NSW Electoral Commission | iVote®

iVote® refresh project for the 2019 NSW State election

Published at
February 2019

Table of figures

1 Summary

State legislation enables the NSW Electoral Commission to implement a remote electronic voting system to provide technology-assisted voting to eligible electors. “Electronic voting” uses electronic or computerised equipment to provide part or all of the vote-casting and vote-collection process. The NSW Electoral Commission has developed the iVote®[1] system, which is a voting system that enables eligible electors to cast their vote using telephones or computers with browsers and internet access.

The iVote voting method is offered, alongside postal and early voting, to improve the enfranchisement of electors who would otherwise not be able to vote independently or have difficulty voting in person at a voting centre on election day.

We recognise that remote electronic voting operates in a complex and challenging technical environment that is developing rapidly. For the 2019 State election, we are undertaking a major project to refresh iVote. This project will not only improve the iVote experience for electors, it also leverages recent advances in electronic voting technology and security. The project aims to improve the general useability of iVote, introduce multi-language support and provide a new and improved method for the elector to verify that their vote is cast as they intended.

The refresh of iVote will also enhance and improve the overall security of iVote including strengthening the encryption, updating the security of all the iVote infrastructure and improving verifiability across key components of iVote. In addition, we will improve the transparency, auditability and scrutiny of iVote.

The iVote refresh project is a major undertaking. We have analysed current and emerging advances in electronic voting as well as engaging with a broad range of experts and academics to ensure iVote remains contemporary. Since the 2015 State election, there have been a number of developments which have influenced the refresh project including the passing of the *Electoral Act 2017*, the report into the conduct of the 2015 State election by the NSW Parliament’s Joint Standing Committee on Electoral Matters (JSCEM), the report on the security of the iVote system by Roger Wilkins AO, the release of the Electoral Council of Australia and New Zealand (ECANZ) principles for internet voting and the electronic voting recommendations developed by the Council of Europe.

[1] iVote®: Registered trade mark of the State of NSW (NSW Electoral Commission).

2 Introduction

This document has been prepared by the NSW Electoral Commission to provide information about the iVote refresh project and what it means for the use of iVote at the NSW State election in March 2019.

2.1 Background

iVote has been offered at:

- the 2011 and 2015 NSW State elections
- 17 NSW State by-elections.

iVote was also trialled at the Western Australian 2017 State election to provide remote voting to approximately 2,000 electors who are blind or have low vision.

We are committed to continually reviewing and improving iVote to ensure it reflects advances in electronic voting. We received funding for the 2017-18 and 2018-19 financial years to implement a 'refreshed' version of the iVote system for the 2019 State election. Details of the procurement strategy, along with other project documentation, are available on the NSW Electoral Commission website[2].

In addition to information about the refresh project, this document also outlines changes made to iVote in response to recommendations made by the JSCEM in its report on the administration of the 2015 State election[3] and by Roger Wilkins AO in his report on the security of the iVote system[4].

2.2 Legislation

On 1 July 2018, the *Electoral Act 2017* replaced the *Parliamentary Electorates and Elections Act 1912* which governed the conduct of the 2015 State election.

Provisions for technology assisted voting are found in the *Electoral Act 2017*.

2.3 Eligible electors

An elector is eligible to use technology assisted voting if:[5]

- The elector has a disability (within the meaning of the Anti-Discrimination Act 1977) and because of that disability he or she has difficulty voting in person at a voting centre or is unable to vote without assistance.
- The elector is illiterate and because of that he or she is unable to vote without assistance.
- The elector's residence is not within 20 kilometres, by the nearest practicable route, of a voting centre.
- The elector is a silent elector (people who have applied for their address to be kept confidential on the electoral roll; this is a new category of eligible elector).
- The elector will not throughout the hours of voting on election day be in New South Wales.

---

[2] Details of the 2019 iVote refresh program
http://www.elections.nsw.gov.au/about_us/plans_and_reports/iVote_reports

[3] Joint Standing Committee on Electoral Matters, Parliament of New South Wales, *Administration of the 2015 NSW election and related matters*, Report 2/56 (November 2016), Recommendations 5, 6, 7, 8 & 9
https://www.parliament.nsw.gov.au/committees/DBAssets/InquiryReport/GovernmentResponse/6091/Govt%20Response%20-%20Inquiry%20into%20the%202015%20NSW%20State%20Election.pdf

[4] Roger Wilkins AO, *Report on the Security of the iVote System* (May 2018), https://www.elections.nsw.gov.au/About-us/Public-interest-information/Commissioned-reports/Report-on-the-iVote-system

[5] *Electoral Act 2017*, section 152.

- The elector is a registered early voter (technology assisted voting)
  (this is a new category of eligible elector[6] commencing after the NSW 2019 State election).

- In relation to a by-election, the elector will not throughout the hours of voting on election day be within the electoral district concerned.

- The elector meets such other eligibility requirements as may be prescribed by the regulations. (Note: no such regulations have as yet been made).

2.4 Strategic context

The provision of iVote at elections directly supports the NSW Premier's priorities of improving government services and the State priority for improved government digital services, which aims to significantly increase the number of government transactions conducted via digital channels by 2019. Further, the NSW digital government strategy sets the vision and imperative for the whole-of-government transformation to a digital, responsive and agile public sector. This transformation is built on three priorities:

1. Improving customer experience of government services[7]

2. Better policies, services and decisions enabled by data insights

3. Streamlined and simplified government processes.

The iVote refresh project is the second-largest digital project within the Premier and Cabinet cluster[8] and aligns with priorities 1 and 3 above.

The NSW Electoral Commission strategic vision is to “maintain confidence in the integrity of the democratic process and make it easy for people to understand and participate”. Technology-assisted voting, using the iVote channel, is a key element in achieving this vision and directly supports two strategic goals:

1. Customer-focused products and services that deliver seamless end-to-end electoral services.

2. Engagement, influence and advocacy to build reach, impact, influence and collaboration with our key stakeholders to improve our engagement and delivery.

iVote also aligns with our customer-centred design principles.

2.5 Approved procedures

The *Electoral Act 2017* provides that the Electoral Commissioner may approve procedures to facilitate voting by eligible electors at an election by means of technology-assisted voting. The Commissioner will approve procedures for the 2019 State election, which will be published on our website[9].

2.6 iVote usage

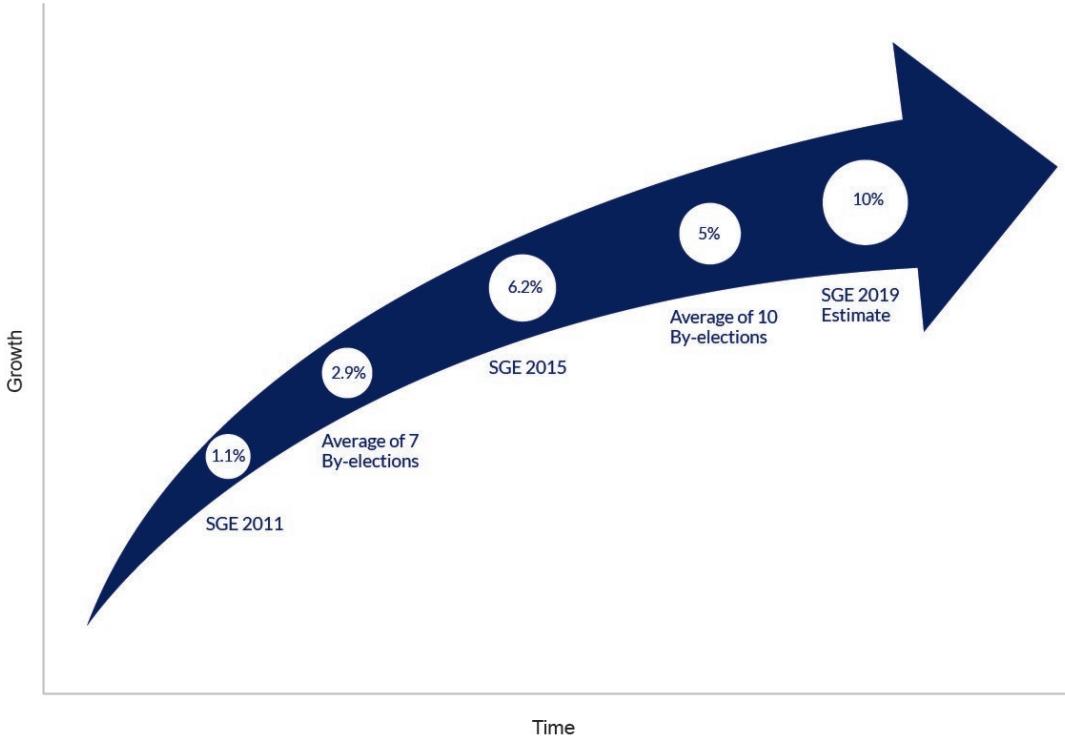
The table below shows the number of electors who have used iVote at each election event since 2011.

[6] Electors will only be able to register as a registered early voters (technology assisted voting) after the 2019 State election
[7] https://www.digital.nsw.gov.au/digital-transformation/digital-strategy
[88] https://www.digital.nsw.gov.au/cluster/premier-and-cabinet
[9] Current iVote Approved Procedures
https://www.elections.nsw.gov.au/voting/iVote/procedures/technology_assisted_voting_approved_procedures_for_nsw_state_elections

Table 1: Votes cast using iVote at NSW State elections and by-elections since 2011

Election event	Date	District	Votes cast using iVote	% of total votes cast
State election	Mar 2011	All 93 districts and Legislative Council	46,864	1.1%
By-election	Nov 2011	Clarence	1,246	2.8%
By-election	Aug 2012	Heffron	798	2.2%
By-election	Oct 2012	Sydney	2,192	5.7%
By-election	May 2013	Northern Tablelands	1,860	4.2%
By-election	Oct 2013	Miranda	679	1.6%
By-election	Oct 2014	Newcastle and Charleston	1,600	1.9%
State election	Mar 2015	All 93 districts and Legislative Council	283,669	6.2%
By-election	Nov 2016	Canterbury, Orange and Wollongong	6,255	4.3%
By-election	Apr 2017	Gosford, Manly and North Shore	6,326	4.7%
By-election	Oct 2017	Blacktown, Cootamundra and Murray	8,095	5.8%
By-election	Sep 2018	Wagga Wagga	2,666	5.5%

Figure 1: Uptake of iVote since 2011



2.7 Research of elector satisfaction

Research conducted following the 2015 State election[10], shows a high degree of satisfaction among electors who used iVote, with approximately 97 per cent of electors surveyed being satisfied with iVote. Electors found iVote easy to use and convenient, and the majority stated they would use iVote again.

