTTP (HTTPS) is used for voter communications with electoral infrastructure over the Internet. The voting application itself consists of a digitally signed applet downloaded and run within the voting client device, which communicates directly with server side components to implement end to end encryption of the voting process. Ballots received would be stored on Write Once Read Many (WORM) media, meaning that no individual ballot could be changed or deleted once received.

[17] HTTPS indicates a secure HTTP connection. HTTPS is not a specific protocol, but refers to the combination of a normal HTTP interaction over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) transport mechanism. Raw Ballots refers to completed ballots as forwarded to a Ballot Storage Server by a valid Ballot Collection Server. WORM refers to Write Once Read Many storage, a media that does not permit data, once received, to be changed or deleted.

[18] The State Services Commission's GLS is an all-of-Government logon service for Government websites. The Department of Internal Affairs is in the process of developing the Identity Verification Service (IVS) to extend the GLS by providing online verification of identity. Whether the IVS would ultimately have a role to play in e-voting is, at this stage, unclear.

19.1.1 Internet voting – Pre-registration

E-voters will have performed e-voter pre-registration prior to attempting to vote. This will have included:

- GLS registration, or establishment of other appropriate login credentials; and
- A unique identifier being generated and associated with the voter within the E-roll.

19.1.2 Internet voting – Authentication

Any time between the commencement and completion of the e-voting period, the voter may access the election portal using a regular Web browser. A secure HTTPS connection is established for this and subsequent Internet communications.

The portal would then redirect the voter to a Ballot Collection Server which, assuming that all-of-Government authentication infrastructure were to be used, would then initiate the GLS login process.

The details of the GLS are laid out in other documents[19], however the basic interaction is described in Figure 13 below.

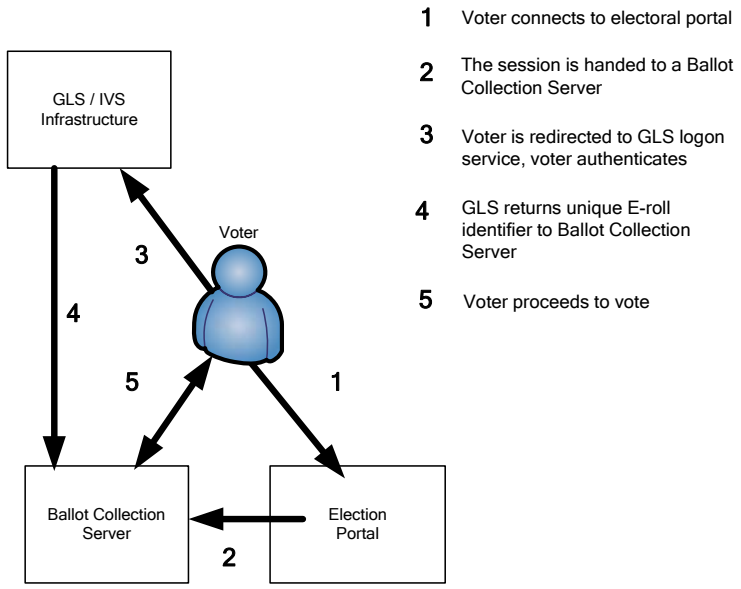


Figure 13

The GLS government authentication infrastructure would perform two main functions. It would authenticate the voter and it would provide the Ballot Collection Server with the voter's unique E-roll voter identifier, which is used in subsequent operations.

19.1.3 Internet voting – Casting the vote

The Ballot Collection Server uses the unique E-roll voter identifier to search the E-roll for the voter in order to:

[19] *Authentication for e-government, Government Logon Service Design Overview*, State Services Commission, 2006.

- Confirm their entitlement to vote;
- Determine the voter's correct electorate; and
- Retrieve a randomized ballot for presentation to the voter.

The voter is then presented with a randomized ballot[20] in which the candidate and party orders have been scrambled. The process by which candidate and party orders have been scrambled (and may be unscrambled using a cryptographic key buried within the ballot serial number), is assumed to be very difficult if not impossible for a third party to replicate, even given significant computing resources. The voting transaction itself makes use of an applet[21] downloaded to the voter's computer from the Ballot Collection Server and run locally on the voter's machine (although this process should be transparent to the voter, to whom everything appears to happen within the browser). As shown in the Figures 14 and 15, the voter selects their chosen candidate/s and party and submits the ballot. Although the simplified MMP-based example shows a very basic ballot, this scheme can be adapted to support more complex ballot formats, such as those used for local body elections.

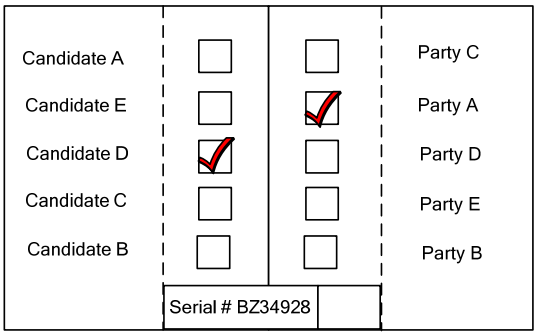


Figure 14

The portions of the ballot containing candidate and party names disappear from the screen once the voter confirms their intent. The remaining portion (shown in Figure 15) is then provided to the voter as a digitally signed voter-verification 'receipt' (although without candidate or party names it cannot on its own be used to prove voter intent - and can therefore be considered 'receipt-free').

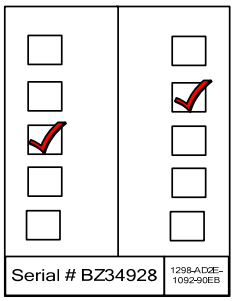


Figure 15

[20] Randomisation of candidate order would require a legislative change as candidate order must currently be represented alphabetically.
[21] A self contained program written in Java, ActiveX or an equivalent widely supported programming language. Applets may be digitally signed to indicate their authenticity.

The receipt may be printed out by the voter if they have a printer or provided to them as a signed PDF or in a similar document format for subsequent verification. Voters are asked to retain their receipts until the final election result is announced.

The client applet and the software running on the Ballot Collection Server now collaborate to generate an election specific voter identifier as a function of both the voter's unique E-roll identifier and a public encryption key specific to the particular election event. This is appended to the ballot before it is digitally signed and transmitted to a Ballot Storage Server.

The Ballot Storage Server confirms that the ballot comes from a valid Ballot Collection Server by checking the signature on the ballot. It then writes the ballot, including the appended election specific voter identifier, to tamper-proof WORM media.

After verifying that the ballot is safely recorded (and in practice, verifying that it has also been recorded by a redundant Ballot Collection Server and WORM drive in another location), the Ballot Storage Server then returns a confirmation message to the Ballot Collection Server.

The Ballot Collection Server then advises the voter that their vote has been received and may be verified by sending an SMS TXT message comprised of their ballot serial number (BZ34928 in the above example) to the electoral authority's ballot verification telephone number, or by comparing their receipt with a copy posted to a publicly available website.

The Ballot Collection Server then marks the E-roll to indicate that the voter has cast at least one electronic ballot in the election.

Should the voter choose to vote again for some reason, their ballot will be recorded again in exactly the same way. This may result in multiple ballots from a single voter being recorded, each with a different ballot number (and potentially signed by different Ballot Collection Servers) but each appended with the same election specific voter ID.

It should be noted that the Ballot Collection Server may represent the weakest link in this or similar architectures, as corruption of Ballot Collection Servers would allow an attacker to insert or cancel ballots. While such attacks would be likely to be detected through voter verification, they would still have the effect of throwing into doubt all votes received through the compromised Ballot Collection Server.

Ballot Collection Servers should therefore be the most vigorously protected, certified and audited components of the E-voting infrastructure.

19.1.4 Internet voting - Ballot Verification

Any time prior to the close of the polls, the voter may text their ballot serial number to the ballot verification service, whereupon the Ballot Verification Server will send a request to the Ballot Storage Server to return the ballot receipt corresponding to the ballot serial number provided.

