NSW Electoral Commission

iVote® Strategy for the NSW State General Election 2015

Key Issues, Guidelines, Application Architecture and Voting Protocol

March 2015

Amendment 4

New South Wales Electoral Commission
ABN. 94 828 824 124

Level 25
201 Kent Street Sydney NSW 2000
GPO Box 832, Sydney NSW 2001

Document Information

Criteria	Details
Document	iVote Strategy for the NSW State General Election 2015: Key Issues, Guidelines, Application Architecture and Voting Protocol
Document author	Ian Brightwell (iVote Manager)
Document owner	Colin Barry (NSW Electoral Commissioner)
Document location	

Contents

Glossary of Terms

Term	Explanation
The iVote® system	The NSWEC electronic voting system comprising software components, hardware, networking, procedures and protocols required to deliver remote electronic voting services for the benefit of eligible NSW electors.
iVote Core Voting System (or Core Voting System)	The software components or modules subject of this RFT, as described in the iVote high level solution architecture, together with their associated interfaces.
iVote Core Voting System solution	The iVote Core Voting System together with associated services for its implementation and support
Absent Vote	A vote made at a designated voting centre by an elector who is outside his or her own electoral district.
Attendance Vote	A vote made by an elector in attendance at a voting centre within NSW (e.g. Sydney Town Hall - STH) where a NSWEC appointed official is available to supervise voting. *(Note: Current legislation only allows iVote to be used at centres outside NSW, see "Remote Electronic Voting").*
By-election	An election held to fill a casual vacancy on a council or in the Legislative Assembly if an elected representative dies or retires.
Completed Virtual Ballot Paper (CVBP)	A used Virtual Ballot Paper containing the preferences as submitted by a voter on completion of the iVoting process.
Credential Hash	The Credential Hash is a number generated by combining the iVote Number and PIN and Salt using a hashing formula. The Salt is such a size that it is extremely unlikely that some randomly selected input text could produce the same hash value. The hash is used to ensure the iVote Number and PIN entered by a voter is valid by using the same hashing formula and Salt (see below) to convert the entered data which is then compared to the stored hash.
Credentials	Information used to identify an individual accessing the system – in the iVote system for an elector this includes a PIN number known only to the elector and an iVote number generated by the system.
Declaration Vote	A vote cast by an elector where the elector declares he/she is entitled to the vote. Typically the voted ballot papers are enclosed in an envelope containing a printed declaration signed by the elector. Envelope based declaration votes are postal votes, absent votes, enrolment votes and section votes. In district pre-poll and Declared Institution votes are cast as ordinary votes.
Declared Institution	A hospital, nursing home or other facility appointed by the Electoral Commissioner and visited by election officials to take votes from residents who are unable to attend a polling place on election day.
Disabled Voting	Voting by an elector who has a disability (within the meaning of the *Anti-Discrimination Act 1977*) and because of that disability has difficulty voting at a polling place.

Term	Explanation
District	Used for state elections, districts are geographical regions with clearly defined boundaries shown on electoral district maps containing approximately equal numbers of voters. Each district is represented by one of the 93 NSW Legislative Assembly seats. For the Legislative Council, the district is the whole state.
Election Management Application (EMA)	A NSWEC developed computer system to undertake administrative tasks including nominations; processing declaration votes and election results.
Elector	A person who is on the electoral roll and certified to vote in an election.
Hashed PIN	The result of applying a one-way cryptographic hash function to a PIN, plus salt, supplied by a elector/voter. Only the hashed PIN is transferred between iVote systems.
Informal vote	A ballot paper left blank and that is therefore excluded from the count. It does not contribute to the election of a candidate.
iVote system	The NSWEC electronic voting system comprising software components, hardware, networking, procedures and protocols required to deliver remote electronic voting services for the benefit of eligible NSW electors.
Legislative Assembly (LA)	The Lower House of the NSW Parliament has 93 Members, 1elected from each district.
Legislative Council (LC)	The Upper House of the NSW Parliament has 42 Members elected for an 8 year term, half of whom are elected at each general election.
Local Government Area	A subdivision of the state into geographical areas that councils are responsible for.
Nomination(s)	The process by which a person applies to become a candidate for a State or Local Government election. In this RFT used as a term for all data that is a result of that process.
NSWEC	New South Wales Electoral Commission (ABN 94 828 824 124)
Optional preferential (voting)	A voting system in which an elector shows by numbers their preferences for individual or groups of candidates but need not show a preference for every candidate or group listed.
PRCC	Proportional Representation Computer Count system
Referendum	A vote taken to allow electors to express their view on a specific subject or issue.
Remote Electronic Voting (REV)	Electronic Voting - From a location of the elector's choice using a device not provided or directly managed by the electoral authority. - At a voting centre that is located outside of NSW using a device provided by that voting centre (Remote Venue voting). Registration and voting are performed on same computer. - By phoning the Voting Call Centre. The call operators use the remote voting system on the elector's behalf and cast the vote under their instructions.
Remote Mobile Voting	Mobile pre-poll voting at remote locations across the State.

Term	Explanation
Pre-Poll (vote)	Electors who cannot vote on election day can vote early at a (pre-poll) voting centre; electors have the option of using iVote, either Remotely (if eligible) or by Attendance in venues such as STH, to cast a pre-poll vote.
Salt	A secret number combined with the PIN and iVote number to make breaking the Credential Hash difficult using brute force approaches.
SGE 2015	The NSW State General Election to be held in March 2015.
SPID	SmartRoll Person ID. A unique voter electoral identifier (held in the electoral roll).
STH	Sydney Town Hall. A Voting Centre based in the Sydney Central Business District.
TPC	Two Candidates Preferred count. Two candidates preferred count refers to a distribution of preferences of the two candidates who are expected to come first and second in each electoral district. Often, but not always, these will be the candidates representing the Labor party and the Coalition (Liberal and National parties).
Virtual Ballot Box (VBB)	A data base corresponding to a physical ballot box in which the cast iVotes are accumulated
Virtual Ballot Paper (VBP)	A blank or empty electronic ballot paper unique to each registration by a voter which is associated with the Credential Hash and available in the Core Voting System for electors to cast their vote.
Voting Centre	A venue where a NSWEC appointed election official supervises voting. These venues can either be either inside or outside NSW.
Ward	Subdivisions, with approximately equal numbers of electors, of a local government area.

1 Introduction and purpose

This document has been prepared by the NSW Electoral Commission to provide an overview of the strategy proposed for the use of the NSW electronic voting system (the iVote® System) for the State General Election in 2015 (SGE 2015). Its purpose is to provide the public, election participants and other interested stakeholders with information about plans for the iVote® system in order to allow informed comment.

Electronic voting (eVoting) is a voting process which uses electronic or computerised equipment to provide part or all of the vote-casting and vote-collection process. The enabling legislation for eVoting in NSW[1] requires the implementation of a Remote Electronic Voting (REV) system. The NSW REV approach as used in 2011 allowed voters to cast their vote using telephones[2] or computers with browsers and Internet access. This approach was selected to meet the needs of the Blind and Low-Vision (BLV) community, which was the group of electors most active in advocating for the introduction of the iVote® system for the 2011 election[3].

Notwithstanding the need to support BLV voters, legislation provides for the system to be used by remote electors, both those who live more than 20 km from a polling place and those who are out of state on Election Day. In the future, changes to legislation could extend eligibility to include other categories, such as those unable to get to a polling place on Election Day.

As a result of the success of iVote® at the 2011 election[4], the NSW Joint Standing Committee on Electoral Matters (JSCEM)[5] supported its use at the next SGE in 2015 following improvements related to transparency and voter confidence[6].

> *In conclusion, the Committee supports technology assisted voting and recognises the NSWEC's considerable progress to date. In the run-up to the 2015 election it is to be*

[1] *Parliamentary Electorates and Elections Act 1912 No 41, Part 5, Division 12A, Technology assisted voting*

[2] Using Dual-tone multi-frequency signalling (DTMF)

[3] NSW Electoral Commission, Report on the Feasibility of providing “iVote” Remote Electronic Voting System, 23 July 2010
http://www.elections.nsw.gov.au/__data/assets/pdf_file/0006/84498/20100723_NSWEC_iVote_Feasibility_Report_.pdf

[4] Evaluation of technology assisted voting provided at the New South Wales State General Election March 2011, Report to the New South Wales Electoral Commission, 11 July 2011
http://www.elections.nsw.gov.au/__data/assets/pdf_file/0004/93766/July_2011_Final_ACG_iVote_Report_ELE01-C_Final.pdf

[5] The Joint Standing Committee on Electoral Matters is a committee of the NSW Parliament, which inquires into and reports on matters relating to the *Parliamentary Electorates and Elections Act 1912* (other than Part 2) and the *Election Funding, Expenditure and Disclosures Act 1981*

[6] Parliament of NSW, Joint Standing Committee on Electoral Matters, Report 2/55 – 20 December 2012, section 4.91
http://www.parliament.nsw.gov.au/Prod/parlment/committee.nsf/0/129dfc87035dd10eca257ad10013144d/$FILE/Report%202-55%20(Administration%20of%20the%202011%20NSW%20Election).pdf

> *hoped that further technological developments and the experiences of electronic voting in other jurisdictions will provide the NSWEC with the means to make further progress and address some of the issues raised during the inquiry, particularly in relation to transparency and verifiability.*

The NSW Electoral Commission (NSWEC) has received funding for the financial years 2013/14 and 2014/15 to implement and operate a new version of the iVote® system for the SGE 2015. This funding will be adequate to cater for the elector eligibility requirements of the current legislation. It is expected that with the current elector eligibility conditions, that the iVote® system will issue around 200,000 votes at the SGE 2015.