Importantly, about 10 per cent of these electors stated they couldn't have voted had iVote not been available. This indicates that iVote has had a positive impact on elector participation. There has also been continued support from electors who are blind or have low vision, who could not vote secretly and independently without iVote.

The research also sought electors' views regarding any improvements that could be made to iVote. Feedback related to aspects of the technical experience, awareness of elector's ability to verify their votes and general security.

2.8 Inquiries regarding iVote

Following each State election, the JSCEM conducts an inquiry into the administration of the election. Following its inquiry into the 2015 State election, the JSCEM made a number of recommendations regarding iVote (see JSCEM iVote recommendations). These recommendations have been considered in the iVote refresh project.

One recommendation was that the NSW Electoral Commission undertake an inquiry to examine the current iVote system. Roger Wilkins AO was commissioned to undertake this inquiry with the following terms of reference:

1. whether the security of the iVote system is appropriate and sufficient
2. whether the transparency and provisions for auditing the iVote system are appropriate
3. whether adequate opportunity for scrutineering of the iVote system is provided to candidates and political parties
4. what improvements to the iVote system would be appropriate before its use at the 2019 State election.

The report made 29 recommendations grouped into the following broad categories:

- national approach
- security
- transparency, auditability and scrutiny
- resourcing and governance.

The report and the NSW Electoral Commission's response to its recommendations have been published on our website.[11]

[10] https://www.elections.nsw.gov.au/NSWEC/media/NSWEC/Reports/Election%20reports/IPSOS-report-for-the-state-election-2015-(PDF-3.4MB).pdf

[11] Roger Wilkins AO, *Report on the Security of the iVote System* (May 2018), https://www.elections.nsw.gov.au/About-us/Public-interest-information/Commissioned-reports/Report-on-the-iVote-system

3 Assessment of internet voting

The NSW Electoral Commission is committed to continually improving and enhancing iVote to ensure it remains a contemporary electronic voting system. This section details the key areas that have been evaluated and have influenced the approach taken in the iVote refresh project.

3.1 Principles standards and guidelines

In the past there have been few agreed principles or standards that can be applied to the field of Internet voting. Principles for an Australian internet voting system were endorsed by ECANZ in 2017. The Council of Europe has developed and released a set of recommendations on standards in the field of electronic voting[12] and the National Institute of Standards and Technology (NIST) and the US Election Assistance Commission (EAC) have published an update to their Voluntary Voting System Guidelines (VVSG). There are also numerous standards, guidelines and principles that cover the broad areas of security, cryptography and secure software development which are listed at 8.8.

3.1.1 ECANZ principles

In July 2017, ECANZ endorsed 11 key principles for an Australian internet voting system. In developing these principles, ECANZ examined the VVSG and the Council of Europe's intergovernmental recommendations for electronic voting. These principles, which have been established to guide the design and implementation of an internet voting service in Australia, are grouped into the three domains of enfranchisement, integrity and privacy, detailed in 8.3 ECANZ principles.

3.1.2 Council of Europe recommendations on standards

The Council of Europe has been the only organisation that has set intergovernmental standards in the field of electronic voting. In 2004 the Council of Europe first released the recommendation on legal, operational and technical standards for electronic voting and in 2017 the Council of Europe released its updated recommendations[13]. These recommendations have been mapped to the ECANZ principles to provide a framework for iVote, not only for the 2019 State election, but also in its future direction. 8.4 ECANZ principles and Council of Europe mapping provides details of these mappings.

3.1.3 Voluntary voting system guidelines

The US Assistance Commission has developed and released the VVSG to provide a set of specifications and requirements against which voting systems can be tested to determine if they provide the basic functionality, accessibility and security capabilities required to ensure the integrity of voting systems. While VVSG is primarily intended for the use of electronic voting machines they provide a useful set of guidelines for the general operation of any form of electronic voting.[14]

3.2 Transparency

- Providing transparency in all phases of an election establishes and maintains public trust and confidence in the electoral process. In paper-based voting, many aspects of the election are observable and well understood. Electronic voting challenges the traditional approach to transparency as many of the observable steps in paper voting channels are automated and processed within computer systems and cannot be observed or scrutinised in the same manner. Transparency is one of the ECANZ-endorsed voting principles and the Council of Europe list five recommended standards grouped as Transparency and Observation:

[12] Council of Europe recommended standards for electronic voting
https://www.coe.int/en/web/electoral-assistance/e-voting
https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f
[13] Council of Europe standards for electronic voting
https://www.coe.int/en/web/electoral-assistance/e-voting
[14] https://collaborate.nist.gov/voting/bin/view/Voting/VVSGPrinciplesAndGuidelines

- Standard 31. Member States shall be transparent in all aspects of e-voting.
- Standard 32. The public, in particular voters, shall be informed, well in advance of the start of voting, in clear and simple language, about:
    - any steps a voter may have to take in order to participate and vote
    - the correct use and functioning of an e-voting system
    - the e-voting timetable, including all stages.
- Standard 33. The components of the e-voting system shall be disclosed for verification and certification purposes.
- Standard 34. Any observer, to the extent permitted by law, shall be enabled to observe and comment on the e-elections, including the compilation of the results.
- Standard 35. Open standards shall be used to enable various technical components or services, possibly derived from a variety of sources, to inter-operate.

3.2.1 Open source software

Open-source software is a type of computer software where source code is released under a license in which the copyright holder grants users the rights to study, change, and distribute the software to anyone and for any purpose.

While there are examples of open source electronic voting projects, none of them are currently suitable for technology-assisted voting at elections in New South Wales.

Often confused with open source software is public access to software source code for review. Public access to electronic voting software source code helps to build public confidence as anyone is able to inspect the source code and assure themselves of its correct operation. We believe this approach has merit as part of election transparency and the key elements of the iVote system source code will be made available for public scrutiny. (See 5.2.2 iVote source code.)

3.3 Scrutiny

An important part of transparent elections is the ability for candidates and political parties to scrutinise key election processes and to observe the overall operation of the election and tallying of results. A similar level of scrutiny of electronic voting can be achieved by allowing scrutineers to observe key events and processes of electronic voting as well as the final decryption and tallying of results.

3.4 Audit and monitoring

The NSW Electoral Commission is required to engage an independent auditor to conduct audits of the use and operation of iVote.[15]

The increasing use of electronic voting has been recognised by the international electoral observation community as one of the paramount challenges facing election observation as there is relatively little experience observing electronic voting. The Carter Center[16] has developed a methodology for observing electronic voting[17] as well as a handbook on observing electronic voting[18]

[15] *Electoral Act 2017*, section 156.
[16] https://www.cartercenter.org/
[17] https://www.cartercenter.org/documents/elec_voting_oct11_07.pdf
[18] https://www.cartercenter.org/resources/pdfs/peace/democracy/des/carter-center-e_voting-handbook.pdf

Alongside external audits, all electronic voting systems must maintain and collate a centralised and immutable[19] regime of logs on every aspect of the voting process. These logs and the monitoring systems need to provide up to date information on the health of the electronic voting systems as well as evidence of tampering making it more difficult for attackers to hide in the event of a system being compromised. These logs may also have to provide evidence in the case of legal challenges or disputes.

3.5 Risks and threats

All electronic voting systems must be resilient and protected against threats that can undermine public confidence in the conduct of the election or, in the worst case, render all votes cast over the channel as invalid. The threats can be broadly categorised as follows:

- Loss or corruption of information. As with all online services, electronic voting systems need to be protected from accidental or malicious loss or modification of data. There are many aspects to threats of this nature and online electronic voting systems need to protect against attempts to "hack" into the systems, software bugs and sophisticated attempts to intercept and change voting data between the elector's device and the election servers. Mitigation of such threats has the added complexity of maintaining the secrecy of the vote while still providing assurance to electors and other stakeholders of the integrity of votes taken and counted using online electronic voting systems.

- The electronic voting systems need to be available throughout the voting period. All the systems and networks need to be planned and designed in such a way that they are resilient and protected against faults in the hardware or networks as well as having sufficient capacity to handle the expected demand. The systems and networks will also have to be protected against attempts to disrupt the service using denial of service attacks.

- As with all channels of voting, online electronic voting systems need to have a mechanism to correctly authenticate and identify the elector. While online voting systems can provide levels of identification that are comparable to, if not stronger than, similar paper voting channels (eg postal voting) there have to be protections against attempts to undertake mass impersonation of electors. This could range from attempts to steal elector's passwords to guessing electors' enrolment details.

- As with postal voting, the act of voting online is not supervised, which means that the elector could be subjected to forms of coercion when casting their vote. Research[20] has shown that in Australia there is limited evidence of interference in voting and that online voting is unlikely to lead to an increase in coercion. Nevertheless, online systems need to provide protection against the possibility of voter coercion.

3.6 Verifiability

While not available for voting using paper ballots, verifiability is an important property for electronic voting and various electronic voting protocols take different approaches to the fundamental goal of assuring integrity. Verification is typically considered in three parts:

1. Cast as intended - the elector's preferences are cast as they intended

2. Recorded as cast - the system has actually saved and stored the elector's preferences correctly

3. Counted as recorded - the saved preferences are all counted correctly.

[19] It is noted that absolute protection is generally unattainable, the need for immutable logs reflects the ideal strength of the log protection

[20] Internet Voting and Voter Interference - A report prepared for the New South Wales Electoral Commission by Associate Professor Rodney Smith, Department of Government and International Relations, University of Sydney https://www.elections.nsw.gov.au/NSWEC/media/NSWEC/Reports/Commissioned%20reports/Internet-voting-and-voter-interference-report-2013-(PDF-437kB).pdf

The first two are performed by the elector, the third should be open to scrutiny by political participants.

Voting protocols and verification options need to strike an appropriate balance amongst three requirements:

1. Proof against vote tampering
2. Secrecy of the vote
3. Usability and accessibility for the elector.

We have analysed the different verification schemes and how they could apply to iVote, see 8.7 for details of this analysis.