Upon receiving this information the Ballot Verification Server replies to the voter via MMS (PXT) message, showing a visual representation of the requested ballot *receipt* (i.e. the completed ballot *without* candidate and party information).

Right up until the close of polls voters will be:

- Encouraged to report any irregularity or request help if required; and
- Able to attend a polling station and lodge a regular vote in place of their e-vote/s if they so desire.

As a second Ballot Verification channel, all ballot receipts are posted to a publicly available website which displays all ballot receipts openly. This website, which remains available until the official election result is announced, allows e-voters to visually check their receipts against the posted images. It also makes all ballots (in this encrypted form) world readable and places them in the public domain, making removal or cancellation of ballots by corrupt electoral officials extremely difficult.

19.1.5 Internet voting – Ballot Count

Internet Based Dual Channel Scheme

Ballot Count Phase

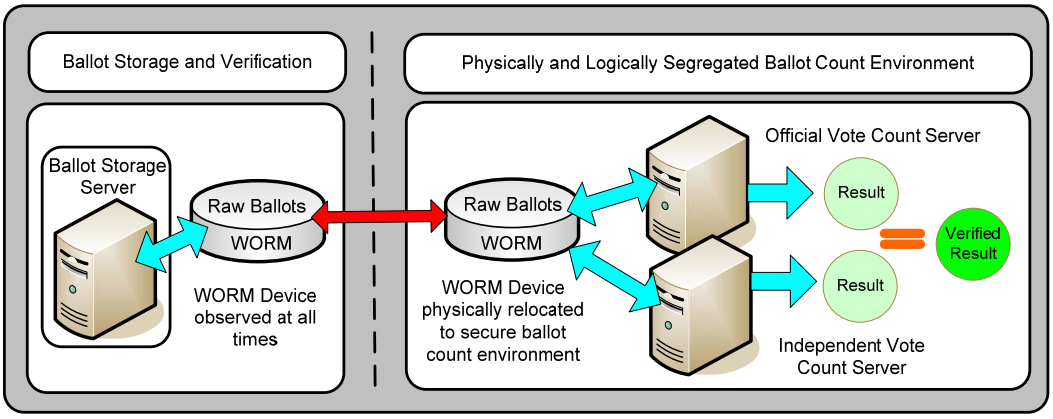


Figure 17

Upon closure of the polls, telephone based ballot verification services are shut down and any secondary WORM drive containing duplicate raw ballots is shut down and sealed.

The primary WORM drive is relocated under scrutiny from the Ballot Storage and Verification Environment to an adjacent secure Ballot Count Environment. Election officials and independent observers scrutinise all activities that occur within this phase and movement of electronic devices, including cameras, telephones and flash storage in or out of the environment is rigidly controlled. It is important to conduct all vote decryption and counting operations in a segregated and rigidly controlled environment in order to mitigate any risk, both real or perceived, of the counting process being subverted, or of voter identity and ballot content being matched in some way.

Figure 17 shows two separate ballot count devices are used to independently count the votes. This approach has not been carried through to the proposed strategy, as verification of the official count process can be established in tests prior to its use in an election, using the method described here. The 'official' Ballot Count Server is built to a publicly available specification and produces a preliminary result. The 'independent' vote count server is developed to the same specification by a third party (perhaps a volunteer group of computer and political science academics) and confirms the preliminary result produced by the 'official' server. Confirmation would be required before the official server is used in an election.

The cryptographic key required by both servers to unscramble the candidate order of each ballot is distributed amongst several senior electoral officials in such a way that none of them alone may decrypt the ballots[22]. Instead the master key must be reassembled from its parts before the ballots can be decrypted. As both counting systems are developed to the same specification and have been extensively tested and independently certified, results should be identical in the absence of any corrupt practices or ballot tampering. Source code for *at least* one of the systems (as certified and deployed) will be available for public scrutiny.

Each Ballot Count Server independently unscrambles the candidate order using the master cryptographic key and counts the votes for each candidate and party accordingly. Where more than one ballot is found to be appended with the same election specific voter identifier only the ballot with the latest time stamp is counted. The output is printed out, signed by witnesses, and entered into the Election Management System (EMS)[23].

In the event of an official recount being declared, the secondary ballot storage WORM drive shall be unsealed and relocated under scrutiny to a secure ballot count environment in order for a secondary count (or recount) to occur.

In order to detect the possible insertion of ballots through corruption of the Ballot Collection Servers, or other parts of the process, the following audit step is undertaken after the initial count. The private key unique to the specific election (physically held until now by electoral officials other than those holding the key used to unscramble candidate order[24]) is now reassembled and used to extract the unique E-roll voter identifier for a statistically significant and truly random sample of final ballots (i.e. ballots for which no later ballot is stamped with the same election specific voter identifier). The voter associated with each of these sample ballots is then contacted over the following days and asked:

- To confirm that they did indeed lodge an e-vote; and
- Whether they would be willing to access the public Ballot Verification Web server and confirm the sample ballot receipt matches the ballot receipt they have in their possession.

Finally, during the period following the initial count but prior to the release of official final results, the E-roll and electoral roll will be reconciled in order to detect instances where voters have voted both electronically and conventionally. In such cases (or in other special cases such as where the voter may have died between e-voting and polling day, or voted in the wrong electorate), the results are adjusted accordingly[25].

---

[22] Some commercial e-voting systems, such as that marketed by Scytl Secure Electronic Voting, use such a multi-part key, each portion of which is held by a separate individual. This master key must be reconstituted by a quorum of trusted officials in order to successfully decrypt the ballots.

[23] The EMS is an application used by the Chief Electoral Office to assist with the administration of elections. One of its core functions is to process and collate election results entered by staff.

[24] As a matter of process it might be appropriate that these two keys never be present in the segregated vote count environment at the same time, as this could potentially enable matching of voter identity and intent.

[25] This will involve the insertion of small numbers of 'cancellation' and 'clone' ballots (which effectively either nullify an entire ballot, or its candidate portion, respectively) and the count being run again to produce a final electronic result.

Throughout these processes, any and all irregularities shall be investigated to the greatest degree possible whilst preserving voter privacy. Voters reporting irregularities should be asked to fill in a declaration to that effect. They may be further asked whether the computer they voted from may be inspected for malware. False claims of ballot tampering will be difficult to make because ballot receipts are digitally signed and therefore very difficult to forge. While it is inevitable that some issues will be reported and that some voters might even have their ballots altered, replaced or deleted by malware on their computers, voter verification and statistical analysis of the issues reported should make it extremely difficult for widespread electoral fraud to go undetected, even if irregularities cannot be prevented altogether.

19.1.6 Internet voting – Infrastructural Fault Tolerance

The examples above mainly describe a linear stream of transactions involving a voter, a Ballot Collection Server, a Ballot Storage Server, a Ballot Verification Server etc. These have been represented in this way in the interests of clarity.

In practice, as shown in Figure 18 below, the Ballot Collection infrastructure would be distributed over several servers in separate geographical locations, both for fault tolerance purposes (i.e. to protect against a single computer failure interrupting the election) and as a mitigation strategy in the event of deliberate sabotage, denial of service attack, or similar events beyond the control of electoral authorities.

Similarly, the Ballot Storage and Verification infrastructure would be mirrored across two locations, with each ballot being written to both WORM drives before the voter was informed that their vote had been received.

This approach provides protection both against a WORM drive failure, or similar catastrophic event invalidating the election, and also provides another barrier against wholesale electoral fraud.