Given the NSW government support of the iVote® system for SGE 2015 and the size and complexity of the project, the NSWEC commenced procurement of an iVote system in July 2013. A tender was issued for a new core voting system late in calendar year 2013, with a contract signed in May 2014.

The remainder of the discussion paper is broken into the following parts:

- a discussion of key issues related to electronic voting in NSW;
- a guideline for the proposed implementation of iVote;
- an outline of the voting protocol proposed for NSW; and
- an overview of the proposed iVote® Data Management and Application Architecture.

The document also outlines recommended extensions to the iVote® system and legislative changes as a result of JSCEM recommendations[7] and to facilitate improvements proposed by the NSWEC.

The implementation of the iVote® system as proposed for the SGE 2015 requires a number of key activities from July 2013 through to the election in March 2015:

- redevelopment of the iVote software application to meet expanded requirements;
- operational planning, development of procedures and implementation of the iVote® system for the SGE 2015; and
- stakeholder consultation and communications to ensure that the iVote® system effectively meets the needs of electors in NSW.

A preliminary schedule of key tasks comprising these activities is provided in Appendix A.

[7] Parliament of NSW, Joint Standing Committee on Electoral Matters, Report 2/55 – 20 December 2012 - Ibid
http://www.parliament.nsw.gov.au/Prod/parlment/committee.nsf/0/129dfc87035dd10eca257ad10013144d/$FILE/Report%202-55%20(Administration%20of%20the%202011%20NSW%20Election).pdf

2 Background and Key Issues

2.1 Why implement iVote?

The main reasons for implementing the iVote® system in NSW are to:

a) Improve enfranchisement of electors who would otherwise not be able to vote independently or have significant difficulty voting using an existing channel.

b) Improve enfranchisement of electors who would, by virtue of location during the election period, not otherwise be able to vote or have significant difficulty voting using an existing channel.

c) Reduce systemic errors in current voting processes. This would include reducing informality in ballots cast, reducing loss of ballot papers in transit between the voter and counting centre, as well as reducing transposition and counting errors.

d) Reduce cost of voting and risks of failure associated with the management of postal voting.

2.2 Research versus Current Practice

Significant research into electronic voting systems has been conducted over the past 10 years. Most of this effort has been focused on the technology of a voting system capable of delivering absolute proof that an election outcome can be trusted. Unfortunately, the research has so far only been able to provide trust for limited parts of the process using mathematically complex proofs, which require significant mathematical knowledge to understand. Although research of this nature is important, it has not as yet produced a totally secure and reliable electronic voting system which removes all the known risks.

Current Remote Electronic Voting systems (REV) mitigate the risks by a mix of people, process and technology to give electors a high level of confidence in the electoral outcome. The following strategies are currently used by the NSWEC to mitigate the known risks associated with electronic voting systems:

- Comprehensively testing the system to ensure it operates as per specification. This should be done before, during and after the election event.
- Independent reviewing to ensure the code only does what is required by the specification.
- Ensuring system availability by replicating it at an independent site.
- Protecting the system by interposing a high capacity website filtering service in front of the core voting system as a defence against volume attacks and malicious access.
- Periodic backing up of data in a live system and storing it at an independent site to allow second level of recovery and time sliced auditing.
- Segregating duties of system operators to reduce potential of insider attack.

- Segregating data and system functions to remove single security breach resulting in compromise of the iVote system.
- Limiting operator access to only those parts of the system necessary to perform the tasks required.
- Supervision of operators when interacting with the system to limit the ability of any one person tampering with the system without another knowing.
- Logging all system activity and monitoring logs for nefarious activity.
- Reporting iVote results separately, allowing comparison with other voting channels.

The above controls have proven effective in managing many high security systems. Although these approaches individually do not provide absolute certainty, when deployed in combination they will give a high level of confidence to system managers and the voting public that the electronic voting system's results can be trusted.

2.3 Verification

2.3.1 Secrecy and Verification

A feature of electoral environments in western democracies is that an elector's vote is secret. Put simply, this means that only the elector knows how he/she has voted. This feature of electoral environments creates a potential issue for electronic voting systems. The main control used in most computer based systems to ensure transaction integrity is to allow computer operators to view and validate transactions at all stages of processing. If this control was possible in an electronic voting system, it would jeopardise the secrecy of the elector's vote, as the electoral authority would know how an elector voted.

The iVote® system has been designed to ensure the electoral authority can never know how a given elector voted. This is achieved by the system removing the elector identifier from the vote as cast prior to the vote being decoded.

Additionally, through a combination of actions by the voter and the NSWEC, it can be reasonably shown that:

- the vote was cast as intended;
- the vote was included in the final results of the election; and
- the NSWEC does not know, nor is able to find out through normal system operations, how a given elector voted during or at the end of the election.

This approach satisfies recommendation 11 of the NSW JSCEM report[8] which says;

> *The Committee recommends that the NSWEC develop and implement voter preference verification for voters using iVote at the 2015 State election.*

[8] Parliament of NSW, Joint Standing Committee on Electoral Matters, Report 2/55 – 20 December 2012 - Ibid, Recommendation 11.

The iVote verification approach is not full "Universal Verification" or "End-to-End" verification which are defined[9] as:

> *A system is voter-verifiable if any voter can verify that his/her vote was correctly recorded and is included in the tally. A system is universally-verifiable if anyone can verify that all recorded votes are properly tallied. A system having both properties is end-to-end verifiable.*

The iVote® system uses a partial "End-to-End" verification approach. This is achieved by allowing the voter to verify their own vote and then the NSWEC to verify that all votes in aggregate are counted as cast. The NSWEC achieves this by using a mixture of people, process and technology and minimises the role of cryptography to achieve a trustworthy election outcome.

This makes it simpler to describe the verification approach to electors and key stakeholders and will provide confidence that the final count reflects the collective voter intentions. The approach selected by the NSWEC to undertake vote verification balances the following issues:

- The time taken to vote and the voting process complexity versus the potential for coercion/intimidation of the elector. Coercion is only a limited issue for the iVote® system as the elector can recast their vote prior to close of poll.
- The ability of the iVote users to comprehend the verification process versus a mathematically provable and intrinsically complex process. The verification process should be sufficiently straightforward such that most electors can understand its concepts and know who they are trusting to make it work. The verification process should be simple enough for electors to understand, so that a positive outcome will engender reasonable *confidence* their vote has been counted. It does not require an advanced level of understanding of complex mathematical algorithms.

The NSWEC does not believe that a Universal Verification approach is suitable for iVote, and therefore it is not proposed for the SGE 2015. The technology is currently unproven and relies heavily on trusting cryptographic experts. The Universal Verification approach is still an area for research, and no trials or public elections as complex and large as the NSW general election have used a Universal Verification approach.

Additionally, the implementation of a Universal Verification approach increases the complexity of the election protocol and reduces the ability of electors, stakeholders and the electoral authority to understand the system and be confident in its results. Given the complexity of Universal Verification approaches, the only people who can attest to the correct operation of the Universal Verification election system are a limited number of cryptographers. This means the validity of an election, which uses a Universal Verification approach, and which relies on public examination for integrity, will have to rely on the

[9] A New Implementation of a Dual (Paper and Cryptographic) Voting System, Jonathan Ben-Nun1, Niko Farhi1, Morgan Llewellyn2, Ben Riva1, Alon Rosen3, Amnon Ta-Shma1, Douglas Wikström, Tel Aviv University Israel.
http://www.e-voting.cc/wp-content/uploads/downloads/2012/10/315-329_Farhi_New_Implementation_of_Dual_Voting_System_corrected.pdf

declaration of people who claim to have the cryptographic knowledge to determine whether or not the system operated as intended.

2.3.2 Coercion and Voting Receipts

An additional desired feature of electoral systems is that the elector should not be able to prove how he/she voted to any other person. However, in many countries like Australia, this feature is not considered mandatory[10]. The iVote® system being a REV system is like postal voting and is not able to satisfy this feature. Also the NSWEC is not willing to introduce complex encryption to try and obscure the electors' preferences as this introduces more complexity and confusion into the voting process.