Verification provides electors with confidence that their vote has been cast and counted as they intended. It is also used as part of the overall assurance that the iVote channel is operating correctly. Our aim is to provide a verification approach that is useable for electors and available immediately after voting, rather than requiring the elector to undertake verification as a separate step to casting their vote.

3.7 Cryptography

Cryptography is at the core of the iVote system and is essential to ensure votes remain secret and unable to be tampered with. We require that all cryptographic schemes are implemented using published, credible and appropriate cryptographic algorithms based on relevant NIST standards [21] and Federal Information Processing Standards (FIPS)[22]. In particular NIST recommends that all new systems deployed until 2030 need to have cryptographic algorithms and schemes with a security strength equivalent to at least 112 bits (strength is based on key length and the algorithm used)[23].

There is ongoing research into quantum computing that could impact cryptography used in iVote. An adversary with access to a hypothetical quantum computer in the future, could break most of the popular public-key algorithms of today. We will continue to monitor this field with a view to the 2023 State election.

[21] https://csrc.nist.gov/publications/sp800
[22] https://www.nist.gov/itl/current-fips
[23] https://csrc.nist.gov/publications/detail/sp/800-131a/rev-1/final

4 Strategy and objectives

Strategy	Objective	Activity
1.1 Make available in key community languages	Broaden access to users with significant needs	1.1.1 New voting system to include six additional languages based on population need
1.2 Improve navigation to iVote	Make it easier for people to find out about iVote and to access it	1.2.1 Linking iVote system to simplified navigation on our website 1.2.2 Communications campaigns
1.3 Maintain or improve the accessibility of iVote	Ensure that iVote is accessible to all eligible NSW electors	1.3.1 Consultation with our reference groups (Disability, Multicultural and Aboriginal) 1.3.2 Undertake testing with key user groups 1.3.3 Accessibility testing
1.4 Publish easy-read information for users	Build user confidence in iVote, including system security and online safety	1.4.1 Promote the security and assurance features of iVote 1.4.2 Provide links to online safety information https://www.staysmartonline.gov.au/
2.1 Introduce end-to-end verification	Transparency and assurance of the process	2.1.1 iVote to provide three key types of verification (i) "Cast as intended" – votes submitted match electors' intentions (ii) "Recorded as cast" – verify that iVote has received and saved their votes as cast (iii) "Counted as recorded" – The proofs and traceability that link the votes cast to those included into the count
2.2 Increase the rate of voter verification by making it easier	A significant growth in the rate of voters verifying will give a high level of statistical assurance.	2.2.1 The new smartphone app for verification via a QR code displayed at the end of voting should prove easier for most voters
2.3 Improve transparency	To increase the publically available information on iVote and the opportunities for scrutineers to observe the processes.	2.3.1 Publish transparency document outlining all other documents and data to be made available
3.1 Credentials	Improve the strength of the elector's credentials to protect against potential "cracking"	3.1.1 Require electors who select to cast vote using iVote voting website to create a password of sufficient strength to resist "cracking"

Strategy	Objective	Activity
		3.1.2 Require electors who select to cast vote using iVote telephone voting system to create a 10 digit PIN
3.2 Enhance data centre security	Secure data centre hosting is a key element of iVote security	3.2.1 New Voting System hosting will be in IRAP certified datacentre with ASD certified PROTECTED cloud and ASD certified PROTECTED gateway 3.2.2 Updated Registration System hosting will be in NSW GovDC (previously NSW Electoral Commission internally hosted)

5 Innovations for iVote at the 2019 State election

The iVote refresh project includes major enhancements to the voting and verification modules, enhanced system security, improved transparency as well as improvements to the scrutiny, audit and monitoring mechanisms. There are also improvements to the websites used by the electors including the provision of the iVote voting website in a number of languages other than English.

Pre-2019	iVote 2019
Verification	
• Electors had to use the iVote telephone verification system requiring a six-digit PIN, eight-digit iVote number and 12-digit iVote receipt using the telephone keypad • People using iVote from overseas might incur international call costs to verify	• Electors who vote by the iVote website can verify as soon as they cast their vote using the iVote verification app on their smartphone, making the verification much simpler and more immediate • Since the iVote verification app runs on a smartphone it provides greater assurance to the elector that their vote hasn't been corrupted by "malware" on their PC or laptop • Those electors who cast their vote by the iVote telephone voting system will still have to use the iVote telephone verification system but will only have to enter their 10-digit PIN and 8-digit iVote number making the process easier
• All voters get a receipt number as proof that iVote had received their vote. • The receipts were only available for checking after the election	• All voters will receive a receipt • All receipts will be available for checking during the voting period as well as after the election • Provides voters a method to assure themselves that iVote has received and retains their vote

Pre-2019	iVote 2019
• Limited number of voters verified their votes	• Easier and more immediate verification is expected to result in more voters verifying, improving assurance and confidence in the operation of iVote
• Proofs of correct decryption emitted as part of the ballot box opening and vote decryption	• Improved verification of the vote decryption by generating mathematical proof that the decryption has completed correctly and has not corrupted the votes in any way • Introduction of a verifiable mixnet that generates mathematical proof that the mixing of encrypted votes (for vote privacy) has completed correctly and has not corrupted the votes in any way
Improved transparency	
• The key components of the iVote core voting system were reviewed by independent reviewers • Published reports for the 2015 State election (available at http://www.elections.nsw.gov.au/about_us/plans_and_reports/ivote_reports) • Engaged independent auditors to monitor, observe and report on key iVote operations • Independent expert panel appointed to review iVote as per JSCEM[24] recommendation – report publicly released in November 2018	• Expand the range of iVote information and documents to be published pre and post election – this will be detailed in a separate document on transparency for iVote • Use a Technical Advisory Group to review and comment on technical aspects in the design, development and throughout the election. • Expand the role of the independent auditor to cover a broader range of iVote operations. Publish the audit and control plan and the post election report • Publish day to day iVote operational information • iVote voting system source code available for review pre-election by application under Deed of confidentiality • Key components of the iVote voting system source code will be available post-election for inspection and comment • An independent expert panel will be created to monitor, advise and report on iVote use at each major election
Improved scrutiny	
• Scrutineers were invited to observe the iVote ceremony at the close of the election to observe the “unsealing” of the iVote ballot box where the votes are decrypted and checked for entry into the count	• The NSW Electoral Commission will offer training to scrutineers to ensure they better understand the iVote system. The training will also provide information on the data to be published and how this can be used to scrutinise the operations of iVote. • Scrutineers will be able to observe more iVote processes, including the “sealing” of the ballot box where the iVote system undergoes a “lockdown” process and testing is

[24] NSW Parliament’s Joint Standing Committee on Electoral Matters

Pre-2019	iVote 2019
	conducted to confirm that test votes correctly pass through the system • Scrutineers will be able to observe the "unsealing" of iVote at the close of voting, with additional proofs of mixing and decryption of the votes prior to entering the count • Scrutineers (and the public) will be able to access the iVote data that is provided on the NSW Electoral Commission website
Improvements in cryptography	
• iVote used SHA1 to "hash" elector's credentials • 6-digit PIN is used by all electors to log into iVote	• SHA256 now used to create electors credential hash as SHA1 no longer considered appropriate • Electors who select to use the iVote website to vote will have to create a password rather than 6-digit PIN • Passwords will be of a strength that should require at least three months to break with a brute-force attack. • Electors who select the iVote telephone voting system will have to create a 10-digit PIN. Whilst not as strong as the web based password, this is harder to crack than the 6-digit PIN, whilst still useable, and appropriate for telephone voting.
Improved user experience	
• No support for community languages • No easy access to How to Vote Cards • Optional secondary identification accepted Australian passport or driver licence	• The iVote voting website will be available in English and 6 other languages • Electors will be able to access How to Vote information from candidates and parties • Improvements will be made to the iVote application website to aid useability • Medicare card can now also be used as a secondary source of identification
Applying the latest standards and guidelines	
• Council of Europe Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting were covered in the Security Implementation Statement for 2015	• 11 Key Principles for an Australian Internet Voting System developed by ECANZ • Updated to Council of Europe Recommendation CM/Rec(2017)5

Pre-2019	iVote 2019
	• New Voluntary Voting System Guidelines (VVSG 2.0) from National Institute of Standards and Technology (USA) and the US Election Assistance Commission

5.1 ECANZ principles and Council of Europe recommendations

Section 8.4 provides a traceability matrix showing the alignment of the Council of Europe recommendations to the 11 ECANZ Principles and section 8.5 iVote mapping to Council of Europe standards details how iVote address each of the 49 Council of Europe recommendations. This framework provides the NSW Electoral Commission with assurance that iVote is conforming to a set of recognised recommendations.

5.2 Transparency, auditing and scrutiny

The provision of transparency, scrutiny and auditing of the iVote channel are interlinked and are intended to provide mechanisms to assure all stakeholders that the iVote channel is operating correctly. It is important to note that the NSW Electoral Commission does not consider any one of these aspects of iVote in isolation but will be developing and delivering each one in a manner that builds a strong picture of the correct operation of iVote.

5.2.1 Transparency

As noted earlier, electronic voting challenges the traditional approach to electoral transparency. iVote for the 2019 State General Election will have a significant number of transparency improvements over previous versions

During the 2019 State election the NSW Electoral Commission will publish key data to provide insight into the progress and functioning of the iVote channel. One important area of improvement is the verifiability features now available and key verification data will also be published alongside other iVote data. As well as publication of the verification data, we will publish the results of the mixnet processing as well as the preferences loaded into the NSW Electoral Commission's Proportional Representation Computer Count (PRCC) system after the election.

The NSW Electoral Commission will publish information on the design and operation of the iVote channel in the public domain. There may be some elements that can't be published either due to commercial restrictions or because the level of detail in itself may pose a risk to the overall security of the iVote systems. The NSW Electoral Commission will use the services of its Technical Advisory Group to review and comment on technical aspects of the iVote system.