Internet Based Dual Channel Scheme
Infrastructure Fault Tolerance View

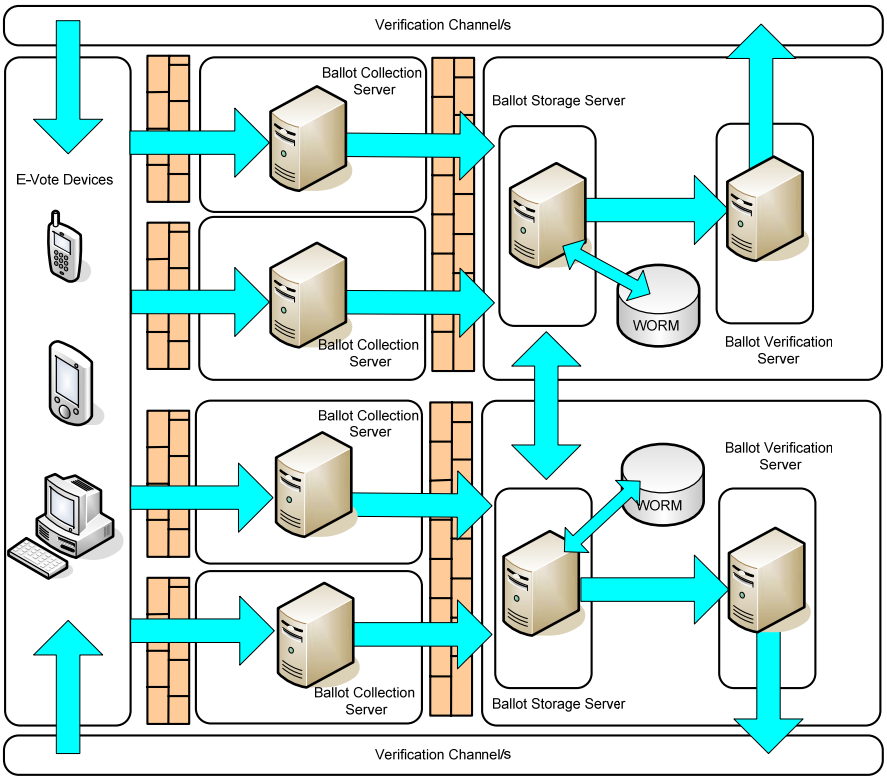


Figure 18

19.2 Sample Architecture - Telephone Based Voting with Ballot Pre-Encryption

The following telephone based voting architecture is provided as an alternative to the Internet based e-voting systems already presented. It should be noted that it is not a complete solution design.

Telephone based voting enjoys strong support from - and has the potential to dramatically improve electoral accessibility for - groups such as the visually impaired. Were telephone based voting to be made available only to this relatively small group, some of the complexity of the process outlined below might be dispensed with (as this would still result in a net improvement to privacy for these voters). This is discussed further below.

If telephone voting were to be made more widely available however, some means of protecting voter privacy and preventing other corrupt practices, such as is outlined below, may still be required.

This architecture seeks to mitigate privacy and security concerns around remote e-voting by obfuscation of the ballot and by distributing voter credentials and candidate information via separate pre-registration channels. Ballot encryption uses the method

proposed by the UK's national technical authority for information assurance, the Communications-Electronics Security Group[26].

The voting process itself is single channel, making use of a touch tone telephone for both e-voting and voter verification of ballots.

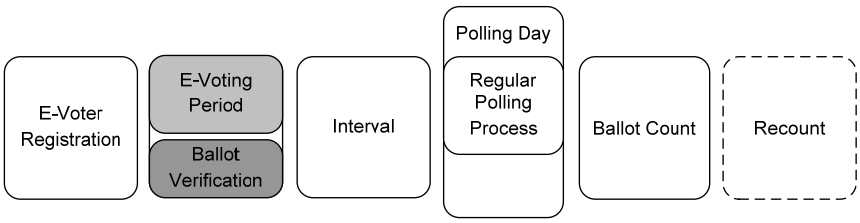


Figure 22

As with the previous architecture, e-voting occurs over a discrete period in advance of polling day. This architecture allows voters to submit as many e-votes as they wish, with only the last ballot cast being counted in the final result.

19.2.1 Telephone Voting – Pre-Registration

E-voters will have performed e-voter pre-registration prior to attempting to vote. This will have included:

- An adequately secure means of registering for telephone voting with the electoral authority. If this is to be done by telephone some means of confirming voter identity will be required. If voice-based biometric authentication is used to secure e-voting, the voter's 'voiceprint' may be taken at this time. Otherwise, the voter will specify a PIN which they will use during authentication;

- A unique E-roll voter identifier will be generated and associated with the voter;

- The voter will specify a channel by which additional confidential information may be received. Options include e-mail formatted for screen reader or posted documents written in Braille, English, or any other supported language;

- The dispatch via post or e-mail (in a form legible to the voter), of the unique E-roll voter identifier; and

- The dispatch via separate post or e-mail (in a form legible to the voter), of candidate/party lists and related voting codes.

[26] *E-Voting Security Study, Issue 1.2*, CESG, Government Communications Headquarters, UK Government, July 2002

19.2.2 Telephone voting - Authentication

Telephone Based Voting with CESG Style Ballot Pre-Encryption
E-voting Phase with Ballot Confirmation

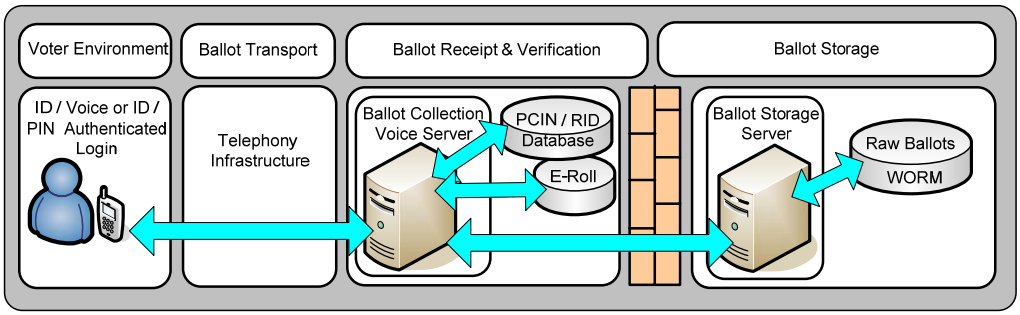


Figure 23

Any time between the commencement and completion of e-voting, the voter may access the telephone voting service using a touch tone telephone. The service will request that the voter authenticate themselves using a combination of unique E-roll voter identifier (entered via the touch tone keypad), and either biometric voice recognition or a pre-established voter designated PIN.

19.2.3 Telephone voting – casting a vote

The candidate/party lists and related voting codes distributed to voters prior to voting are based on the ballot pre-encryption scheme devised by the CESG in the UK. Each candidate is listed with both a Personal Candidate Identification Number (PCIN) and an expected Response ID (RID); both codes being unique to the specific candidate and to the specific voter. The process of generating of these codes is not explored further in this report, being somewhat complex and well detailed elsewhere[27]. A simplified example is provided in Figure 24 below. It is written in English; however Braille, screen-reader formatted, or foreign language versions would be distributed according to voter preference.

[27] Practical Pollsterless Electronic Voting, T. Storer, University of St Andrews, Scotland, 2006

Voter Information Card
John Smith
Voter ID 785 463 746

Electorate Vote

Candidate	Party	PCIN	Expected Response (RID)
Barney Ruble	Barneysparty	3322	2945
Fred Flint	Fredsparty	9977	8712
Wilma Wales	Wilmasparty	4488	3821
Zelda Jones	Zeldasparty	5511	7596
Intentionally Spoiled Electorate Ballot		1100	7221

Party Vote

Party	PCIN	Expected Response (RID)
Barneysparty	2251	9201
Fredsparty	6670	5290
Wilmasparty	8801	0029
Zeldasparty	1142	7123
Intentionally Spoiled Party Ballot	7700	4387

Figure 24

Once the voter has authenticated themselves to the telephone voting service, the Ballot Collection Voice Server consults the E-roll in order to:

- Confirm entitlement to vote;
- Determine the voter's correct electorate; and
- Retrieve the appropriate candidate codes and associated response IDs for the voter (note that the Ballot Collection Voice Server need not know which candidate is associated with each pair of codes).

The voter is then guided by voice prompts through the process of entering candidate codes (PCINs) for each race. In each case, when the voter enters the PCIN associated with a candidate, the corresponding RID is returned verbally by the Ballot Collection Voice Server, providing the voter with some surety that their ballot has been properly received. After all selections have been made, the voter may review all RIDs before final ballot submission.