2.4 Transparent and Project Governance

The iVote® system to be implemented at the SGE 2015 will be managed under a governance structure to ensure transparency and information disclosure. The governance structure will include a best practice approach to project and programme management as typically applied to all NSWEC projects. However, for the iVote® project this will be tailored to be suitable for proposed participation by external stakeholders and a public audience in addition to internal NSWEC management processes.

The following documents will be prepared by project team members or advisors as part of the iVote® project and published on the NSWEC website:

- Approved Procedures;
- Project Charter;
- Risk Register which would be seeded from a rigorous Threat and Risk Assessment;
- Standards Compliance Assessment;
- System Architectural Overview;
- Voting Protocol;
- Pre-election System Security Review;
- Pre-election Source Code Review;
- Post-election System Integrity Analysis;
- Post-election Result Audit; and
- Governance and Manual Procedures Audit.

In addition to publishing the above documents the NSWEC will publish updates on progress of the iVote® project.

[10] Internet Voting and Voter Interference, A report prepared for the New South Wales Electoral Commission, March 2013.
http://www.elections.nsw.gov.au/__data/assets/pdf_file/0003/118380/NSWEC_2013_Report_V2.0.pdf

2.5 Stakeholder consultation and communications

The NSWEC plans an extensive program of consultation and communications to ensure that the iVote® system proposed for the SGE 2015:

- effectively and appropriately addresses the needs of voters in NSW; and
- engenders a high degree of trust amongst stakeholders so that the objectives of security, reliability and secrecy are met.

The redevelopment of the iVote® system is being undertaken by suitably experienced software developer(s) selected following rigorous evaluation processes. In addition, the NSWEC has appointed specialist contractors to provide expert services in relation to:

- quality assurance and testing processes;
- system security;
- risk management; and
- systems audit.

Consultation and communications are planned to be undertaken through several groups to be established in the early stages and expected to be active throughout the project up to the SGE 2015. Also, general communications will include publication of key project documents and update bulletins throughout the project, to the press and through the NSWEC public website.

Stakeholder consultative groups include:

- Technical Advisory Group
  membership by invitation by the NSWEC, on the basis of expertise and ability to make a contribution to the design and implementation of iVote, and subject to confidentiality conditions;
- Stakeholder Reference Group
  membership by invitation by the NSWEC, based on involvement with aging, disabled, vision-impaired and other target voter categories, involvement in political processes and ability to make a contribution to understanding the requirements of these stakeholders; and

2.6 Source Code Access

The NSWEC will allow e-voting experts who are members of the Technical Advisory plus expert consultants to scrutinise the iVote® system. However, the NSWEC believes it is important that expert reviewers do not diminish the trust placed in the Electoral Commissioner and the electoral process through sensationalised public comment. Also the involvement of members of the Consultative Group should not add significantly to the cost of running the election.

The NSWEC believes that unfettered access to source code by the general public would not be in the best interest of the State. In particular, the NSWEC believes that the publication of source code on the NSWEC website may result in one or more of the following outcomes:

- Increase the risk of a security breach by providing information which may assist in attacks on the core voting system.
- Increase the cost for the project as a result of:
  - effort required by the NSWEC to publish code in a suitable form for public review;
  - answering poorly considered questions from members of the public who do not have the skills required to undertake an effective review of the code; and
  - increased payment to contractors to compensate for the potential loss of intellectual property.
- Increase the potential for misinformation being circulated in the community through reviewers making ill-considered comments or comments influenced by self-interest or as a result of the reviewer's inability to understand the code.

The NSWEC considers that in striking the correct balance between security and transparency, source code and other iVote® related information should only be available to members of the public who satisfy the conditions outlined below and apply in writing. They will be selected from their applications before they are allowed access to iVote project information. Their applications will need to demonstrate they have the specialist skill and knowledge to effectively assess the iVote® system and provide useful comment. They will be required to:

a) agree to keep information provided, and to undertake the review, in a secure manner, and to not provide it to unauthorised person/s or organisation/s without the expressed written permission of the Electoral Commissioner;

b) agree to provide all comments about the iVote® system to the Electoral Commissioner in a written form and not make further public comment on the code (unless required by law or to the Electoral Matters Committee) until after expiry of the period during which the election can be contested in the Court of disputed returns; and

c) undertake the review of the iVote® system solely for the benefit of the electors of NSW.

2.7 Difficulties with Postal Voting

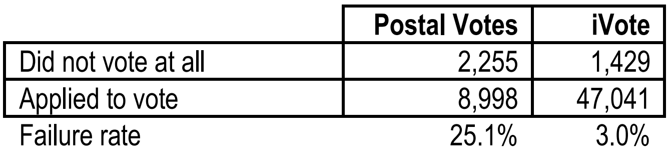
Postal Voting is becoming increasingly problematic as an effective channel for remote voters. As use of postal services declines in the face of digital alternatives, so will service levels of first class mail. It can be expected that in the not too distant future, reduced postal service delivery schedules will challenge the feasibility of completing postal vote application, ballot distribution and return within election timetables to the point where, for many electors, postal voting ceases to be a viable voting channel. Australia Post in their 2012 annual report[11] said:

> *At Australia Post, the impact of digital substitution on our traditional core business reached a tipping point in 2008–09, when the combination of the global financial crisis and electronic substitution contributed to the first significant year on year*

[11] Australia Post 2012 annual report, http://auspost.com.au/annualreport2012/chairmans-message.html

> *decline in the volume of mail posted by Australians (up until 2000, our letter volumes had grown – or contracted – in tandem with GDP)…. Unfortunately, Australian mail volumes have not recovered since – and this year our total addressed mail volumes were 17 per cent lower than the mail peak of 2007–08. While the Internet and digital communications are causing the steady erosion of our mail volumes*

Combine the above issue with the fact postal voting for Interstate and Overseas voters compared to iVote® gives a much poorer outcome i.e. 22% more Interstate and Overseas electors successfully vote using the iVote® system compared to postal voting.



	Postal Votes	iVote
Did not vote at all	2,255	1,429
Applied to vote	8,998	47,041
Failure rate	25.1%	3.0%

Voters shown as “Did not vote at all” are voters who did not vote some other way and did not return their postal or vote using iVote® after registering. As the iVote® system could only identify interstate and overseas as a group, this group was the only reliable point of comparison with postal voters.

3 Maintenance of Elector Trust

The following are the key controls to be used by the iVote® system for the SGE 2015 to support elector trust:

- **Identify any instances of elector impersonation** – registered iVote® electors, who did not use two factors when registering, will be sent an acknowledgement letter to their registered enrolled address, advising them of their iVote registration and requesting they notify the NSWEC if they did not register for iVote.
- **Limit voter coercion** – allow voters the ability to re-register and re-vote up to the close of the election under controlled conditions.
- **Confirm to remote voters that their vote was cast as intended** – allow voters the ability to verify that their vote preferences were captured as intended by providing the voter with their captured preferences through another communication channel.
- **Remote votes are not tampered with during the election** – require an auditor to confirm that electors' votes as cast are in aggregate the same votes decrypted at the close of the election.
- **Votes verified are included in the count –** the receipt number provided to the elector at the time of voting is published to advise the elector their vote was included in the count.
- **Votes are correctly counted** – provide a full list of all formal votes with all preference markings for any member of the public to undertake their own vote count and compare to the results published on the NSWEC virtual tally room website.

4 Implementation Guidelines

The implementation of iVote for the NSW SGE 2015 will follow the guidelines below. These guidelines broadly align with internationally accepted standards and only deviate from these standards where the Commissioner considers such deviation as appropriate considering NSW jurisdictional issues.

4.1 Electoral Environment

The following will be respected when introducing the iVote® system:

a) iVote® should only be available to electors who qualify under approved eligibility grounds and register to vote electronically;

b) the introduction of the iVote® system should augment current voting channels;

c) voters can make an informed decision to cast their vote using the iVote® system, based on a clear understanding of the level of privacy and security provided by iVote

d) within the constraints of legislation, the NSWEC will provide access to party and candidate information, to voters who are using remote electronic voting at or before the time of voting;

e) election results from the electronic voting channel should not be reported in sufficient granularity to allow electors' preferences to be deduced by the public;

f) the overall risks associated with the iVote® system will be commensurate with other forms of voting available to electors;

g) iVote® will commence remote registration for voting at the same time postal vote registration commences;

h) iVote® will commence voting at the same time pre-poll voting commences;

i) iVote® will close registration for remote voting at the same time as pre-poll voting ceases;

j) iVote® will allow re-registrations from the time pre-poll voting starts to 6pm EST on election day;

k) voting at designated remote venues will occur from the commencement of pre-poll to close of pre-poll;

l) iVote® will cease accepting votes at 6pm EST on election day.