5.2.2 iVote source code

The NSW Electoral Commission will make the iVote voting system source code available for review and it will be published under the following conditions:

- From January 2019 all the iVote voting system software supplied by Scytl will be available for review, by application, under deed of confidentiality.
- As previously, the NSW Electoral Commission will engage selected experts to independently review the iVote system source code. We will also proactively encourage other experts to review the source code under deed of confidentiality.
- After the election the NSW Electoral Commission will release certain components of the Scytl Voting System. The components listed below, will be available for review and comment:
    - voting client (JavaScript)
    - verification application (mobile app)

- voting service
    - validation of the encrypted vote
    - validation of the cryptographic proofs
    - digital signature of the receipt
- verification service
    - validation of the encrypted vote
    - validation of the cryptographic proofs
- counting service
    - vote decryption
    - digital signature

5.2.3 Auditing and monitoring

For the 2015 State election, the scope of the mandatory independent audit of the use of iVote was:

- assess the processes and controls used to secure access to iVote before the commencement of voting
- assess the NSW Electoral Commission processes for testing the logic and accuracy of the iVote system prior to the commencement of iVote voting
- assess the processes and controls used for the voting decryption ceremony once the election has ended
- review relevant reports created by third parties.

For the 2019 State election the scope and role of the auditor will be expanded to enhance the overall transparency mechanisms. There will be an iVote audit plan that will aim to cover all aspects of the operation of iVote including the performance of the key controls. In addition, the NSW Electoral Commission will engage an expert advisory panel to report on key elements of the use of iVote during the election.

5.2.4 Scrutiny

Scrutineers provide an important role in the overall transparency of an election as they are able to observe and report on key electoral processes as representatives of candidates. The role of the scrutineer is equally as important for the iVote channel. The NSW Electoral Commission will provide scrutineers with access to the key iVote events, including the testing and locking down of the electronic voting ballot box prior to start of voting and the decryption of the ballot box at the end of voting. We will also provide training to scrutineers to enhance their observation and understanding of the iVote logic and accuracy testing, the lockdown and the decryption process. Scrutineers will be provided transparency and audit information and will also be able to access the iVote data published during the election.

5.3 Risk management

The NSW Electoral Commission's risk appetite statement outlines the amount of risk we are prepared to accept to achieve our strategic and operational objectives. We face a range of risks and overall, we have a low risk appetite. This means we look to avoid risks and uncertainty and have a preference for options that have a low degree of inherent risk. We do accept there is a certain level of inherent risk in our activities and acknowledge that a certain level of risk helps us develop and innovate to better serve our stakeholders and clients. iVote is an example of our innovation in service delivery.

We conduct extensive risk modelling and analysis on all aspects of iVote and ensure that controls and mitigations are in place. We recognise that, as with all of our voting options, it is not possible to completely mitigate all risks to iVote.

5.4 Verifiability

Section 3.6 details the forms of verification that need to be in place in order for electors to be assured their vote is not only cast but also counted as they intended. The iVote channel has undergone a significant improvement in the forms of verifiability offered to electors and other interested stakeholders as detailed below.

5.4.1 Cast as intended verification

“Cast as intended” confirms the elector’s submitted vote matches their intentions. This can be achieved with a sensible user interface and the ability to confirm preferences before submitting.

The iVote system provides a voting website designed to ensure an elector casts valid Legislative Assembly and Legislative Council votes in accordance with the relevant directions. Electors are allowed to cast a blank ballot paper if they wish, although receive a warning before submitting the vote. After completing both ballot papers, the elector is presented with their preferences for review and optionally changing prior to submitting to the iVote voting system.

On successful submission and storage of the elector’s vote, the iVote system generates and returns to the elector a receipt. The iVote receipt is a signed hash of the encrypted vote and provides the elector with a “digital fingerprint” of their vote. The iVote receipt can be used by electors to verify that their vote is unchanged. Electors will be able to check their receipt on the iVote receipt portal once their vote has been cast. This provides the elector with the ability to check at any time that their vote has been received and is securely held in the iVote system.

5.4.2 Recorded as cast verification

“Recorded as cast” provides the elector with assurance that the NSW Electoral Commission has received and saved their vote as cast. The iVote system provides an improved “Recorded as cast” verification for electors. Electors who cast their vote using the iVote website will be able to verify that their votes have been received and the preferences are recorded as they intended by using the iVote Verification Application, which they will have to download onto their smartphone. Once the elector submits their vote they will be presented with a QR code on their web browser that they can scan using the iVote Verification Application. The elector will then have to enter their iVote number and password into the iVote Verification Application to complete the verification process. The iVote Verification Application requests the encrypted vote from the iVote voting system. The encrypted vote is retrieved and forwarded to the iVote Verification Application on the smartphone. The iVote Verification Application uses the elector’s iVote number and password with the verification data embedded in the QR code to decrypt the vote on the smartphone and display the elector’s vote.

Electors who cast their vote using the iVote telephone voting service can verify their vote by calling the iVote telephone verification service. The elector will have to enter their iVote number and PIN, which is then used by the iVote telephone verification service to decrypt the elector’s vote and repeat the vote details back to them over the telephone.

This approach provides a number of key assurances not only to the individual elector but also the NSW Electoral Commission:

- requiring the elector to verify their vote on a device separate from the one on which they cast their vote will reduce the possibility of the vote being corrupted by malware on the device used to cast the vote
- assure the elector that the vote has been received and stored correctly by iVote
- for those who have voted using the iVote voting website the provision of the QR code immediately after submitting their vote increases the likelihood the elector will verify their vote

- this approach is intended to increase the overall assurance to the NSW Electoral Commission that iVote is operating correctly and increase overall confidence in the integrity of the iVote channel.

5.4.3 Counted as recorded verification

"Counted as recorded" provides the traceability and proof that link the votes saved to the count.

For the 2019 State election, iVote will improve the ability to verify, prove and trace that the votes are correctly anonymised, decrypted and included in the overall count. After the close of voting there are a number of important steps in downloading the votes held in the iVote voting system for inclusion in the count. Each step provides proof and traceability that only valid votes are included into the count and that the votes have been securely stored and remain as cast by the elector. The steps are:

- Prior to the mixing and anonymising of the votes there are a series of cross-checks between the various iVote systems to ensure the votes cast can be reconciled between the number of iVote applications and the votes cast.
- The electronic ballot box is cleansed and validated to ensure only valid votes are passed to the mixing and decryption processes.
- The valid votes are mixed to ensure that there are no links between the votes cast and the elector and the results of the process are passed to the decryption process.
- The votes are decrypted.
- The decrypted votes are then loaded into the NSW Electoral Commission systems for the tallying and counting of the iVote votes alongside votes cast through other channels.

Details of the three steps of cross-checking credentials, reconciling receipts and cleansing the ballot box are provided below.

5.4.3.1 Pre-mixnet verification

The NSW Electoral Commission will undertake a series of checks and reconciliations prior to the mixnet that ensures that only eligible electors have cast votes and that only the valid votes are passed to the mixnet and decryption process. These checks will be undertaken as part of the decryption ceremony at which scrutineers and auditors will be present.

Cross checks between credential management and iVote voting systems

The NSW Electoral Commission will undertake a cross check between the credential management system and the iVote voting system. The credential management system ensures that only eligible electors can apply for iVote as well as handling the electors' credentials, while the iVote voting system holds the votes cast by the eligible electors. The two systems maintain a common identifier called VoterKeysID. Using this common identifier, we undertake the following cross checks:

- reconcile that for each VoterKeysID held in the credential management system there is a corresponding ID in the iVote voting system
- for each VoterkeysID in the credential management system, the Legislative Assembly district linked to that ID is the same as the corresponding ID in the iVote voting system
- for each VoterkeysID in the credential management system, the status of the vote (valid or not valid[25]) is the same as the corresponding ID in the iVote voting system.

[25] A vote in iVote is marked not valid if the elector has applied for more than one iVote, in which case the last vote cast in iVote is considered valid

The checks provide the following evidence:

- only eligible electors have cast a vote using iVote
- there is only one vote in the iVote voting system for each application
- there is no evidence of votes having been inserted into the iVote voting system for which there is no linked elector
- the validity of the votes held in the iVote voting system has not been changed
- the Legislative Assembly districts of the votes held in the iVote voting system have not been changed.

It is important to note that once the cross checks have been completed that all the VoterKeysIDs in the credential management system will be irrecoverably deleted ensuring that the links cannot be reconstructed at any time in the future.

Reconciliation of iVote receipts

The next step is to compare receipts for each vote cast and held by the iVote voting system against the receipts held by the iVote assurance system. When the elector submits their vote they receive a receipt which is a digital "fingerprint" of the encrypted vote stored in the iVote voting system. At the same time, the receipt is copied into the iVote assurance system. The elector checks the existence of their receipt against the copy held by the iVote assurance system.

The receipts in both the iVote voting and assurance systems can be cross checked and compared to ensure that the receipts in both systems are the same.

The checks provides the following evidence:

- votes haven't been added to the iVote voting system without generating a valid receipt
- since electors check their receipts against the iVote assurance system, and the iVote voting and assurance systems match, the iVote voting system has been storing and handling the votes correctly.

Ballot box cleansing

Only valid votes can pass on to the decryption process. Ballot box cleansing ensures the checks below are undertaken on all votes held by the iVote voting system:

- The NSW Electoral Commission's Election Management Application (EMA) provides a list of electors who have cast a vote through iVote as well as another voting channel[26]. This is passed to the cleansing process and the votes in iVote for these electors are all marked as not valid.
- The cleansing process checks that there is only one vote for each elector.
- The cleansing process also validates the integrity of each vote inside the ballot box by checking the following attributes:
    - the authentication token of the vote
    - the chain of the x.509 certificate used to sign the vote is valid
    - the different aspects of the cryptography forming the vote.

[26] postal vote or early vote

The ballot box cleansing provides the following outputs:

- the cleansed ballot box contains only valid encrypted votes. It is important to note that the correlation between the elector and their vote has now been irrecoverably broken
- receipts for each of the valid encrypted votes
- receipts of votes that did not pass the cleansing
- a file of IDs for elector's whose votes have been marked as not valid
- a file containing the reason why the votes were marked as not valid.

The checks provides the following evidence:

- Only valid votes are passed to the decryption process, ensuring there is only one vote per elector.
- All the votes passed to the decryption process have all the correct encryption integrity attributes.
- Comparing the valid and invalid receipts with the receipts held in the iVote assurance system allows us to reconcile the number of votes cast.