The Ballot Collection Voice Server then generates an election specific voter identifier as a function of both the voter's unique E-roll identifier and the public key of the specific election itself, and appends this to the compiled list of voter's PCIN choices. It then signs the resulting ballot with its own private key and forwards it to the Ballot Storage Server.

The Ballot Storage Server confirms that each incoming ballot comes from a valid Ballot Collection Voice Server by checking the signature on the ballot. It then writes each compiled list of PCINs, including its associated election specific voter identifier, to tamper-proof WORM media, as in previous examples.

After verifying that these items are safely recorded on redundant media, the Ballot Storage Server returns a confirmation message to the Ballot Collection Voice Server.

The Ballot Collection Voice Server then advises the voter that their vote has been received before disconnecting.

19.2.4 Telephone voting - Ballot verification

In this architecture, ballot verification occurs at the time of voting, as each candidate's PCIN code is entered and the corresponding RID is returned.

It provides a weaker form of ballot verification (analogous to a Voter Verified Paper Trail) because it only verifies the ballots as they are received by the Ballot Collection Voice Server, not as they are stored by the Ballot Storage Server.

Right up until the close of polls, voters:

- Will be encouraged to report any irregularity or request help if required; and
- Will be entitled to attend a polling station and lodge a regular vote in place of their e-vote/s if they so desire.

19.2.5 Telephone voting – Ballot count

Telephone Based Voting with CESG Style Ballot Pre-Encryption
Ballot Count Phase

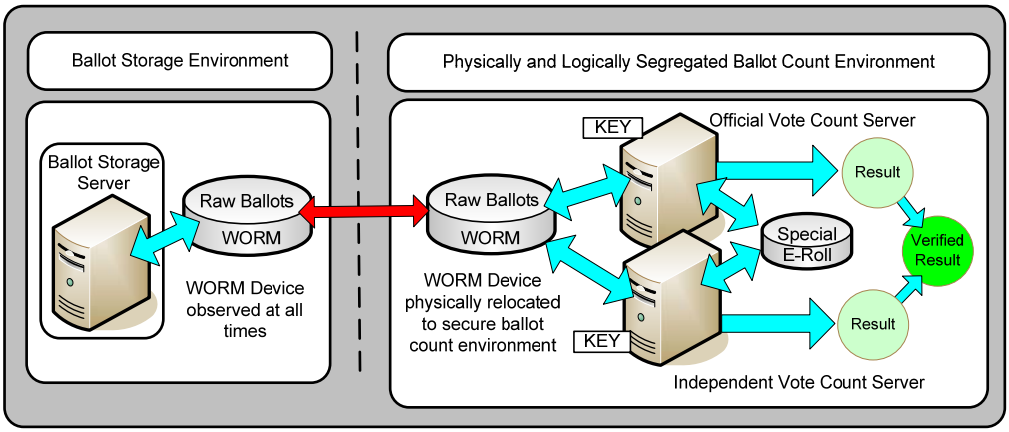


Figure 25

Note that the 'independent vote count server' in the above Figure is used for testing, not real election environments. Upon closure of e-voting, any secondary WORM drive containing duplicate raw ballots is shut down and sealed.

As in sample Architectures 1 and 2, the primary WORM drive is physically relocated under scrutiny from the Ballot Storage and Verification Environment to an adjacent secure Ballot Count Environment. Election officials and independent observers scrutinise all activities that occur, and movement of electronic devices in or out of the environment is rigidly controlled.

The vote count server now uses the election's private key (physically held until now by the chief electoral official attending), to extract the unique E-roll voter identifier for each

ballot and then to retrieve or regenerate the link between each PCIN and its associated candidate from a special copy of the E-roll containing only the information necessary to perform this function. Where more than one ballot is found to be appended with the same election specific voter identifier, only the ballot with the latest time stamp is counted.

Each Ballot Count Server then performs the necessary operations to determine each voter's intent based on PCIN to candidate matching and counts the votes for each candidate accordingly. Assuming the results of both systems match, the output is printed out, signed by witnesses and subsequently entered into the Chief Electoral Office's EMS.

As in the previous examples, in the event of a conflict, both systems will be reset and the count run again. In the event that results still differ, the official server's count will be considered the provisional result and forensic analysis of both systems will be undertaken as a matter of urgency, to determine both the cause of the difference and to confirm the correct result.

As in earlier examples, a truly random sample of ballots is selected and their associated unique E-roll voter identifiers (only) are extracted. Each of these voters is then contacted over the following days and asked to confirm that they did indeed lodge an e-vote.

Any and all irregularities should be investigated to the greatest degree possible whilst respecting voter privacy. Voters reporting irregularities should be asked to make a declaration to that effect.

19.2.6 Telephone voting – Infrastructural fault tolerance

Sample Architecture 3 would make use of a distributed infrastructure in exactly the same way as Sample Architectures 1 and 2.

19.2.7 Telephone voting – Low security version

As is discussed above, ballot obfuscation through the use of PCINs and RIDs adds complexity to the voting process. If it was deemed that protections for voter privacy could be relaxed in the interests of simplifying the voting process, then the following changes could be made to this architecture to achieve this:

- Voters could simply vote by entering a number associated with each candidate or party (or even by speaking the candidate or party name), with the Ballot Collection Voice Server repeating the name back to the voter verbally; and

- In order to prevent replay attacks voters would only be allowed to telephone-vote once under such a scheme. A replay attack would occur when some party recorded a voting transaction and replayed the login process to a Ballot Collection Voice Server allowing them to vote again using the voter's identity, overriding their original vote. The voter would still be able to vote at a polling place if they have any concerns about their telephone vote.

20 Appendix 3, Comparison with reference voting architecture

This section is taken from Working Paper 8, *System Architecture, Integration and Requirements.*

20.1 Reference Architecture – Postal Voting

Postal voting has a number of weaknesses in that:

- It does not necessarily provide a strong means of authentication. A stolen postal ballot may be used fraudulently if voter and witness declarations are forged;
- It does not ensure voter privacy during the vote. A coercer may observe the voter voting and posting the ballot, which leaves postal voting open to vote buying or intimidation;
- It is considered non-voter verifiable, in that a voter may know what the contents of the posted ballot were but has no way to know that it has been received or will be counted;
- Postal ballots are potentially vulnerable to interception while within the postal system; and
- Postal votes must be opened and processed manually, resulting in an associated vote count delay and related overheads.

Despite these flaws, postal voting is considered to be an acceptable voting method for widespread use in *local body* elections and for *limited* use in general elections. In general elections, postal ballots form a relatively small proportion of the votes cast overall, meaning that the potential for wholesale fraud is limited. More widespread use of postal voting in general elections would carry a more significant risk.

Voter privacy is not strongly protected in postal voting and voter coercion is not prevented.

20.2 Internet Based Dual Channel Scheme

The Internet based dual channel scheme outlined in this report has several limitations, including:

- A third party physically present during voting may observe the voter's intent, making the system potentially subject to violations of voter privacy and coercion (although the latter is partially mitigated by allowing voters to lodge subsequent e-votes or to vote again at a polling place);
- Malware (or even legitimate computer management software) installed on a voter's computer may allow a remote party to observe voter intent without the voter's knowledge. This slightly increases the system's vulnerability to violations of voter privacy;
- Malware installed on a voter's computer may alter a voter's ballot without their knowledge, although this risk is mitigated to some degree by the provision of a "receipt free" ballot verification channel; and

- Measures taken to provide receipt free voter verification of ballots add some complexity to the voting process.

This voting method is fairly trustworthy from the voter's perspective (in as much as the voter can determine whether or not their ballot was accurately received).

It has some vulnerability to coercion and vote buying, although in these cases the risks are mitigated through the ability of voters to revote.

A scheme similar to this one could be considered appropriate for widespread use only if: i) some degree of risk to voter privacy was considered acceptable; and ii) the voting method remained optional.