4.2 Controls and System Features

The iVote® channel will have the following controls and system features.

a) Electronic voting will comprise no more than 15% of the votes cast for any one electoral contest. This limitation will allow comparisons of results with other voting channels which have similar electoral demographics. Hence a substantial difference in the percentage of first preference results by candidate or group would highlight if tampering has occurred within the electronic voting channel. Limiting votes taken can be achieved by reducing eligibility for categories of iVote® during the registration period.

b) Provide as part of the results reporting all the formal ballot paper preference markings in an electronic format. This will allow independent checking of the count.

c) Vote-as-cast verification will provide the elector access to the full details of the cast vote as seen by the elector at the time of submitting the vote. Access to the verified vote is available to the elector prior to close of voting. Access will require the entry of credential information (iVote® number and PIN), plus an additional Receipt Number provided at the time of voting[12]. Vote-as-cast verification will be via a phone-based voice response system.

d) After close of voting, electors will be able to confirm that their vote was counted by entering the Receipt Number provided to them at the time of voting on the verification page on iVote website (www.ivote.nsw.gov.au).

e) Independent auditors will confirm that the votes held in the verification system are the same as votes counted. This verifies there has been no vote tampering as the vote passes through the iVote® system.

f) The NSWEC will record and report the number of electors who require re-registration, declare they did not register when sent a letter advising of a registration in their name, or identify problems accessing the electronic voting system. All these incidents will be reviewed by an independent auditor to ensure the integrity of the iVote® system.

g) Independent auditors will review the implementation and operation of the system and provide an audit report to the NSWEC for public disclosure.

h) Instances of voter impersonation will be identified by electors declaring they have been impersonated after receiving notification at their enrolled address that they had registered to iVote® and they knew they had not registered. This will be achieved through the registration process sending an acknowledgement letter to the enrolled street address (or, if provided, the enrolled postal address) of the registering iVote® user. This approach will identify if large scale impersonation has occurred and allow the NSWEC to remove the impersonated ballots prior to the close of the election.

[12] Internet Voting and Voter Interference, A report prepared for the NSW Electoral Commission, Associate Professor Rodney Smith, Department of Government and International Relations

University of Sydney, Sydney, March 2013

http://www.elections.nsw.gov.au/__data/assets/pdf_file/0003/118380/NSWEC_2013_Report_V2.0.pdf

The NSWEC considers the benefit in confidence to the elector of being able to see their vote as cast when retrieved from the iVote system, is greater than the need to minimise the potential that the voter could be coerced. Most coercion resistant systems rely on vote verification being done using complex mathematical algorithms which can only be decoded with a coding sheet sent separately to the elector. These systems are difficult for electors to understand and add risk to the electoral process as they are difficult to manage. The NSWEC believes that the use of coercion resistant processes will potentially increase an elector’s uncertainty in the integrity of iVote rather than improving their confidence in the system.

i) A Virtual Ballot Paper will only be created when a person registers. Credentials will be unique to the registering voter which reduces the risk of votes being submitted by selecting random credentials.

j) Complete iVote® credential information will be known only to the registered elector. The system will be designed such that under normal operation (i.e. the system has not been compromised) only the elector will possess voting credentials[13].

k) The iVote® system will limit the number of unsuccessful attempts a given iVote Number can be used to access a vote from a given IP address. In particular, access to the iVote system will be restricted for IP addresses which make a significant number of unsuccessful access attempts. Similarly, IP addresses from which a large number of votes are taken will be investigated to ensure this is reasonable.

l) Once a vote has been successfully submitted by the elector, the vote credentials will become unavailable, thus preventing their reuse. Should a voter try to vote using a valid iVote® number and PIN credential for a vote already cast the system will advise the voter that the vote has been cast and that they should apply to re-register. Re-registrations of this type will be advised to the iVote® Manager and verification auditor when they occur for investigation. Votes cast using the iVote® system, available for inclusion in the count, will be limited to those votes which have been accepted during preliminary scrutiny. These votes will not be accepted if the voter has already had a vote accepted using another voting channel.

m) All iVotes cast remotely will be held in the Verification system in an encoded form allowing electors the opportunity to view their vote as cast and captured by the iVote system. This feature will be available to electors using the iVote® system at any time up to the close of remote voting.

n) Voters will have the option to re-register and re-vote by contacting the registration call centre. Provided the NSWEC call centre operator is confident of the voter's identity based on their response to questions, the voter will be issued a new iVote number. This process will then mark as deleted the current vote for the Voter and create a new Virtual Ballot Paper. The Voter can then proceed to recast his/her vote by computer or phone as previously.

o) Votes cast using the iVote® system will be encoded and managed in such a manner as to prevent an election official or any other person from determining how a given elector cast their vote and will allow the NSWEC to identify if a vote was altered after being encrypted.

[13] Typically this would entail at the time of registration an elector providing a credential to the NSWEC (the PIN). Then the NSWEC would provide the elector with a unique electronic vote identifier (the iVote Number). Only when the iVote Number has been distributed can the electronic ballot paper be created and made available for the elector to vote. The NSWEC will not hold the elector PIN and iVote Number and only retain the hashed credential. Encoding of the combined credential to a hash will be done using a secret Salt to limit the possibility of brute force decryption by external persons therefore preventing other persons from determining the elector's PIN and vote identifier.

p) The iVote® procedures will require that at least two authorised election officials, witness all manual tasks performed on the system which could influence the outcome of the election.

q) Voter identification data will be separated from the vote as cast before the vote is decoded, therefore preventing the voter's identity from being determined.

4.3 Integrity

The NSWEC will ensure that iVote system is secure and operated in a manner which minimises the risk of vote tampering and maximises electors' confidence in the electoral outcome.

a) The Commissioner will appoint a person to be the iVote Manager.

b) iVote® Systems will be "locked down" and managed in such a manner that only the Commissioner and iVote® Manager will have the ability to access the system. Prior to lockdown, access to the iVote® system will only be provided to staff for the level required by them to perform their prescribed function and only with appropriate supervision. The lock-down will occur when an approved version of the iVote® software is installed and configured, and as soon as the final testing is complete. This will only be done after iVote has been independently verified.

c) Only approved and tested software applications will be used for production voting. The production server will limit applications it can run by using a "white list" approach. The "white list" will allow only tested and approved software to operate.

d) All internal network routing between computers and network devices will be configured in such a manner as to ensure, during normal operation, data can only travel to those computers and ports required to operate the iVote® system.

e) The iVote® system will log and monitor all relevant system activities and configuration changes. The logs will be immutable. The logs will not capture information which will allow a vote's preferences to be explicitly associated with a given voter.

f) A snapshot of the system will be taken by an auditor during the system's operational period at a time selected by the auditor and compared to a benchmark approved system. This could be further strengthened by digitally signing the approved system executables and verifying their integrity on a continual basis during the operational period

g) Hardware and software shall be penetration tested by qualified technicians prior to commencement of the voting period and shown to be resistant to known relevant threats.

h) Critical software elements of the iVote® system will be independently reviewed at the code level to identify non-compliance with specification as well as potential flaws or faults, which may allow the software to be compromised.

i) The NSWEC will implement a risk assessment approach to determine if the iVote® system is suitable for live operation. This would also have a degree of independence to increase public confidence.

j) Vote-as-cast verification will be provided via an independently hosted and managed system.

k) The NSWEC will ensure that the iVote® system is fully backed up periodically during operation to an independent site. This will allow audit verification of the system in various stages of the election should it be needed and allow recovery should both the primary and replicated system become corrupted or destroyed.

l) The iVote® core and verification system will be hosted in at least a tier 3 data centre, separated from the NSWEC's own network, registration system and the iVote® audit system. These systems will also be managed independently with clear legally enforceable reporting responsibilities for each module's manager. This approach will reduce the risk that a single breach of security of any one system or management group would impact voter secrecy or vote integrity.

m) The internet facing components of the systems will be protected by internet filters which will be able to detect and prevent nefarious internet activity designed to harm the iVote® system.

4.4 Consultation and Transparency

The iVote® system will have a similar or improved electoral integrity and transparency to the voting channel it supplements or replaces.

a) Appointed Scrutineers can have supervised access to all relevant elements of the project from the issue to the return of the Writ(s).

b) Source code will be available for inspection to suitably qualified persons who are willing to comply with the NSWEC's terms of engagement (see Section 2.6).

c) The NSWEC will publish all review documents provided as a result of work completed in item b) with a NSWEC response.

d) The NSWEC will publish key project documents during the course of the project (see Section 2.4).

e) The iVote® logs during the voting period will be available for inspection to suitably qualified persons who are willing to comply with the NSWEC's terms of engagement, during and after the election to the extent legislation allows and to a level which will ensure the secrecy of an elector's vote and system integrity. These logs will be used to ensure that the votes counted match the votes entered and the system has not been compromised.

f) The NSWEC will fully inform stakeholders of the operation of the iVote® system.

g) The NSWEC will consult with low vision and disability bodies to ensure that all critical aspects of their requirements are satisfied and the most appropriate solution for NSW is implemented.

h) A survey of electronic voters will be implemented after the election. The survey will, amongst other issues, assess trust in the iVote® system.

i) The NSWEC will implement a public information and education campaign to ensure electors are aware of the security and secrecy features of the iVote system.

j) The NSWEC will consult as necessary with organisations or individuals who are willing to work with the NSWEC terms of engagement and have appropriate skills and knowledge to assess the system meets stated specifications or reasonable community expectations.