5.4.3.2 Mixnet verification

The mixing process breaks any correlation between the votes collected in the iVote ballot box and the votes to be decrypted, by shuffling and re-encrypting them. The mixnet produces proofs of the correct computation of the mixing process to ensure that the mixnet did not manipulate any of the contents of any of the votes.

After the shuffling and re-encryption has been performed, the mixing process outputs two sets of files related to the input cleansed ballot box:

- mixed ballot box that is composed of the list of shuffled and re-encrypted votes corresponding to valid votes
- cryptographic proofs to demonstrate that the shuffled and re-encrypted votes in the mixed ballot box are the same that those in the cleansed ballot box.

5.4.3.3 Decryption verification

The mixed votes are decrypted and outputs the following:

- list of decrypted votes
- cryptographic proofs to demonstrate that the decryption has been performed correctly
- list of decrypted votes with decryption errors.

Transferring votes to the NSW Electoral Commission count systems

Additional controls have been implemented to ensure the decrypted votes are authenticated and traceably transferred into the count systems for production of the election results.

5.5 Cryptography

The iVote voting system has improvements in the cryptography used including a new approach that leverages the ElGamal encryption system:

- the iVote hashing algorithms used to derive the elector's hashed credential now uses SHA256 instead of SHA1

- the use of ElGamal[27] cryptography allows cryptographic proofs that the content of the encrypted vote has been unaltered without requiring decryption of the ballot box
- the addition of a cryptographic mixnet strengthens the anonymity of the vote handling. The mixnet breaks the association between the elector and their encrypted vote by removing the link between the credential hash and the vote, shuffles the vote and provides mathematical proof the integrity of the vote has been maintained.

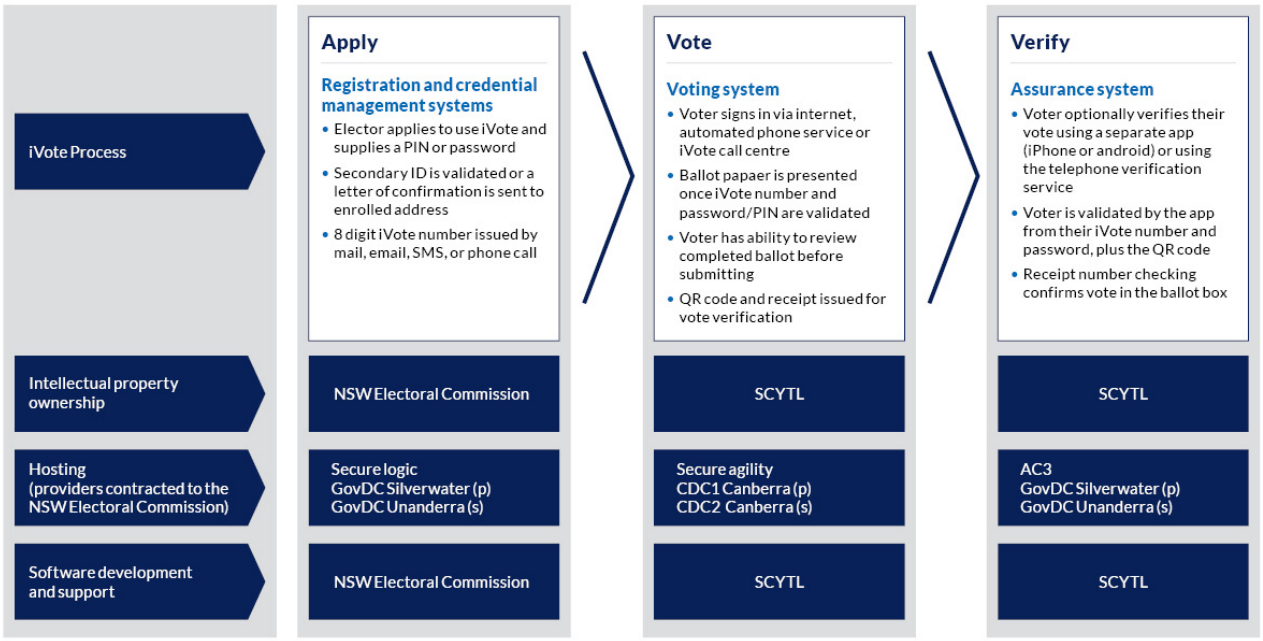
6 iVote systems

iVote is made up of three systems that provide the platform for the iVote channel as follows:

1. registration and credential management
2. voting system
3. assurance system – verification and receipt website.

See illustration below of the iVote ecosystem. The paragraphs below provide details of each of these systems.

Figure 2: iVote ecosystem



(p) - primary site | (s) - secondary site

[27] ElGamal cryptographic system allows for randomized re-encryption of cypher texts, and supports proof of knowledge of parallel shuffle and proofs of knowledge of correct decryption

6.1 Registration system and credential management

We have developed and own two systems that provide electors with the ability to apply to use iVote:

- registration system, which is used by electors to apply to use iVote
- credential management system, which is an internal application used to manage and administer all aspects of an elector's iVote application.

The registration system provides a public website for the elector to apply to use iVote. The elector's enrolment eligibility is checked against the authorised roll of electors prepared for each election in the NSW roll management system and there are also interfaces to our EMA system as well as the federal government's Document Verification Service (DVS). Once the elector completes their iVote application, the registration system submits the details to the credential management system for processing. An important feature of registration website is the "hashing" of the elector's password\PIN inside the elector's web browser before it is submitted to the iVote registration system. This creates a scrambled version of the password\PIN and greatly reduces the chances of password theft as it is the hashed value that is sent to the registration system, which then encrypts the hashed password/PIN before sending to the credential management system.

When the credential management system receives the elector's application from the registration system, it creates a unique iVote number. This iVote number is passed to the voting system together with the elector's encrypted, hashed password\PIN. The voting system then creates a unique internal system identifier[28] based on the elector's hashed password\PIN and iVote number received from the credential management system. At the same time, the iVote voting system creates a blank virtual ballot paper linked to the internal identifier.

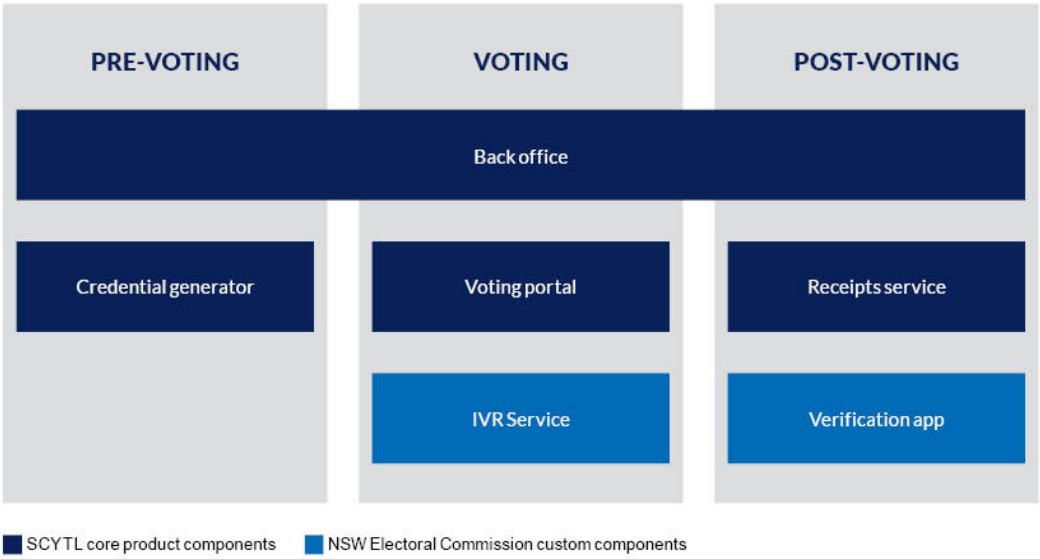
An elector can, in certain circumstances[29], apply for a new iVote. In the case of a re-application the credential management system also instructs the voting system to mark any previous vote that may have been submitted as no longer valid. Once the elector's new virtual ballot paper has been created, the elector's original hashed password/PIN is discarded and unusable. The credential management system also allows us to manage the distribution of iVote numbers to electors over the various channels – SMS, e-mail, post and by telephone call, as well as sending reminders to electors who have applied for iVote but haven't yet voted.

6.2 Voting system

The iVote voting system is supplied by Scytl and hosted on NSW Electoral Commission managed infrastructure in a separate data centre from that hosting the registration and credential management and assurance systems. The Scytl voting system provides the secure voting platform for casting votes over the internet or by telephone. The product provides a number of modules as well as interfaces to integrate with all the other iVote systems as illustrated below.

[28] This is known as a Credential Hash
[29] Electors can apply for a new iVote if they have lost or forgotten their password\PIN, if the vote they cast is not correct following verification or if they state that they were coerced into voting.

Figure 3: Scytl voting system – conceptual architecture



The modules of the iVote voting system are used at different stages of the election:

- Prior to the start of voting, the election is configured, the one-off election private keys are created and distributed amongst the Electoral Board on SmartCards and the election is tested and locked down.
- When electors apply to use iVote, the credential management system interfaces with the voting system[30] to create the elector's virtual ballot paper and hash their iVote credentials.
- The voting system provides the website and all the underlying cryptography for the elector to securely cast their vote over the internet. Alternatively, the voting system provides the interface for electors to cast their vote using a telephone.
- The voting system provides a service for electors to undertake "Cast as intended" verification as well as providing vote receipting services.
- Once voting has closed, the voting system will mix and decrypt the votes cast including the mathematical proofs of the integrity of the decrypted ballot papers to be included into the count.

6.2.1 Election configuration

The voting system's election configuration module allows us to setup election parameters such as the Legislative Council and Legislative Assembly details, key election dates, candidates, audio files etc. Most importantly, an Electoral Board needs to be created for each election. The Electoral Board generates the public and private encryption keys used to seal the electronic ballot box and encrypt the votes. The Electoral Board is made up of senior officials of the Electoral Commission who together create these keys which are then cryptographically split and shared amongst the members of the Electoral Board. Once created, only a quorum[31] of the Electoral Board can successfully re-create the keys to perform the decryption of the votes. We are also able to test that the election is configured correctly and to lock down and "seal" the ballot box prior to the start of voting.