20.3 Telephone Voting with CESG Style Pre-Encryption

The telephone voting architecture described in this report has some limitations, including that:

- A third party present during voting and able to observe both the voting process and candidate/party information used by the voter may be able to perceive voter intent, although potential for coercion is partially mitigated by allowing voters to lodge subsequent e-votes;

- Measures taken to protect voter privacy and to provide receipt free voter verification of ballots add significant complexity to the voting process; and

- Voter verification of ballots is not as strong as some other examples.

It should be noted that, while generally this scheme has some vulnerability to coercion or violation of voter privacy, for the visually impaired it would have the effect of significantly *reducing* the risk of these events.

In other regards, the model is relatively effective, as long as the required level of complexity is not seen to be excessive from the voter's perspective.

If voter acceptance of the necessary privacy and integrity measures could be achieved, telephone voting secured by some means such as ballot pre-encryption may be considered as a possible e-voting channel for widespread adoption in the future.

20.4 Telephone Voting Low Security Variant

A telephone voting architecture which did away with the ballot pre-encryption and allowed transmission of voter intent and verification information in an unencrypted form would have the following limitations:

- Not only third parties physically present but those able to listen in on the telephone call during voting would be able to discern voter intent;

- Each voter would be able to lodge only one vote, making the system vulnerable to coercion and vote buying; and

- Voter verification of ballots would not be as strong as some other examples.

For these reasons such a scheme would be appropriate only for smaller scale deployment, such as a replacement for postal voting, rather than as a widely available voting channel.

21 Appendix 4, High level cost estimates

- Withheld: sections 9(2)(f)(iv) and 9(2)(i) Official Information Act 1982

Pilot Implementation

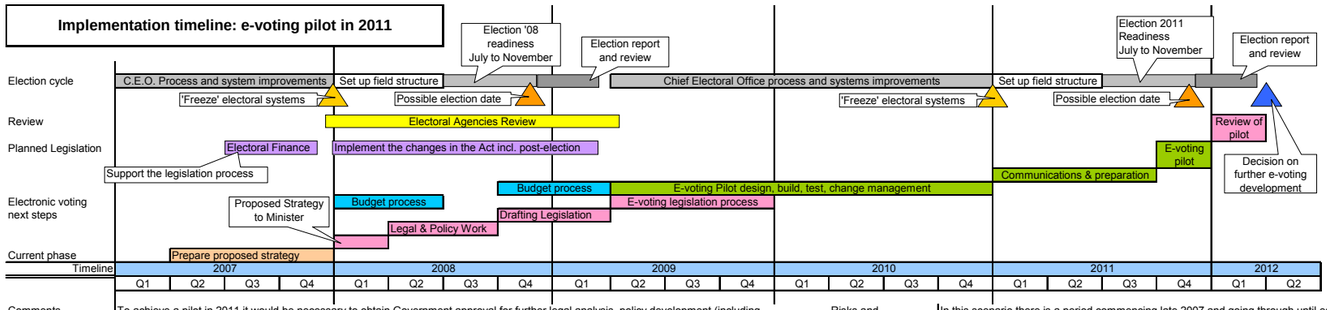
- Withheld: sections 9(2)(f)(iv) and 9(2)(i) Official Information Act 1982

Widely available implementation

- Withheld: sections 9(2)(f)(iv) and 9(2)(i) Official Information Act 1982

- Withheld: sections 9(2)(f)(iv) and 9(2)(i) Official Information Act 1982

22 Appendix 5, Implementation timeline issues



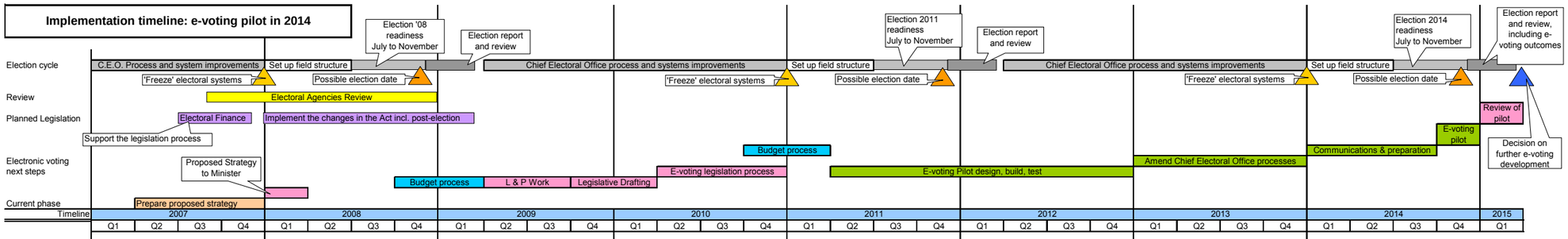
Assumptions for both scenarios: The scenarios consider only the work streams up to the first e-voting pilot. Further development would be required in subsequent election cycles. It is assumed that the e-voting system piloted in both scenarios is relatively fully featured. This allows as many elements as possible to be assessed during tests and actual voting, and ensures that subsequent developments can build on previous work. It is also assumed that the development time for such a system is at least 18 months including any tendering and certification processes.

Comments

To achieve a pilot in 2011 it would be necessary to obtain Government approval for further legal analysis, policy development (including public consultation) and legislative drafting work to take place during 2008. This would enable Parliament to consider and pass enabling legislation during 2009. Budget approval for expenditure associated with this work would be required. Technical work on the pilot should commence in parallel with the passage of legislation in order to be complete by the time electoral systems are frozen in late 2010. Budget approval would be required in 2009 for expenditure associated with this work. This timeline assumes policy continuity into the term of the next Parliament.

Risks and uncertainties

In this scenario there is a period commencing late 2007 and going through until early 2009 of intense policy-related demands on the Chief Electoral Office. This coincides with the mission-critical delivery of the 2008 general election. To manage this risk and deliver good quality policy development for e-voting it would be necessary to provide sufficient resource and management capability for the project to proceed without impringing unduly on the other work streams of the Office. This would not be possible at current (2007) staff levels. Risks would arise from technical and operational work proceeding in the absence of legislative certainty (this is a significant difference from the 2014 option, below). Unforeseen electoral events such as by-elections or referenda in 2008 and 2009 would increase project and operational risks. This scenario would reduce the risk that public demand for electronic voting channels would get well ahead of readiness, and enable early benefits to be gained. The Chief Electoral Office would be perceived to be fully supporting e-Government initiatives and state sector development goals.



Comments

To achieve an e-voting pilot in 2014, Government policy approval would not be required until 2009. Further legal analysis, policy work (including public consultation), and legislative drafting would take place during 2009. This would enable Parliament to consider and pass enabling legislation during 2010. Budget approval for expenditure associated with this work would be required. Technical work on the pilot would commence after passage of the enabling legislation, finishing in 2012. Budget approval would be required in 2010 for expenditure associated with this work. In 2013, the Chief Electoral Office's procedures could be integrated and amended. This timeline leaves key policy decisions till after the 2008 election.

Risks and uncertainties

In this scenario the development of e-voting policy and legislative options does not coincide with the late 2007 - early 2009 period of intense policy-related demands on the Chief Electoral Office or the delivery of the 2008 general election. E-voting work streams through 2009 to 2013 should allow a 2014 pilot to be prepared with low project risk. Compared to the 2011 scenario, the additional resource and management requirements for the project would be reduced, but would still exceed current (2007) levels. Expectations of e-voting in 2011 would be disappointed, and opportunities to accelerate subsequent development would be limited by the 3 year electoral cycle and the need to retain a cautious step-by-step approach. There would be an increased risk that voter demands for electronic channels would get well ahead of readiness. The Office's support for e-Government initiatives could be perceived to be low.

23 Appendix 6, Summary of E-voting implementations

This summary is taken from Appendix 1 to Working Paper 1.

A working committee appointed by the Norwegian Minister of Local Government and Regional Development described the international experience of electronic voting up to December 2005[28]. These are summarised below, with updates in some cases.

The Nordic Countries

Sweden – investigations have concluded by not recommending e-voting. Swedish voters have great confidence in their elections, and voter participation is strong.

Denmark – electronic solutions have been tested in some local referendums, but no initiatives have been taken by national authorities.