4.5 Usability

The NSWEC will ensure that the iVote® system will be usable by implementing the following:

a) The system will be tested by potential voters for the purposes of improving the voter experience and gauging the level of trust prior to the election.

b) iVote® telephone voting system will be implemented in compliance with the Australian Electoral Industry Standard "Automated Telephone Voting" Dec 2011[14] from the Electoral Council of Australia.

c) The iVote® system will allow the voter to save a partially completed vote and exit the system. By re-entering credentials, voting can be continued on their Virtual Ballot Paper, from the point of exit and preferences changed or completed, prior to the vote being submitted.

d) The iVote® system will allow the submission of an informal[15] vote but will warn the voter prior to being submitted that the vote will not be counted.

e) The web based iVote® system may present instructions in other common languages in addition to English. Such other languages should be selected by the elector at the commencement of voting.

f) The web based iVote® system may present links to candidate and group information to better inform the voter of their background and electoral platform.

g) The web based iVote® system will, where practical, render ballot papers on the voter's device in a manner which replicates the printed paper. However where the voter's device does not allow this type of rendering the iVote® system will follow the logic flow of the telephone voting system,

h) The web based iVote® system will follow appropriate standards in relation to access by disabled voters to ensure independent voting is available to as many electors as possible.

[14] http://www.eca.gov.au/research/files/telephone-voting-standard-reviewed.pdf

[15] The only type of informal vote allowed will be a Blank vote

5 Voting Protocol

5.1 Registration

5.1.1 Registration for Remote Voting

The registration process requires the elector (or a call centre operator) to identify an elector's enrolment details in the registration system and then enter against the enrolment record, their iVote® registration entitlement and contact details. The elector also enters into the system a six digit numeric PIN. This PIN is not permanently retained in the system[16], however it is retained by the voter. The PIN is only used by the system to create the voting credential which is created using a hash of the PIN and an eight digit numeric iVote number and a Salt. The PIN is the critical credential the elector retains. The PIN should only be known to the registered elector.

However, some 25% of voters will need assistance registering (based on SGE 2011 experience); hence when they register through the registration call centre their PIN will be known to the operator. This is not a security issue as the registration call centre operator does not have access to the iVote® number so they do not have enough information to cast the elector's vote. Also call centre operators phone calls will be recorded and their keystrokes logged to enable detection of a call centre operator using a voter's details to cast a vote.

If a voter cannot vote successfully using their current credentials due to, for example, a forgotten PIN, the registration call centre operator is able to re-issue an iVote® number (which is not disclosed to the operator through this re-issuing) for that elector. This process is called re-registration and the system will in these circumstances remove the elector's current iVote® number (whether it has been used or not) and issue a new iVote® number (using the same process as previously) which will allow the elector to vote again. If the elector had voted the first vote, it will be set aside and not counted.

5.1.2 Secondary identification

After an elector is found on the Roll and has determined their eligibility to use the iVote® system, they will have the option of providing secondary identification in the form of an Australian Driver licence number or Australian Passport number. Any numbers supplied will be checked automatically via a service provided by NSW Roads and Maritime Services.

NSWEC is introducing secondary identification for SGE2015 to provide an additional measure to prevent elector impersonation. It is optional for the elector to supply additional ID details, but if they do not supply a valid licence or passport number, a letter will be sent to the enrolled address instead as a means to prevent impersonation.

[16] The PIN will be only stored in volatile memory of the registration and credential management systems and will not be captured in logs or other permanent storage. Should a system failure occur and the PIN is lost before the Credential Hash can be created the elector will have to re-register.

5.1.3 Registration for Remote Venue Voting

When the iVote® system is used by attending a Remote Venue electors register using a self-service roll look up on a computer in the voting venue.

Once electors find themselves on the roll they then select and enter into the system a six digit numeric PIN and finalize their registration. Voters do not need to record their contact details as they remain at the same computer for voting.

If the electors have any problems finding their personal enrolment record, an election official will provide assistance.

5.2 Credential Creation and Distribution

5.2.1 Credential Creation and Distribution in Remote Voting

This process starts after Close of Nominations when all Virtual Ballot Papers are set up with the correct Candidate and Group information in the Core Voting System, and the Core Voting system has been locked down and released for use by the public.

For each registration an iVote number is created. The iVote Number is combined with the hashed PIN and a secret Salt to create a credential hash[17]. The Credential Hash will be used as both the unique identifier (primary key) and as a device to validate the voter's credentials (being the PIN and iVote® number) when voting.

The iVote® number will be sent to the registered elector as soon as it is created. The iVote number is distributed to the registered elector using one or more of the available channels as requested at the time of registration. The channels available are SMS (preferred), mail[18], email and phone (phone is only allowed for Australian phone numbers).

Except for those who provide secondary identification (see 5.1.2 above), all electors will be sent a letter to their enrolled address which advises they have registered for the iVote® system. The letter requests electors contact the NSWEC in the event they did not enrol. This letter will be the primary control to identify any instances of impersonation.

5.2.2 Credential Creation and Distribution for Remote Venue Voting

The iVote® Number will be issued to the elector immediately upon successful registration. The elector will choose and enter their PIN as part of the registration data entry. The background process of creating the Credential Hash is as above.

Distribution of the iVote® Number to the elector occurs on the spot as a re-direct from the Registration system to the Core Voting Web interface. The Login page will already be populated with the iVote® number on screen so the elector only needs to provide the PIN to start casting their vote.

[17] The iVote number and the hashed PIN are hashed with a "Salt" which is a number that increases the difficulty of determining the entropy of the iVote number and PIN, thus reducing the risk of a brute force attack being used to break the hash. The Salt will be kept a secret but will need to be stored on the Verification website and the Core Voting system to allow entered iVote numbers and PINs to be compared to the Credential Hash.

[18] Using secure external mail house

5.3 Electronic Ballot Box Key Management

The encoding of cast votes will be done using public/private key cryptography. The keys used to create the public key are held by trusted key holders. The keys may be held in the form of tokens like smart cards or passwords created by the key holders. At least five key holders are needed to seal the ballot box. A quorum of at least three of these key holders is needed to open the ballot box.

This process is the same for all modes of iVote®.

5.4 Sealing the Ballot Box

Different iVote® modes use the following virtual ballot boxes. Remote and Remote Venue modes share the same ballot box; if offered in the future, Attendance Voting would use one ballot box for Pre-Poll voting and one for absent iVoting on Election Day.

All electronic ballot boxes are sealed prior to the commencement of voting by all key holders entering their keys into the system. The ballot boxes must be checked to ensure they are holding no votes at the time they are sealed. The keys are used to create a public key which is used by the system to encode all the ballots created during the voting period.

5.5 Vote Management

For a State General Election the Virtual Ballot Paper for each registration consists of:

- The Legislative Assembly ballot paper for the electoral district the voter is enrolled at
- The Legislative Council ballot paper.

Once the ballot box is sealed and the elector's Credential Hash has been created, the unused Virtual Ballot Paper is inserted into the Core Voting System for each registration using the Credential Hash as the unique identifier. At this point the registered elector is able to vote.

Voting closes at 6 p.m. on Election Day:

- When voting remotely, electors logged in at that time can still finish casting their vote but no new logins are allowed.
- When Voting at remote venues the local election officials would ensure that nobody joins the queue after 6 p.m., but electors in the venue would still be able to cast their votes using the iVote system, even if they log into the system after 6 p.m. However none of the Interstate remote venues is expected to be open on election day for SGE2015 and so remote venue voting would close at the end of the business day in each location on Friday 27 March.

A Virtual Ballot Paper (whether empty or completed) will not be included in the count, in the following circumstances:

- the registered elector has voted using another channel;
- the elector is unable to successfully vote using the current credentials; or
- the elector wishes to vote again

5.6 Casting the vote

5.6.1 Casting the vote - Remote Voting

Registered electors log on to the iVote® system by entering their iVote® number and PIN into either a web browser[19] or phone[20] for validation against a Credential Hash held by the system. Once their credentials are validated, access is provided to lists of candidates and groups for the relevant election contest against which voters can enter their preferences on their Virtual Ballot Paper.

Once the elector has submitted their vote, the system creates a random and unique twelve digit receipt number which is provided back to the voter on the voting device. The vote is then encoded using the receipt number and sent to the Verification website.