[30] The iVote Voting System Credential Generator
[31] The minimum number of the Electoral Board determined by the Electoral Commissioner who together can re-create the keys for decryption.

6.2.2 Voting website

Electors access the iVote voting website and enter their iVote number and password, which is authenticated by the voting service. The elector must make a declaration that they haven't previously voted at the election and is presented with their Legislative Assembly and Legislative Council ballot papers. The elector completes the ballot papers, which are checked for the relevant formality rules before being submitted[32]. When the elector submits their vote it is encrypted and digitally signed inside their browser and an integrity proof is generated before the vote is securely transmitted to the iVote voting system and included into the electronic ballot box. Once received, the iVote voting system returns to the elector an iVote receipt based on the value of the encrypted vote. Along with the iVote receipt, the elector is presented with a QR code which can be used to verify that their vote has been correctly cast.

6.2.3 Telephone voting

For electors who have applied to cast a vote using a telephone rather than over the internet, we have developed an interactive voice response (IVR) telephone voting service. The iVote telephone voting system enables electors to cast their vote privately using a standard landline or mobile phone. Votes cast via the telephone voting system are encrypted into the same ballot box as votes cast over the internet.

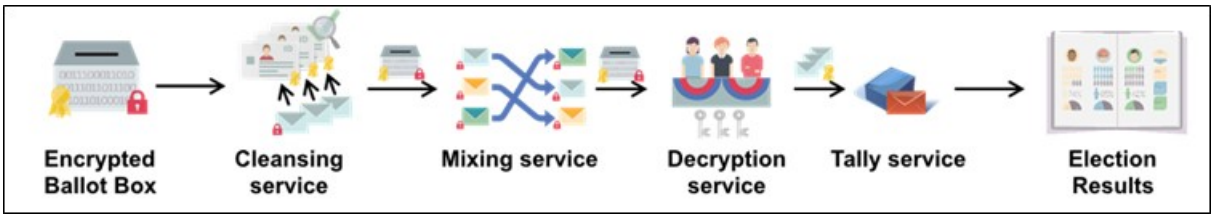
The elector calls the iVote telephone number and is guided through the voting process. The elector's iVote number and PIN are authenticated by the voting service and using the telephone keypad the elector is able to navigate through the voting process and cast their votes for the Legislative Assembly and Legislative Council.

The elector is presented with a final confirmation of both ballots before proceeding to confirm and submitting their ballot papers. The elector's ballot paper is encrypted by the voting service and the iVote receipt generated in the same way as votes cast over the internet.

6.2.4 Close of voting

After the close of voting, the votes held in the iVote voting system are decrypted and made available for importing into the NSW Electoral Commission's Proportional Representation Computer Count (PRCC), along with the votes from all the other voting channels, to count and tally the results. Information is also loaded into our EMA system to provide early overall results figures from the iVote channel[33]. The iVote voting system provides a process that preserves the elector's anonymity and at the same time maintaining overall verifiability.

Figure 4: iVote voting system – opening the ballot box



As illustrated above, the decryption of the ballot box has four distinct steps:

1. The cleansing service verifies the correctness and the integrity of the ballot box and its contents before proceeding to the decryption and counting. There is a process that ensures only valid votes are included into the count as the cleansing process ensures votes that are marked as "invalid" due

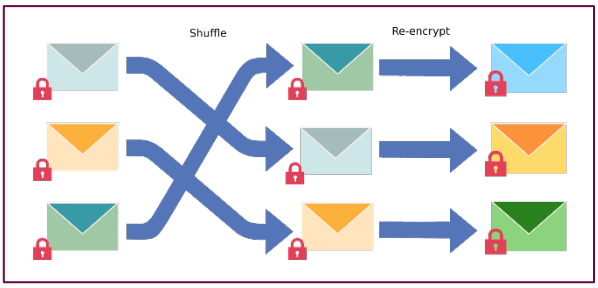
[32] iVote will only accept preferences cast in accordance with formality rules. If the elector chooses not to cast any preferences, however, iVote will permit a blank ballot paper to be submitted, which will be informal

[33] A tally of the 1st preferences and Two Candidate Preferred count for each Legislative Assembly District. A tally of the 1st preferences cast for each Legislative Assembly Group

to the elector having re-applied for iVote or where the elector has cast a vote in iVote and a vote through another voting channel[34] are excluded from the decryption process.

2. The mixing service breaks the correlation between the votes collected in the ballot box and the votes to be decrypted by removing the link between the vote and the electors' credential hash. This is done by shuffling and re-encrypting the votes in a process that also produces mathematical proofs of the correct mixing process[35] and verifiable decryption processes.

Figure 5: Scytl voting system – mixnet



3. Once the valid votes have been mixed they are ready to be decrypted and passed to the NSW Electoral Commission's PRCC[36] for inclusion into the count. To begin the decryption process the quorum of the Electoral Board meets to re-assemble the election private key needed to decrypt the votes. The decryption process also generates a proof that the decrypted content is exactly the same one inside the encrypted vote[37].

4. Once the votes have been decrypted they are available to be included into the count along with votes from all the other voting channels.

6.2.5 Immutable logs

The iVote voting system stores all the important actions performed by the system, including electors' and administration activities, in logs. These logs are protected by means of cryptographic mechanisms[38] that ensure changes to the logs can be detected. The information stored in the logs could be used to trace and resolve any conflicts in case there is an inconsistency with the votes cast and those recorded in the ballot box.

6.3 iVote assurance system

The iVote assurance system provides the electors with two "Cast as intended" verification channels; the iVote verification application for those who voted on the iVote web channel and iVote telephone verification for those who voted on using the telephone voting channel. The iVote assurance system also holds copies of all the iVote receipts from the iVote voting system which is used by the receipt checking website.

[34] If an elector cast a vote in iVote and then casts a Postal Vote or an Early Vote then the iVote is discarded
[35] Bayer, S., Groth, J.: Efficient zero-knowledge argument for correctness of a shuffle. In: Advances in Cryptology - EUROCRYPT 2012. LNCS, vol. 7237, pp. 263–280 (2012)
[36] The PRCC is the NSW Electoral Commission's counting software used to calculate the results of the election. The decrypted votes from iVote are loaded and all the paper votes from all other channels are data entered. Once complete the PRCC calculates the results of the elections
[37] Chaum, D., Pedersen, T.P.: Wallet databases with observers. In: Advances in Cryptology - CRYPTO '92. LNCS, vol. 740, pp. 89–105 (1992)
[38] The system is based on chaining the log entries using a combination of Message Authentication Codes (MACs) and Digital Signatures (DAs). Each logger has a pair of signing keys, thus the log authenticity and non-repudiation can be demonstrated

6.4 System security and resilience

As described, iVote is made up of a number of systems which are grouped into three functions – apply, vote and verify. We have designed the infrastructure, security and data centre hosting based on the following principles:

- **Separation of environments**

  We have physically separated the systems that provide the three steps of iVote – apply, vote and verify. This means that the registration and credential management system are not managed by the same hosting vendor that manages the voting or assurance systems. This separation ensures that no one system holds all the information regarding the elector and how they voted limiting the damage that can be done if a breach does occur. In addition, once the iVote systems are "locked down" access to each system by NSW Electoral Commission administrators use the same levels of separation ensuring that no single user has overall administrative rights across all the systems.

- **Digital continuity**

  All the iVote systems have to be available for the period of the election and resilient to failures in any of the components. To provide this level of service requires careful planning and designing of every layer of the iVote systems as there are many factors that can affect availability. We undertake capacity planning to ensure the network connections, hardware, storage and software can handle the potential peak loads on the iVote systems. All aspects of the data centre infrastructure have to be designed to ensure that there is no single point of failure and, in the case of a component failure backup, components can cope with a failure seamlessly. In the case of a complete data centre disaster each data centre will have a disaster recovery site which can provide a mirror of the primary site to allow continuity of service.

  We use tier 3 or 4 data centres (as defined by the Uptime Institute[39]) which are able to provide 24 hours a day / 7 days a week operations with zero downtime during election periods. All data centres have to provide disaster recovery sites that are geographically separated and all iVote data must remain in Australia. Data centre operations are expected to meet NSW Government ISO 27000 series[40] quality requirements, including security and privacy.

  We will ensure the iVote systems are optimised for performance and recovery in order to achieve both Recovery Point Objective (RPO[41]) and Recovery Time Objective (RTO[42]) approaching near zero.

- **Principle of least authority**

  The principle of least authority is aimed at ensuring that users are given and use only the privileges needed to perform their role and no more and, where users are given privileged access, they should not assume that level of privilege until it is required by the current operation they are performing. It can also be applied to system processes with each system component or process having the least authority necessary to perform its duties. This helps reduce the "attack surface" of the computer by eliminating unnecessary privileges that can result in network exploits and computer compromises

  Access to any component of the iVote systems will be controlled and the principle of least authority will be implemented using agreed procedures. No user access[43] can be created and granted without the appropriate approval of our iVote team.

[39] https://uptimeinstitute.com/tiers
[40] The ISO 27000 series consists of ISO 27001 through to ISO 27018
[41] RPO is focused on data and loss tolerance in relation to data. RPO is determined by looking at the time between data backups and the amount of data that could be lost in between backups
[42] RTO is the target time for the recovery of iVote after a disaster has struck.
[43] These are users who are required to administer the iVote systems and not electors or general NSW Electoral Commission users.

- **Integrated monitoring**

  As with the iVote systems, logs will be maintained across all the infrastructure components to monitor not only the health of the overall iVote systems and components but also security incidents. We use Splunk[44] to aggregate and report on these disparate logs to provide a centralised view of the health of the environment and provide alerting of issues and problems.