Norway – four pilot projects have been run in local and regional elections, using a touch screen kiosk and a smart card for voter identification. Evaluations focussed on voter responses and the user-friendliness of the technology.

The United Kingdom

E-voting, primarily outside regular polling places, is playing a major role in electoral modernisation. The background for this is a serious decline in voter participation. Several experiments have been run, particularly at the local level, using a range of different technologies and suppliers. The most important issue for the British Electoral Commission is the security of electronic solutions, for which they have set a benchmark at least as good as the traditional methods.

Voting over the Internet – the voter could access the ballot receiver from any computer with Internet access. Voters logged on with a personal password obtained from their official polling card. Voters were able to confirm their choice, and received a receipt that their ballot had been registered. Evaluations showed up weaknesses including mailing PINs with polling cards in the same envelope, rather than separately.

Voting over the telephone – Free calls were answered by a machine and voters would log on by pressing a code supplied on a polling card. Voters then pressed candidate codes which would be read back to the voter for confirmation (or another choice). At the completion of the ballot there was voice confirmation that the vote had been registered. The Electoral Commission did not recommend this option for further use, for reasons of poor accessibility for people with disabilities, and confusion resulting from relatively complicated strings of numbers.

[28] *Electronic voting – challenges and opportunities*, Norwegian Ministry of Local Government and Regional Development, February 2006, available at http://www.regjeringen.no/upload/kilde/krd/red/2006/0087/ddd/pdfv/298587-evalg_rapport_engelsk201106.pdf

SMS messages – this solution was not interactive, and not free of charge. Casting of the vote took place with a single message containing the voter's code, the code for the district, and the code for the candidate(s). A return message confirmed the vote had been registered, but not the voter's choice. This solution was not viable for many people with disabilities, and was considered to have trivialised the act of voting.

Digital Television – a process was similar to voting over the Internet except using television menus to log on, rather than a computer keyboard.

Touch screen kiosks – these were set up in some cases as the only election day voting option, in some cases alongside paper ballot systems in polling stations, and in other cases in libraries and malls as supplementary alternatives to polling stations. In some municipalities, a smart card option facilitated registration.

The UK Electoral Commission was able to draw a number of lessons from these wide-ranging experiments (reports are available from the Commission's web site, http://www.electoralcommission.org.uk/about-us/publications.cfm).

The United States

E-voting in polling stations is now the custom in the US. Over 40 million electronic votes were cast in the 2004 presidential election. Voting over the Internet, on the other hand, is viewed with great scepticism because of concerns over Internet security.

The Help America Vote Act was passed after the 2000 elections, creating among other things, the Election Assistance Commission as a clearinghouse for information and review of procedures for the administration of federal elections. Federal legislation on elections is meagre because it is up to individual states, who may introduce electronic voting as one of, or the only, option(s). One state (Oregon) has adopted postal voting as the sole approach.

Estonia

The concept of e-voting, in the form of Internet voting in uncontrolled environments, was introduced in Estonia in 2001. The objectives were of: increasing participation by keeping voters interested; making voting easier; and keeping in touch with modern ICT. The first e-voting took place in local elections in 2005.

The Estonian system uses the personal ID card which every citizen is required to hold. This card is designed for use in all transactions that require secure user identification and legally binding signatures.

Voting over the Internet is made available only during the advance voting period (from the 13th to the 4th day before the election). To mitigate against the buying and selling of votes, and to avoid undue influence, multiple submissions of e-votes are allowed, but only the last vote is counted. Voting from home required a personal computer with Internet access and a smart card reader. In 2005, banks, government offices and telecommunications companies also provided voting facilities. 9000 voters

used the system in the 2005 election. (See below for an update which post-dates the Norwegian summary).

Switzerland

Switzerland has four to six elections or referendums each year, offering a lot more return from the introduction of e-voting than most other countries. Voter participation is weak, and led to the introduction of postal voting in most cantons about ten years ago. Internet voting is seen as a possible extension of postal voting, and surveys suggest that Internet voting is strongly supported (66 percent of voters want the opportunity).

Geneva was the first canton to use Internet voting, and the system has now been used a total of eight occasions since 2003 (with binding votes), including two national level referendums (though not elections to representative bodies). In the advance voting period, voters may vote by post or the Internet. Voting on election day must take place in a polling booth.

In 2005, four municipalities offered Internet voting in a federal referendum, and 23 percent of the votes in those districts came in over the Internet. In 2007, the national parliament is expected to make a decision about the introduction of e-voting nationwide. (Updated information in this section from[29]).

The Netherlands

E-voting in polling booths has been an option in the Netherlands since the late nineties. During the 2005 election for the European Parliament, voters living overseas had the opportunity to vote over the Internet or by phone. The reports of subsequent evaluations were published. Usability, particularly for older people, has been a strong consideration.

Post-dating the Norwegian report, overseas voters in the Netherlands 2006 general election also had the opportunity to register to vote over the Internet, using an authorisation code mailed to them in advance. Voters were able to select an option to check, over the Internet, that their votes were counted. A report by an invited assessment mission from the Organisation for Security and Cooperation in Europe (OSCE)[30] – which has an Office for Democratic Institutions and Human Rights (ODIHR) – noted that a total of 19,815 votes were cast this way, using a system developed for district water board elections (RIES) in 2004. The assessment mission identified several areas of potential security weakness or difficulties for observers to satisfy themselves that security requirements had been met. The mission reported a broad consensus among both developers and critics of electronic voting that RIES would not be a suitable system for expansion of Internet voting to the general population.

[29] http://www.lunchoverip.com/2007/05/the_swiss_evoti.html and *Swiss E-voting Pilot Projects,* Nadja Braun, presentation to Electronic Voting 2006 Conference, Bregenz, 2-4 August 2006, at http://www.monitortv.at/monitortv/website/evotingconference06/pdfs/Swiss_Experiences.pdf

[30] *The Netherlands: Parliamentary Elections 22 November 2006* , OSCE/ODIHR Election Mission Report, Warsaw, 12 March 2007, http://www.osce.org/documents/odihr/2007/03/23602_en.pdf

The report also noted that:

"Currently, in the Netherlands, electronic voting is overwhelmingly the preferred method, and it has broad public support based on a high degree of trust in government and the electoral authorities. Whilst there have been no suggestions that trust at any level has been abused, the OSCE/ODIHR EAM believes that there is now a timely opportunity to further enhance transparency of implementation of new voting technologies, and public confidence, in an increasingly questioning and sceptical public environment. In particular:

Electronic voting systems should be monitored by an independent entity distinct from the authorities responsible for conducting elections. Such an entity should have broad technical expertise, and should be also responsible both for formulating and reviewing voting system standards.

There should be routine testing of voting machines before elections, and randomly selected machines should be subject to testing by an entity other than local election authorities. Mechanisms should be considered to verify that voting machines, as used on election day, are configured with the approved firmware and ballot definition.

In order to enhance public confidence in DRE voting machines, and to provide for meaningful audits and recounts, legislation regulating use of such systems should include provisions for a Voter Verified Paper Audit Trails (VVPAT) or an equivalent verification procedure. Software dependent vote recording mechanisms which do not permit an independent check on their operation should be phased out.

Voting system standards should not permit the use of systems which depend for their security on the secrecy of any part of their technical specifications. Reliance on proprietary systems should be reduced, where neither citizens, nor electoral officials, nor observers can determine how they operate.

Source: pages 15, 16 *The Netherlands: Parliamentary Elections 22 November 2006* , OSCE/ODIHR Election Mission Report

Netherlands Internet and Telephone Voting Experiment 2004

In the European Parliament election of June 2004, the Netherlands Ministry of the Interior and Kingdom Relations conducted an experiment in which voters abroad were able to vote by Internet or telephone. The experiment was closely monitored, including voter feedback, and was generally considered successful[31].

The parameters of the experiment were:

- The experiment was authorised by an Act of Parliament. The Act required evaluations to be conducted, including of the voters' experience;

- The Municipality of The Hague's register of voters abroad (this is the national register for voters abroad) recorded 7197 voters who had registered that they wished to vote by Internet or telephone.