The original vote[21] and receipt number are then encoded in an electronic envelope using the ballot box public key. This encoded vote is stored in the Core Voting System until the close of polls.

The purpose of the receipt number is to allow the elector to confirm that their vote was cast and captured by the iVote® system as intended (i.e. was not tampered with in transmission). It is also used to confirm that their vote has been processed through the system and forms part of the count (see 5.9.1).

The iVote® system limits preference marking as follows:

- Preference marking is allowed only in accordance with the voting directions;
- Informal voting is only possible by submitting a blank ballot;
- Once a vote has been submitted it cannot be re-submitted, however a voter can re-register and vote again with new login credentials (their previous vote will be discarded); and
- Voters can exit the system with a vote partially completed, and re-enter the system to complete and submit.

5.6.2 Casting the vote at Remote Venues

Once the elector has been redirected to the Core Voting Web interface, the Login page will already be populated with the iVote® number on screen so the elector only needs to provide the PIN to authenticate and then start casting their vote. The voting computer is securely connected to the iVote® system using a self-signed certificate installed on the voting computer which only allows designated remote venue voting computers to access the system for validation against the Credential Hash held by the system. iVote® web servers will have digital certificates installed that are signed by a trusted Certificate Authority.

[19] Using a secure SSL connection.

[20] Using the public switch telephone network and DTMF tones or calling a specialised voting call centre if the voter is disabled to the point they cannot attendance vote.

[21] Preference markings against candidate/s or group/s names

Upon submission of the vote a receipt number is provided to the voter on screen, with the option to print it and take it away for later verification.

5.7 Preference Verification

5.7.1 Preference Verification in Remote Voting and Remote Venue Voting

The vote, as captured and encoded by the receipt number, will be sent to an independently managed verification system, which can be accessed via a phone voice response system using DTMF tones. At any time up to the close of re-registration, voters can hear their preferences as captured by entering their voting credentials and their receipt number into the Verification Service. If voters believe their preferences as shown are not as they voted, they can re-register and re-vote using new credentials.

The Credential Hash and Salt held on the verification site is destroyed prior to the ballot box being opened, but after the electors who have re-registered have had their old votes removed, after re-registration has closed and prior to votes from electors who have voted via another channel being removed. The manager of the verification website will be legally bound to destroy the Credential Hash and Salt and ensure they are kept secure prior to their destruction.

The main reason for deleting the Credential Hash and Salt from the verification system is to further ensure that a receipt encoded vote cannot be associated with an elector, thus reducing the risk that the elector’s voting preferences could be determined.

5.8 Opening the Ballot Box and Vote Audit

5.8.1 Opening the Virtual Ballot Box and Vote Audit in Remote Voting and Remote Venue Voting

Prior to the ballot box being opened, those votes of electors who already have an accepted vote via another voting channel must be removed[22] from the iVote® system using the Credential Hash as the key. This is done by processing the list of successful votes cast using the iVote® system against accepted votes in EMA[23].

The encoded votes are then passed to the Vote Mixer which removes the connection to the Credential Hash. This process is equivalent to an elector placing a vote into a ballot box, which is where the elector is separated from the vote.

Decoding is equivalent to opening of the ballot box[24] in a normal election. It is done by a quorum of 3 key holders who participated in sealing the ballot box. The opening of the ballot box is achieved by each quorum key holder entering their key into the system.

The ballot box is then opened by decoding the votes using the election private key. This reveals the votes in the clear and their associated receipt number.

[22] This is the same as preliminary scrutiny preformed on other forms of declaration votes held in envelopes

[23] The NSWEC Election Management Application.

[24] The opening of the ballot box is achieve by decoding the votes held by the system

The vote audit process will be performed by NSWEC and other independent people, and witnessed by scrutineers and independent observers, as follows. After the ballot boxes have been opened, all the votes residing in the Remote ballot box (which contains votes cast remotely and votes cast at remote venues) are re-encoded with their associated receipt number to allow their comparison to the votes held in the Verification Service.

The re-encoded votes are then compared to the votes held on the Verification System to verify they are the same. If there is a complete match of valid encoded votes it is a reasonable demonstration that votes were not tampered with between being cast and prior to decoding. Given that the encoding process used at this point in the process is the same as used to create a vote on the Verification System, the votes available for counting must be the same votes as verified.

Once the vote audit process confirms the verified votes match with the votes passed through the core system, the preference markings for the decoded votes can be published and passed to the counting system for processing. Note that the independent people who have performed the audit process can also perform an independent count of the votes to check against the NSWEC count.

Receipt numbers are then sent to the receipt website for publication as a verification that the given elector’s vote has passed through the voting system. Note the votes removed from the count prior to the decoding will not be present on the Receipt website. Electors who cannot find their receipt number on the web site can contact the call centre to inquire the reasons why their vote was not admitted to the count.

5.9 Verification of Votes Cast

5.9.1 Verification of Votes Cast in Remote Voting and Remote Venue Voting

Voters can verify their votes using the Verification Service. It is expected that some voters will not be able to find their vote using credentials provided or will believe their vote is not as submitted. In either case, the voter will be given a new vote after re-registration for iVote. The instances of verification failure will be recorded and the reason for failure will be recorded. The Commissioner and iVote Manager will be continually updated with this information and should a systemic problem be identified, the Commissioner will take appropriate action, which could include cessation of voting using the iVote® system.

At the time of close of poll, the vote audit process takes the votes from the decoding process, which are encoded with the receipt number and compares them with the encoded votes held on the Verification Service. The matching of all the encoded votes will confirm that votes have not been tampered with during the election period.

When all votes are verified, the Auditor advises that their receipt numbers can be published and the count can commence. The publication of receipt numbers allows voters to individually verify that their vote has passed through the system and is part of the count. The voter can also read the auditor’s report that all votes have passed audit and as such have not been tampered with since being captured by the iVote system. As a result, those voters who verified their votes individually will be confident that their vote was captured as intended and entered the count as cast.

All preferences for all votes cast using the iVote® system, will be published and be available for anyone to download and count. Therefore electors can check that the final results of the election count are the same as the count they have done using the published results.

Reports will be available in the Core Voting System that will allow comparison with equivalent reports in the Counting Systems to enable checking of vote integrity in the transfer from the iVote® system to the Counting Systems.

Finally, the results of all election contests are reported by voting channels. This approach allows a comparison between iVote results and votes taken through other voting channels. The public can then confirm that the differences are within expected tolerances hence supporting a view that vote tampering has not occurred in the iVote® channel.

6 Application and Data Structure

This section and associated appendix outline the overall application architecture and data structure for the proposed iVote® system. The system comprises the following sub-systems: Core Voting; Registration; Verification; and Credential Management.

A detailed description of the Data Storage Management and Application Architecture for these systems is contained Appendix B.

The underlying design objective for the iVote® system is to ensure voter secrecy. Two or more systems would need to be breached for this to be compromised. The data needed to identify how a given elector voted spans at least two systems and is encoded in both systems. As such, a breach of vote secrecy could only occur if two insider and/or system breaches occurred and the vote encoding was broken.

Similarly, there is a very low risk of vote tampering occurring without detection. Vote tampering without detection would require either a third party or insider to access the core voting system without leaving any trace of their actions. Access to the core voting system is restricted during voting and all actions in the system are held in immutable logs.

Additionally, a verification process is undertaken post-election which compares verified votes stored on a separate audit server with the final vote after decoding. Any deviation between the votes held in the audit system and the core voting system after decoding would indicate tampering had occurred. This checking process can only be subverted if both systems are compromised in a harmonised way and the tampering was not evident in the logs.

7 Expansion of iVote for the SGE 2015

The iVote® system was used at the SGE in 2011 with four elector eligibility types. As a result of experiences at that election and subsequent analysis and reviews, the NSWEC believes the iVote® system is well positioned to address a range of problem voting areas which are satisfied by the current four iVote® eligibility types. The problem voting types are either high cost and/or have high electoral failure.

7.1 Interstate and Overseas Voting

The iVote® system as implemented at the SGE in 2011 was not capable of supporting attendance voting at designated venues outside NSW, because at that time there was a 24 hour delay between registering to use the iVote® system and distribution of the credentials required for an elector to vote. This problem will be overcome with the SGE 2015 iVote system, which will create an iVote® number within seconds of registration and place the ballot into the core voting system ready for the elector to vote.

The NSWEC will use of a version of the iVote® system at the traditional interstate voting venues in place of paper based attendance voting. This proposal can be implemented under the current legislation at interstate voting venues.

Electors who are overseas at the time of the election will be eligible to use the iVote® system and can cast their vote through a web browser or on the phone.