- **Security by design**

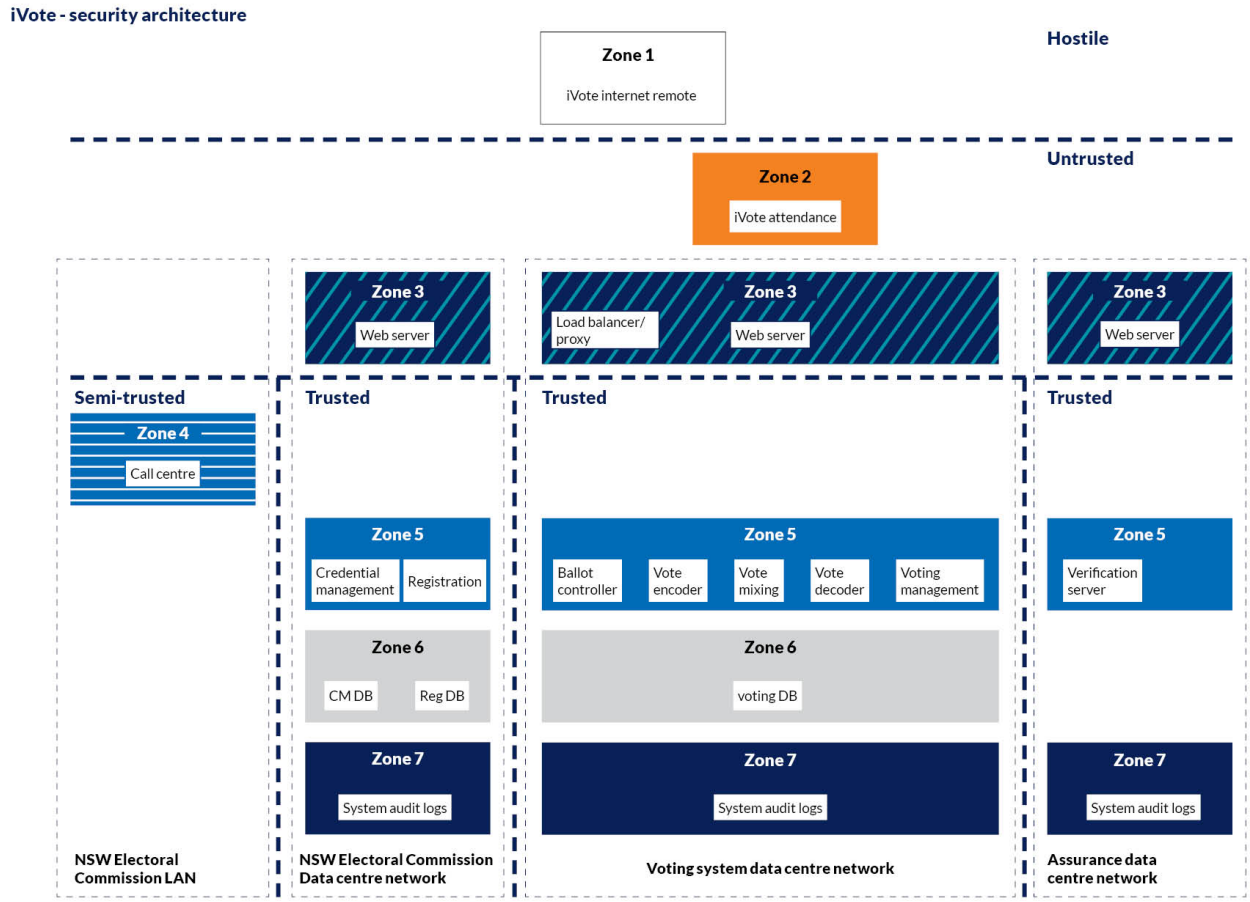
  It is critical that all the iVote systems are protected and secured against both internal and external attacks. In order to deliver the level of security required, there are five mandatory security principles that we require of all data centres:

  1. minimal trust design
  2. role-based network segregation and segmentation (eg public facing web systems must be separated form storage and processing systems)
  3. minimal functionality — all systems are configured such that any unused operating system services are disabled and only the minimum required set are enabled
  4. all infrastructure will be hardened[45]
  5. firewalls used to segregate key components within each system are configured to only allow required network traffic between these components.

An accepted approach to designing a security architecture that meets these principles is to create security segments as illustrated below and all data centres will be required to implement this approach.

[44] https://www.splunk.com/
[45] Hardening is the process of securing a system by reducing its surface of vulnerability. Examples of hardening typically includes changing default passwords, the removal of unnecessary software, unnecessary usernames or logins, and the disabling or removal of unnecessary services.

Figure 6: iVote – security architecture



In addition to provisioning a secure environment for the iVote systems, the data centre is expected to provide protection against distributed denial of service (DDoS) attacks, ensure all the iVote infrastructure is physically secured from unauthorised access or tampering and that all data between client devices and the service is encrypted to a minimum of AES 256 bit or better.

The data centres hosting the iVote voting system are ASD IRAP certified[46]. In addition the following ASD guidelines will be used with regard to security:

- Network segmentation guidance[47]
- Cloud security guidance[48]
- Strategies to mitigate cyber security incidents (ASD Essential 8).[49]

The NSW Electoral Commission has engaged the services of providers who specialise in security operations to provide 24 hours a day / 7 days a week proactive monitoring of all the iVote systems and infrastructure.

[46] https://www.asd.gov.au/infosec/irap/irap_assessments.htm
[47] https://www.asd.gov.au/publications/protect/network_segmentation_segregation.htm
[48] https://www.asd.gov.au/publications/protect/cloud-security-tenants.htm
[49] https://www.asd.gov.au/publications/protect/Essential_Eight_Explained.pdf

- **Minimise change**
  An important design goal is to ensure that changes to software and configuration are minimised as changes can introduce unacceptable levels of risk. One of the key systems is the iVote voting system supplied by Scytl. Previously the voting system was a version of Scytl's mainstream product customised for the NSW Electoral Commission, which required us to apply continual customised upgrades. One of the design goals for 2019 was to minimise this level of change by using the Scytl's core product and therefore have access to the product's upgrades and patches as they are released. This approach also lowers the implementation risk for the NSW Electoral Commission.

6.5 iVote controls and features

iVote provides an extensive range of controls and features that are used to mitigate against threats and risks as well as build overall elector trust in the functioning of the iVote channel. Many of these have been described in detail within this document. Listed in the table below are details of features and attributes of the iVote channel and how they contributes to the overall electoral environment and integrity of votes cast using iVote.

Table 2: Features and attributes of the iVote channel

Control\feature	Comments
Electoral environment	
iVote is provided alongside other voting channels	• Eligible electors are provided a choice of voting channels and can choose not to use iVote • Electors can make an informed decision to cast their vote using iVote system, based on an understanding of the level of privacy and security provided by iVote
The elector has to select the iVote eligibility criteria they meet	• If the elector fails to meet the iVote eligibility they are presented with the opportunity to apply for a postal vote, if eligible, and information about other voting channels that are available • Ensures electors are provided with a method of voting if they are unable to use iVote
The Electoral Commissioner makes a determination of the Legislative Assembly districts that could have residential addresses that are more than 20 kilometres from a voting centre	• Only electors who live in these electoral districts will be able to apply for iVote using this eligibility criteria
The iVote application will check against EMA to ensure the elector has not already voted through another channel, if they have then the iVote application cannot proceed	• Protects against multiple voting
The iVote systems will be integrated into the NSW Electoral Commission's EMA to provide the status of an elector's iVote transaction (from application through to casting the vote).	• This will allow us to ensure that if an elector cast an early vote through an alternate voting channel prior to casting their iVote then the iVote will not be included into the count

Control\feature	Comments
The NSW Electoral Commission ensures election results from iVote aren't reported in sufficient granularity to allow electors' preferences to be deduced by the public	• With the numbers of electors expected to use iVote this is unlikely to occur
The overall risks associated with iVote will be commensurate with other forms of voting available to electors	See section 5.3
iVote will commence applications the same time as postal vote applications start	• Ensures that iVote isn't presented as a preferred voting channel and allows electors an equal choice of voting channels
iVote voting will commence at the same time early voting starts	• Ensures iVote is consistent with all other voting channels
Integrity	
Silent electors are unable to apply for iVote online	• The iVote registration system does not hold addresses for silent electors. • Protects the privacy of silent electors
The NSW Electoral Commission requests iVote applicants to provide a secondary source of identification which is used to check against the DVS	• Protects against impersonation of electors • Electors who do not provide a second confirmation of identity will receive an acknowledgement letter at their enrolled address confirming that they have applied for iVote and how to proceed with their iVote application
The elector's iVote password strength will be checked to ensure it is adequately protected against brute force hacking	• The iVote application website will provide the elector with a strength meter to assess the elector's password strength taking into account both the length and the ease of guessing using password dictionary attacks • The aim is to achieve an elector password that would take at least three months to crack[50], using current techniques • We recognise that the password strength required to attain 112bit encryption may not be achieved using this technique

[50] The protection against a brute force hack of the password is set against the length of the election – less than six weeks

Control\feature	Comments
	• We have chosen this approach as a balance between useability and securing the elector's vote
For iVote phone voting the elector must create a 10-digit PIN	• Increased from six digits in 2015 • Whilst a 10-digit PIN doesn't offer the same degree of strength as the proposed password for the internet channel NSW Electoral Commission has struck a balance between useability and security.[51].
All electors receive an iVote receipt which is a "digital fingerprint" of their encrypted vote	• The iVote receipt checking website will be available from the start of voting until just before the declaration of results • Electors have the opportunity to check that their vote has been received and continues to be stored securely
The provision of the iVote receipt checking website from the start of voting provides a mechanism to protect against vote coercion\buying	• If an elector has been coerced they can phone the iVote call centre to request another iVote • The call centre provides the elector with a new password\PIN and iVote number • The original credentials and vote are marked as no longer valid ensuring that though vote is not included into the count • The second vote will generate a different iVote receipt and the second vote will be included into the count as iVote only accepts that last vote cast • The original receipt will still be valid on the iVote receipt checking website and can be shown to the coercer as "proof" of the original vote
The use of the separate iVote verification application replaces the previous process for those who voted using the iVote voting website	• Verification is conducted on a different device to that which the vote was cast protecting against malware on elector's voting device • Likely to increase the number of electors verifying their vote
On application, iVote creates unique credentials and a blank virtual ballot paper for each elector	• Greatly reduces the chances of submitting votes by guessing credentials

[51] The only restriction will be the elector will not be able to set their PIN to their mobile phone number