[31] *Report on the Internet and telephone voting experiment,* Netherlands Ministry of the Interior and Kingdom Relations, December 2004 http://www.minbzk.nl/bzk2006uk/subjects/constitution_and/internet_elections/publications

This was approximately 44% of those registered to vote in the European Parliament election;

- Voting documents for voters were produced (securely) with an explanatory letter, candidate lists, candidate codes and personal voting codes. Regular mail, diplomatic mail, and army mail were used to distribute the voter packs to voters in a large number of countries;

- Demonstration of Internet and telephone voting methods were provided (on the web site and on a special telephone line) in advance. These provided practice for voters and allowed them to check that their telephones and personal computers would be suitable;

- 480 votes were cast by telephone (9.0%) and 4871 via the Internet (91%). The 5351 total electronic votes represented 74% of the number of packs sent out;

- There were no problems experienced with attempts to misuse the voting service and no denial of service attacks. A few visitors to the voting website entered random access codes, and a few attempts to exploit 'standard' Internet vulnerabilities were observed;

- A help desk was available for several months, and during the ballot period it was staffed 24 hours/day. 423 queries were received during the voting period, mostly by email. The biggest problem was the non-delivery on time of the voting packs. Other reported problems were forgetting the access code, the Internet connection, and not being able to find the voting web site; and

- A special committee oversaw the experiment and the count.

Belgium

E-voting in the polling station was introduced in Belgium in 1991, mainly because the traditional voting procedure is very complex and time-consuming. E-voting has been used extensively since 1999. In 2003, 44 percent of votes were cast electronically. The voting machine is a personal computer with a screen, an optical pen, and a magnetic card reader.

Ireland

Test projects were run in 2002 with a view to using touch screen kiosks in the Irish Election for the European Parliament and local elections in 2004. The plans were put on hold when an Evaluation Commission had not assured itself that the system would work.

Others in Europe

E-voting in polling places was trialled in local elections in Brest in 2004..Pilots have been run in many constituencies in European Parliament elections and the referendum on the European Constitution in 2005.

Spain undertook small scale experiments during 2003 and 2004, and a larger pilot project in 2005 involved 10,000 electronic votes in a non-

binding referendum. Voters could use any Internet-connected computer and identified themselves with a smart card and PIN.

In Portugal, more than 9000 voters participated in an e-voting pilot in 2004, testing three different solutions: a touch screen voting machine; a light pen system; and an electronic card solution.

Romanian military personnel stationed abroad took part in a referendum pilot in 2003, using the Internet.

India and Brazil

Brazil in 2000 and India in 2003 held elections using e-voting in controlled environments, with the objective of making voting more accessible for illiterate voters. India has also had problems with sabotage of traditional polls. Around 370 million Indians submitted electronic votes using a million voting machines in the 2004 general elections. Voters used a button next to the candidates' names and symbols. The system has been criticised for lack of an audit trail or receipt to the voter.

Brazil has extended e-voting to the point where 400,000 voting machines were provided in the 2000 and 2002 elections.

Venezuela

The re-election of President Chavez, which was marked by claims of large scale electoral fraud, included the option of e-voting in polling stations. A review of election results, offered by election observers, was not accepted because of concerns the electronic re-count would not lead anywhere.

Australia

The Norwegian report from which most of the above examples have been taken did not take into account Australian e-voting experiences.

E-voting in the Australian Capital Territory (ACT) was reviewed by the ACT Electoral Commission in 2005[32]. The electronic voting and counting system first used in 2001 for the Legislative Assembly election was used again, in an improved form, for the 2004 election.

In 2004 a total of over 28,000 votes were recorded at four pre-poll voting centres and eight polling places on election day, an increase of 70 percent over the 2001 electronic vote total. Electronic votes represented 13.4 percent of all votes in 2004.

The review concluded there was robust security and ease of use for voters. In particular:

- the system (known as eVACS) eliminated the need for manual counting, thereby removing the possibility of counting error;
- was reliable and secure;

[32] *Electronic Voting and Counting System Review*, ACT Electoral Commission, a report to the Attorney General of the ACT Legislative Assembly, June 2005.

- significantly reduced the number of voter errors and contributed to an overall drop in the proportion of informal votes;

- allowed blind and sight impaired people to vote without assistance and in secret, through use of headphones and recorded voice instructions; and

- provided on-screen voting instructions in 12 different languages.

Preferences recorded on paper ballots under the ACT Hare-Clark electoral system were entered by two operators independently and electronically checked for errors, and combined with the electronic votes. The system proved accurate, reliable, and cost-effective.

While there were some public concerns about the need for a paper audit trail for electronic votes, the Commission was satisfied that the use of open-source software, independent audit of the software code, and security provisions (including physical security), ensured that the system was transparent and reliable.

The ACT Commission considers that electronic voting should be provided again in 2008, and will explore further technology enhancements.

In November 2006, the Australian State of Victoria conducted an e-voting trial for the vision-impaired. Private electronic terminals at six 'E-centres' allowed voters to cast their preferences unassisted using read-aloud software, headphones, and a modified numerical keypad. A touch screen with large print was also available for people with partial vision. This initiative contributed to the State goal of making voting as accessible as possible.

The Victorian system records votes and later prints out the corresponding ballot papers. This provides an auditable ballot trail. Voters have their names checked off the role in the traditional manner, but then receive a smart card containing their electorate details, and their audio and visual presentation preferences. The card is entered into a reader on the voting terminal. Disability groups submitted that this approach provided the ballot secrecy available to other voters. In the past, blind and vision-impaired voters have needed help to record their preferences.

Security features included:

- Recording votes in two different places in the computer - on the hard disk and on a USB key;

- An independent software module that reads votes back to the voter during the verification step, so that the voter can double-check the vote;

- Voting computers enclosed in sealed, transparent cases to prevent and detect unauthorised access to the computer;

- No connection to any network, making it impossible to access voting computers via the Internet;

- An uninterruptible power supply that allows the kiosks to operate for at least half an hour in the event of a power failure. This allows voters who have started voting to complete their vote. Votes already cast will not be affected by a power failure;

- Only authorised Victorian Electoral Commission (VEC) staff are able to view votes. This can only happen at the end of the election and must involve at least two election officials present together; and

- Extensive tests conducted by the VEC and an independent software auditor who has certified the source code to ensure that voting is secure, accurate and free from any malicious code. The software will only be used after it has completely passed these tests.

The intention is to extend these trials in 2010, possibly to include Australians living in Antarctica.

In April 2007 the Australian Electoral Commission announced[33] a trial allowing blind and visually impaired voters to independently vote using electronic voting machines in up to 30 locations at the 2007 federal election. A second trial will allow defence force personnel overseas to vote using the Department of Defence's secure intranet. Empowering legislation was passed in early 2007.

Estonia 2007

Post dating the Norwegian study, in March 2007 Estonia completed the first national elections at which Internet voting was open to all. 30,000 voters, about 3.5 percent of registered voters, had used the system when it closed on the Wednesday before polling day (Sunday). The system developers had conducted extensive trials, including a test run earlier in 2007 in which citizens voted for the "King of the Forest" in order to learn the process.[34] No media reports of problems with the Internet vote have been sighted, but a report can be expected from an observers' mission (under the auspices of the Organisation for Security and Cooperation in Europe) in due course. The Estonian National Electoral Committee has an English language website which includes a number of papers and a statistical analysis of the 2007 Internet vote[35].

Also since the Norwegian study was completed, the following developments have been noted from media reports:

- 26,000 Filipino voters registered in Singapore were to have been given the opportunity to vote over the Internet, however the threat of legal challenges and a Senate directive have resulted in these voters having to cast their ballots by mail. Internet voting will be available, but e-votes will not be tallied with the official votes.[36] (A

[33] *AEC advancing e-voting trials for the 2007 elections,* The Tally Board, Issue 3, April 2007
[34] *Estonians will be first to allow Internet votes in national election*, International Herald tribune, 22 February 2007, http://www.iht.com/articles/2007/02/22/business/evote.php
[35] Estonian National Electoral Committee website http://www.vvk.ee/engindex.html#0002
[36] *Internet voting results in Singapore nonbinding*, 28 February 2007, http://www.gmanews.tv/story/32427/

representative of the Chief Electoral Office NZ attended the final stages of the e-voting trial in August 2007).