Voting Location	Attendance Votes
Interstate	3,813
Overseas	3,088
Grand Total	**6,901**

7.2 Operator or Voice based Phone Voting

The iVote® system will also take phone votes through call centre operators. This approach will allow disabled and elderly electors to use their phone to vote. Many of these electors do not have access to the internet and could find the use of iVote over the phone using DTMF too daunting.

> *4.33 The NSWEC stated that it would be using the call-centre based approach in all by-elections between now and the next State election. It would also be investigating the use of voice actuated phone voting for the next State election and surveying users on all three options (DTMF, voice actuated and call centre based voting) before reporting those findings to the Government.*

8 JSCEM Recommended Legislative Changes

The following are legislative changes to the iVote® system recommended by the Joint Standing Committee on Electoral Matters (JSCEM) from its review of the SGE in 2011[25], and are supported by the government in their response[26].

The following recommendation is supported by the NSWEC. This recommendation will be addressed as a separate submission to government.

> *RECOMMENDATION 5*
>
> *The Committee recommends that the NSWEC facilitates a dialogue between disability advocacy groups and parties and candidates, on the importance of providing voter information in accessible formats.*

The following recommendation would be addressed by amendments to section 120AF of the current Parliamentary Electorates and Elections Act.

> *RECOMMENDATION 9*
>
> *The Committee recommends that the NSW Government considers introducing legislation to amend the Parliamentary Electorates and Elections Act 1912 to enable technology assisted voting results to be counted separately to postal votes at State elections and by-elections.*

The following recommendation would be addressed by amendments to section 120AB (4) of the Parliamentary Electorates and Elections Act.

> *RECOMMENDATION 10*
>
> *The Committee recommends that the NSW Government considers introducing legislation to amend the Parliamentary Electorates and Elections Act 1912, to enable electors at a by-election, to use technology assisted voting if they are to be more than 20 km outside their electorate on polling day.*

It should be noted the government has taken this recommendation further and said in their response:

> *For by-elections, anyone who will be outside their district on polling day should be eligible to register to use technology-assisted voting. The Government will therefore consider introducing legislation to enable electors at a by-election to use technology-assisted voting if they are to be outside their district on polling day.*

[25] Parliament of NSW, Joint Standing Committee on Electoral Matters, Report 2/55 – 20 December 2012 – Ibid

[26] Parliament of NSW, Joint Standing Committee on Electoral Matters, Report 2/55 – 20 December 2012 - NSW GOVERNMENT RESPONSE
http://www.parliament.nsw.gov.au/prod/parlment/committee.nsf/0/129dfc87035dd10eca257ad10013144d/$FILE/Government%20Response%20-%20Administration%20of%20the%202011%20NSW%20Election%20and%20Related%20Matters.pdf

The following recommendation does not need legislative change and will be implemented by the NSWEC. A description of this implementation is contained in earlier sections of this paper.

> *RECOMMENDATION 11*
>
> *That the NSWEC develop and implement voter preference verification for voters using iVote at the 2015 State election. The NSWEC has confirmed that this project is already underway.*

Appendix A – Schedule

The table below presents a preliminary plan for the key activities required to implement a redeveloped iVote system as proposed in this document for the SGE 2015. This plan will be further developed and refined as the project proceeds.

Activity/Task	Start	Finish
Redevelop iVote software application	Jul 2013	Mar 2015
RFT for Core iVote System	Sept 2013	Feb 2014
Core iVote System development	May 2014	Feb 2015
Other system components development	Feb 2014	Feb 2015
Security planning and implementation	Jun 2014	Mar 2015
QA processes and testing	Feb 2014	Mar 2015
Risk analysis and management	Sep 2013	Mar 2015
Operational planning and implementation	Jul 2014	Mar 2015
Operational planning	Feb 2014	Mar 2015
Develop amended procedures	Mar 2014	Mar 2015
Implementation logistics and management	Nov 2014	Mar 2015
Stakeholder consultation and communications	Sep 2013	Mar 2015
Technical advisory group	Sep 2013	Mar 2015
Stakeholder reference group	Dec 2013	Mar 2015
Technical consultative group	Nov 2013	Mar 2015
Public communications	Mar 2013	Mar 2015

Appendix B – iVote Data Management and Architecture

This Appendix outlines the proposed application architecture and data held by different parties and systems involved in the voting process. As outlined in Section 6, the system comprises the following sub-systems described below:

- Registration System
- Credential Management System.
- Core Voting System
- Verification System

The iVote Application Architecture is provided in Figure 1.

Registration System

The registration system performs the following functions:

a) provides a facility to capture an elector registration either as self-services over the internet or through a call centre;

b) passes the PIN and registered voter details to the Credential Management system to create a ballot; and

c) provides a facility for voters who need to have their vote re-registered.

The following data is held in the Registration System:

- Unique Voter Electoral identifier (SPID);
- all NSW elector enrolment details;
- voter contact details; and
- status indicating that the elector is either registering for first time or re-registering.

The voter PIN is captured but not held in the registration system. The PIN is only held in volatile memory and is not written to any permanent storage. All the above data is passed to the Credential Management System together with the hashed PIN.

Credential Management System

The Credential Management System is connected to the Registration System and to the Ballot Controller using a secure web service. It receives information from the Registration System and prompted by that transaction creates a unique iVote Number and sends that to the Ballot Controller, together with the hashed PIN. The Ballot Controller then creates a new vote (a unique Credential Hash). If the transaction is a re-registration, the Credential Management System sends a message to the Core Voting System to delete the old vote. Re-registrations will use the Unique Voter Electoral identifier (SPID) to find the Credential Hash used by a voter to then delete his/her old vote.

The Ballot Controller confirms the iVote® number with the Credential Management System once a new ballot has successfully been created in the Core Voting System. The Core Voting System then discards the PIN and iVote® number and retains only the Credential Hash and the new unused virtual ballot paper.

The Credential Management System distributes iVote® numbers via mail using a mailing house, SMS to voice and SMS, and provides details for electors who have opted to receive their iVote® numbers by phone. It also manages the distribution of acknowledgement letters to elector's enrolled addresses, where the elector has not enrolled with two factor identifier or is not having their credentials mailed to their enrolled address.

The Credential Management System also provides iVote® numbers to electors over a private internet connection when a valid URL with SPID is provided. This feature is used for supervised attendance voting at remote venues (outside of NSW) where the elector both registers and votes on the same computer.

The following data is received from the Registration System:

- Unique Voter Electoral identifiers (SPID);
- Enrolment details;
- Voter Contact Details; and
- Status indicating that the elector is either registering for first time or re-registering
- Hashed PIN

The following data is received from the Ballot Controller:

- Credential Hash for a given iVote® Number and hashed PIN

The following data is held in the Credential Management System:

- Data for iVote registrations as received from both above interfaces
- Correspondence management information (if, when and through which channels the registration was communicated to the elector)

EMA

EMA provides a facility for electors who use the iVote® system, who already have an accepted vote (recorded in EMA through another voting channel) to be identified and their iVote deleted before it is decoded. Also records the SPID of electors who use the iVote® system who have successfully completed an iVote® which therefore is to be counted.

Counting System

Provides a facility to count both Legislative Assembly and Legislative Council votes, by direct entry from the Vote Decoder.

Core Voting System

Voice Server

The Voice Server provides a voting interface for phone voters using DTMF tones. No voting data is permanently held on this server. Voters only need to enter their iVote® number and PIN to vote.

Web Server

The Web Server provides a voting interface for voters using the common web browsers (including mobile devices) over the internet. No voting data is permanently held on this server. Voters only need to enter their iVote® number and PIN to vote.

Ballot Controller System

The Ballot Controller performs the following functions:

a) Creates credential hash of iVote® number, PIN and Salt;

b) Creates a Virtual Ballot Paper unique to each registration and sends it to the Vote Encoder;

c) Deletes votes from Vote Encoder which should not form part of the count; and

d) Creates and passes Credential Hashes for new and re-registered votes to the Credential Management System.

The following data is sent from the Credential Management System:

- A unique iVote® number.
- Hashed PIN

The Ballot Controller creates a Credential Hash for each new registration or re-registration. The following data is stored in the Ballot Controller for each Virtual Ballot Paper:

- Credential Hash; and
- Flag showing status of vote.

The Ballot Controller also securely stores the Salt[27]. The Credential Hash generated by the Ballot Controller system when a PIN and a unique iVote® number is received from the Credential Management System. The iVote® number is used with the PIN and Salt to generate the Credential Hash. The iVote® number and PIN are only used to create the Credential Hash and then discarded.

The Credential Hash is held in the Ballot Controller system and passed to the Vote Encoder system as the primary key for the Virtual Ballot Paper.

[27] A secret number combined with the PIN and iVote number to make breaking the Credential Hash difficult using brute force approaches.