- Honolulu, Hawai'i, will include an Internet option in the 2007 neighbourhood boards elections. It is a pilot project to enable greater participation in a cost-effective manner. The elections were previously held only by mail. The e-voting services will be provided by the same company that operates Kids Voting Hawai'i (an online programme that allows children to vote in mock elections that parallel the real ones). Voters will need to 'opt in' after receiving a voter number by mail.

- The Irish Commission on Electronic Voting completed its evaluation in July 2006[37] and many, but not all, of the original issues have been resolved or require relatively minor changes. The major remaining issue concerns not the voting machines but the administration's election management system. It appears that 7000 voting machines remain in storage.

- The UK Department for Constitution Affairs gave the go-ahead, despite some concerns of the Electoral Commission[38], for e-voting pilots to proceed in selected local body elections in May 2007, including Internet and telephone voting. A number of evaluations of these pilots are available. They are notable for criticism of the short timeframes allowed to local electoral officials to implement the pilots, and the consequent risks to the electoral process[39].

Other Implementations

This summary has not attempted to be comprehensive. For example, there have been successful implementations in a number of Canadian cities (e.g., Internet voting in Peterborough and Markham, Ontario). There are also many cases of electronic voting being used in commercial settings, and student and union elections.

In New Zealand (as elsewhere), Internet voting has been used successfully for several years by commercial and community organisations for board elections and similar purposes. Examples include Fonterra, Meat & Wool NZ, the WEL Energy Trust and others. Case studies are available from Electionz.com, the supplier of e-voting services in these examples. Internet elections for tertiary student associations have been organised by EVSL.

---

[37] *Second Report of the Commission on Electronic Voting on the Secrecy, Accuracy and Testing of the Chosen Electronic Voting System,* report to the Government of Ireland, July 2006, available at http://www.cev.ie/htm/report/download_second.htm

[38] *Minister ignores e-voting fraud warning*, Sam Coates, The Times, 2 March 2007, http://www.timesonline.co.uk/tol/news/politics/article1459274.ece

[39] See http://www.electoralcommission.org.uk/elections/pilotsmay2007.cfm and http://www.openrightsgroup.org/e-voting-main/ and http://www.aea-elections.co.uk/news/article.jsp?id=1093

24 Selected Bibliography

Full sources are cited in footnotes to the Working Papers (see Part 2 of the proposed strategy). The following were particularly valuable in forming the proposed e-voting strategy (web links were valid at the time of writing):

A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), Dr David Jefferson, Dr Aviel D. Rubin, Dr Barbara Simons & Dr David Wagner, January 2004, available at http://servesecurityreport.org

Electronic Voting and Democracy: A Comparative Analysis, Norbert Kersting and Harald Baldersheim, Palgrave Macmillan, 2004

Electronic voting – challenges and opportunities, Norwegian Ministry of Local Government and Regional Development, February 2006, available at http://www.regjeringen.no/upload/kilde/krd/red/2006/0087/ddd/pdfv/298587-evalg_rapport_engelsk201106.pdf

Electronic Voting Summary Paper: May 2007. Electoral Pilot Schemes The Electoral Commission of the United Kingdom, August 2007, available at http://www.electoralcommission.org.uk/about-us/statutoryreports.cfm

E-voting Security Study, Issue 1.2, Communications-Electronics Security Group (CESG), Government Communications Headquarters, UK Government, July 2002 Available at http://www.ictparliament.org/CDTunisi/ict_compendium/paesi/uk/uk54.pdf

Implementing Electronic Voting: a report addressing the legal issues raised by the implementation of electronic voting, Bob Watt (Senior Lecturer in Laws, University of Essex), March 2002, accessed from www.dca.gov.uk/elections/e-voting

Improving Access to Voting: A report on the technology for accessible voting systems, Noel H. Runyan, February 2007, available at http://www.voteraction.org/reports/improving_access.pdf

Legal, Operational and Technical Standards for E-Voting, Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe, 30 September 2004, Council of Europe Publishing (and the associated explanatory memorandum)

Polls Apart: developing inclusive e-democracy – an evaluation of the May 2003 electoral pilot schemes, Liz Daone, Gwilym Morris & Ruth Scott (Scope), commissioned by the UK Electoral Commission, available at http://www.pollsapart.org.uk/docs/e%20democracy.pdf

Pret a Voter: a Systems Perspective, Peter Y. A. Ryan and Thea Peacock, September 2005, available at http://www.cs.ncl.ac.uk/research/pubs/trs/papers/929.pdf

Report on the Internet and telephone voting experiment, Netherlands Ministry of the Interior and Kingdom Relations, December 2004, available at http://www.minbzk.nl/bzk2006uk/subjects/constitution_and/Internet_elections/publications

The Shape of Elections to Come: A strategic evaluation of the 2003 electoral pilot schemes ,The Electoral Commission of the United Kingdom, 2003, available at

http://www.electoralcommission.org.uk/files/dms/EC25(2003)TheShapeofElectionstocome_12091-8366__E__N__S__W__.doc

25 Project Members

25.1 Governance

Project Sponsor – Robert Peden, Chief Electoral Officer, Ministry of Justice

Business Owner – Kristina Temel, Manager Electoral Policy, Chief Electoral Office, Ministry of Justice

Project Manager – Kevin Ward, Management Integration Limited

25.2 Steering Group

The project reported to a steering group comprising:

- Robert Peden, Chief Electoral Officer, Ministry of Justice
- Gavin Valentine, Programme Manager, All of Government Authentication Programme, State Services Commission
- Robert McShane, Manager Local Government Policy, Department of Internal Affairs (later seconded to another department)
- Danny Mollan, Manager Architecture & Standards, Ministry of Justice
- Michael Petherick, Senior Adviser, Public Law, Ministry of Justice (for Lauren Perry, Policy Manager Constitutional)
- Kristina Temel, Manager Electoral Policy, Chief Electoral Office, Ministry of Justice
- Kevin Ward, Project Manager
- Lenore Simmonds, steering group support, Chief Electoral Office

25.3 Project Contributors

- Kevin Ward (Working Papers 1 *Strategic Context and Value*; 2 *Chief Electoral Office Voting Processes*; 4 *Guiding Principles*; 6 *Future Business Model, Chief Electoral Office*; 7 *E-Voting Issues.*
- Kristina Temel (Working Paper 5 *Legislative Analysis*)
- Tim Woodill, Infrastructure & Security Architect, Technology & Services, Ministry of Justice (Author, Working Papers 3 *Technology Options & Opportunities* and 8 *System Architecture, Integration & Requirements*)
- Anna Hughes, communications adviser.

26 The project was assisted by discussions with...

In no particular order:

Statistics New Zealand (e-Census Project)

Electoral Enrolment Centre, New Zealand Post

Electoral Commission

The Association of Blind Citizens

Independent Election Services

Electionz.com

Squiz.net

Diversityworks

Local Government New Zealand

E-government Strategy & Policy, State Services Commission

All of Government Authentication Programme, State Services Commission

Identity Verification Services Programme, Department of Internal Affairs

27 Acknowledgements

The entire Chief Electoral Office team made their expertise, time and resources available to the project without hesitation. The advice and input from Anthony Pengelly (e-voting, electoral information, statistics), John Lloyd (operations and procedures), Joe Glover (the electoral management system), Liz Ropeti (costs), Ross Shadbolt (field costs), and Lenore Simmonds (Steering Group support) was particularly appreciated.

Tim Woodill of the Ministry of Justice willingly invested considerable thought and expertise in system concepts and architectures.

The Electoral Commission (Helena Catt, Chief Executive and Peter Northcote, Communications Manager) generously provided the opportunity and expertise for questions relating to e-voting to be included in the Commission's 2007 public survey programme.