Vote Encoder

The Vote Encoder performs the following functions:

a) Holds Virtual Ballot Papers ready for voting;

b) Identifies if voting credentials entered match an available blank ballot;

c) Captures preferences into Virtual Ballot Papers to create Completed Virtual Ballot Papers;

d) Encrypts Completed Virtual Ballot Papers with Receipt Number and sends them to the Verification Service;

e) Encrypts Completed Virtual Ballot Papers and the Receipt Number with the public election keys and stores the encrypted votes;

f) Flags deleted ballots which are not to be decoded or counted; and

g) Passes the election key encrypted votes to the Vote Mixer on close of polls.

The Vote Encoder securely holds a copy of the Salt prior to the commencement of voting to allow credential checking. The following data is received from the Ballot Controller to create a new vote:

- Credential Hash; and
- Unused virtual ballot paper.

The following data is received from the Ballot Controller system to delete an existing vote when a re-registration occurs:

- Credential Hash (for vote to be deleted).

Upon successful vote submission, a Receipt Number is generated and sent to the elector. The Receipt number is also used to encode the voter preferences; this is sent to the Verification Service. The Receipt Number and the voter preferences are encoded with the election keys and then held in the system until the ballot box is opened. The following data is stored in the Vote Encoder:

- Credential Hash; and
- completed vote with voter preferences first encoded by Receipt Number then the Receipt Number and encoded vote encoded with election keys.

Also the Vote Encoder will send the Receipt Number back to the voter via the web or voice server used by the voter. The vote encoded using the Receipt Number is then sent to the Verification Service with its associated Credential Hash.

Vote Mixing

The Vote Mixer removes the connection between the voter and the encoded vote.

Vote Decoder

The Vote Decoder performs the following functions:

a) decodes votes using election private key

b) passes decoded votes with Receipt Number to audit process

c) Publishes Receipt Numbers on Receipt Number website.

After close of poll the votes are decoded using the encryption keys held by a quorum. The Completed Virtual Ballot Papers encoded with Receipt Number is then made available in the audit system.

After the audit process verifies the encoded votes available after decoding match encoded votes on the verification website, the following occurs:

- Receipt Number is placed on Receipt checking site, so voters can see that their iVote was admitted to the count
- Voter Preferences in the clear are published. These votes are then ready to be counted.

Voting Management

The voting management module performs the following functions:

a) populates the ballot papers for each contest;

b) manages the voice files used by phone voting system;

c) configures the dates and times of key system events;

d) monitors the progress of the election;

e) removes votes cast using the iVote® system which appear in EMA as accepted prior to decoding; and

f) performs election night count on votes and publishes results to the Counting Systems

g) setup and monitoring of the Core Voting System

Receipt Number Website

The Receipt Number Website publishes the Receipt Numbers of all the votes which will enter the count. The voter enters their Receipt Number. The site then confirms if it matches a number on the site. No other credentials are present on the site.

Verification Service

The Verification Service allows a voter to confirm by phone using DTMF that their preferences were captured by the system correctly. This is done by a voter entering their voter's credentials and then entering the Receipt Number to decode the encoded vote and provided to the Voter with the submitting vote. This facility closes at close of polls to allow the connection between the encoded vote and the Credential Hash to be destroyed, thus reducing the risk of a breach to voter secrecy.

The following data is received from the Vote Encoder after and elector votes:

- Credential Hash; and
- Completed Virtual Ballot Paper encrypted with Receipt Number containing Voter Preferences;

The following data is received from the Credential Manager for a re-registration, or for an elector who has cast a vote via another channel (after check against EMA):

- Credential Hash (for vote to be deleted).

After close of polls, but before decoding votes with election keys, the Credential Hash is removed from the encrypted votes held on the Verification Service.

Vote Audit Process

The audit process allows the votes passed through the system to be compared to the votes as captured at the time of voting and placed on the Verification Service. This comparison is done without revealing the voter preferences or the voter’s identity. The audit process demonstrates that the votes to be counted have not been tampered with when all votes emitted from the ballot box match the votes held on the Verification Website.

The following data is received from the Vote Decoder after voting:

- All completed Virtual Ballot Papers containing voter preferences in the clear plus the receipt numbers.

The following data is received from the Verification Website after close of poll:

- All completed Virtual Ballot Papers containing voter preferences encrypted with Receipt Number.

The audit process uses the receipt numbers to re-encode the Virtual Ballot Papers containing voter preferences in the clear, so that they are encrypted the same way as on the Verification System and can be compared.

Voter

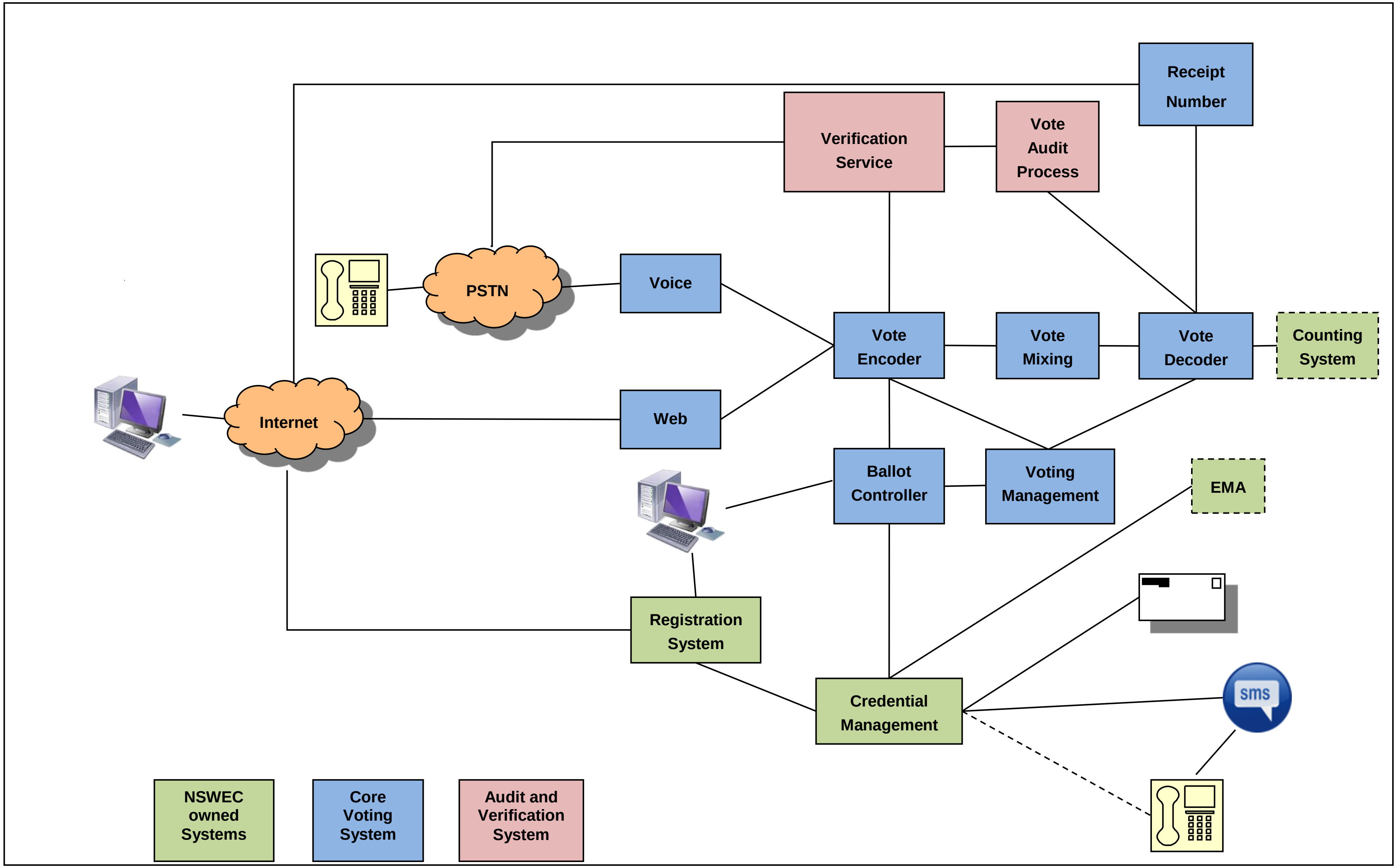
The key data held by the voter which is not held by any other party in the clear is the PIN and the Receipt Number. As long as the voter does not provide this data to anyone else their vote preferences should remain secret.

The following data must be known by the voter prior to voting:

- PIN;
- iVote® Number; and
- vote preferences.

The Receipt Number is provided to the voter after vote submission to be used to as evidence the vote preferences are captured correctly and the vote has traversed the system correctly.

Figure 1 - iVote Application Architecture


Receipt Number
Verification Service
Vote Audit Process
PSTN
Voice
Vote Encoder
Vote Mixing
Vote Decoder
Counting System
Internet
Web
Ballot Controller
Voting Management
EMA
Registration System
Credential Management
sms
NSWEC owned Systems
Core Voting System
Audit and Verification System