Control\feature	Comments
Electors can apply for iVote before voting opens but for these electors the virtual ballot paper will only be generated once voting starts	• Ensures electors can't cast a ballot prior to the early voting period opening
Complete iVote credential information - iVote number and password\PIN are known only to the elector and not held in any iVote system	• Ensures privacy as their credentials are only known to the elector
For the 2019 State election, the initial display of the Legislative Council ballot paper will be randomised and not favouring groups on the left hand side of the ballot paper	• Due to the size of the Legislative Council ballot paper it is not physically possible to show the entire ballot paper in a single window • For the 2015 State election the initial display always started at the left hand side of the ballot paper but couldn't show all the groups on the screen • Analysis of the results suggested that this may have favoured the groups on the left-hand side of the ballot paper.[52]
Comparisons of results with other voting channels which have similar electoral demographics will be undertaken after election day to identify any substantial difference in the percentage of first preference results by candidate or group	• Provides further assurance that iVote has operated correctly • May be an indicator of tampering within the electronic voting channel
The NSW Electoral Commission will record and report the number of electors who report failed verification, declare they did not register when sent a letter advising of an application in their name, or identify problems accessing the electronic voting system	• Provides confidence in the overall operation of iVote • Aligns with recommendation 23 of the Wilkins Report
Instances of elector impersonation will be prevented by checking a secondary ID (passport, driver license or Medicare), or where ID is not provided; by electors declaring they have been impersonated after receiving notification at their enrolled address that they had applied for iVote and they knew they had not applied	• This will be achieved through the iVote registration system sending an acknowledgement letter to the enrolled address of the applicant • This approach will identify if impersonation has occurred and allow the NSW Electoral Commission to remove the impersonated ballots prior to the close of the election
A virtual ballot paper will only be created by the iVote voting system when a person applies to use iVote.	• Ensures an iVote ballot paper is linked to an eligible elector which can only be accessed by the elector logging on to iVote with linked credentials

[52] https://www.elections.nsw.gov.au/NSWEC/media/NSWEC/Reports/iVote%20reports/Response-by-the-NSW-Electoral-Commission-to-observations-of-bias-in-iVote-results-(PDF-1.8MB).pdf

Control\feature	Comments
	• Protects iVote against "ballot box stuffing" if the iVote Voting system is compromised
Once a vote has been successfully submitted by the elector their iVote number and password\PIN cannot be used again[53]	• If an elector tries to login to the iVote voting website using a valid iVote number and password\PIN for a vote already cast the system will advise the elector that the vote has been cast and that they need to re-apply • Re-applications of this type will be carefully reviewed to ensure there has not been any impersonation of the elector
The elector's hashed password/PIN is encrypted in the elector's web browser before being transmitted	• Protects against the elector's credentials being intercepted in transit between the elector's browser and the iVote servers
The iVote hashing algorithm used to derive the elector's hashed credential now uses SHA256 instead of SHA1	• SHA1 is now obsolete
The introduction of a mathematical provable mixnet improves the verifiability of iVote	• Proof that iVote mixnet hasn't corrupted the vote as the process of mixing and decryption of votes • See section 6.2.4
Network traffic to iVote is continually monitored for anomalies that could be indicators of problems or attempts to attack the iVote systems	• Ensures problems are proactively acted on ensuring the protection of the iVote systems
iVote has been used at State elections and by-elections and the NSW Electoral Commission has enough data to understand the expected iVote usage trends over the period iVote is available. Our operations team will monitor the usage trends during the 2019 State election and using the 2015 trends as a benchmark monitor for any anomalies in usage patterns and trends	• This will allow us to take proactive action if anomalies occur that could indicate problems with iVote
The iVote support team undertakes monitoring of key indicators during the election as well as daily checks of the integrity of the iVote system, these include: • verification of the integrity of the registration system\EMA election roll	• Ensures problems are proactively acted on ensuring the protection of the iVote systems

[53] The only exception will be the Verification Application which requires the elector to provide their password\PIN and iVote Number in order to verify their vote

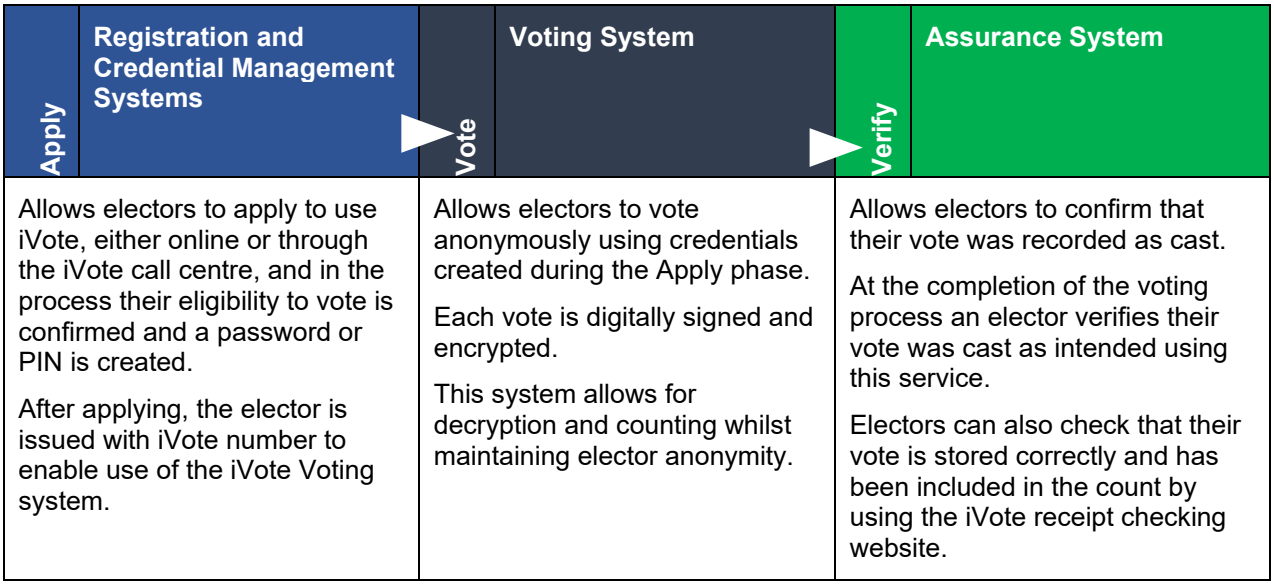
Control\feature	Comments
• monitoring the use of the same e-mail or mobile phone for multiple applications • matching the number of applications for corresponding virtual ballot papers • checking the number of iVotes cast against the iVote status codes • monitoring the number of iVote removals match the number of "invalid" virtual ballot paper • monitoring the iVote system interfaces for errors • undertaking daily ballot box integrity checks	
Prior to the sealing of the ballot box and locking down iVote ready for electors to cast their votes the NSW Electoral Commission undertakes an extensive logic and accuracy test of the iVote systems	• The purpose of the logic and accuracy test is to ensure all parts of the iVote systems are functioning correctly prior to the start of voting and the NSW Electoral Commission is confident in the functioning of the iVote channel
During the election the iVote systems are configured in "lockdown" mode	• In this mode, all operating system accounts, except one for each environment, will be locked out. The remaining account password will be re-set and split between two Electoral Board members. This ensures that it requires both members to gain access to iVote systems • This ensures that no one person is capable of accessing the iVote systems during an election. Should any change to the system at this level be required during an election, it will require the two Electoral Board members to agree to the change, which in turn is recorded and submitted for audit and scrutiny. All access to systems will be monitored and logged to ensure compliance
Useability	
The iVote voting website will be offered in English and additional languages	• Improves the useability and accessibility of iVote
iVote telephone voting system will be implemented in compliance with the Australian Electoral Industry Standard "Automated Telephone Voting" Dec 2011 from the Electoral Council of Australia	

Control\feature	Comments
iVote will allow the submission of an informal vote but will warn the elector prior to being submitted that the vote will not be counted	• Provides the electors with the same options when casting their votes as alternative voting channels • The iVote ensures electors don't cast an informal vote in error
The iVote 'Landing page' at iVote.nsw.gov.au will present a link to where HTVs and group information are available on the main NSW Electoral Commission website, to better inform electors using iVote	• See JSCEM recommendation 9
The iVote websites will follow relevant standards in relation to access by disabled electors to ensure independent voting is available to as many electors as possible	
Electors will have the option to re-apply and re-vote by contacting the iVote call centre	• Provided the NSW Electoral Commission call centre operator is confident of the elector's identity based on their response to questions, the elector will be issued a new iVote number • This process will then mark the current vote as no longer valid and create a new virtual ballot paper. The elector can then proceed to recast their vote
Transparency and Communication	
The NSW Electoral Commission will publish key documents during the course of the project	
The NSW Electoral Commission will inform electors of the security and secrecy features of iVote	• Ensure eligible electors are aware of their voting options, how to correctly use iVote and the protections provided to ensure their privacy and secrecy of their vote

7 Using iVote

The iVote experience for electors involves three steps: apply, vote and (optionally) verify their vote.

Figure 7: iVote user process



7.1 iVote dates for the 2019 State election

Table 3: 2019 State election\iVote key dates

Key election event	Date	Comments
iVote applications open	11 February 2019	
Issue of writ	4 March 2019	
Close of nominations	6 March 2019	
Ballot paper draw	7 March 2019	
Candidate audio files available for review	8 March 2019	By 6pm
iVote voting starts Verification and receipt checking open	11 March 2019	iVote numbers distributed from 8am
Election day	23 March 2019	
iVote applications close	23 March 2019	1pm
iVote voting closes	23 March 2019	6pm
iVote decryption	23 March 2019	After election close
iVote Receipts website closes	29 March 2019	5pm

- Electors will be able to apply to use the iVote system from 11 February 2019. Since the voting phase cannot start until after the close of nominations, all iVote applications are held in the iVote credential management system until the voting period starts.

- Following the close of nominations and the ballot paper draw all the candidate details are loaded into iVote, the logic and accuracy testing is conducted and iVote is locked down ready for voting. Once this is complete the iVote operations team will generate and distribute the iVote numbers for all the electors who have pre-applied.

- The iVote voting period lasts from 11 March until 6pm on the 23 March 2019. During this period electors can apply for and cast their votes using iVote.

- Applications for iVote will close at 1pm on 23 March 2019. This allows the NSW Electoral Commission to process all iVote applications and ensure the electors receive their iVote Number prior to the close of voting at 6pm on 23 March.

- iVote closes, along with all other channels, at 6pm on 23 March 2019. Any elector who has started to cast their vote prior 6pm but hasn't completed at 6pm will not be stopped from casting their vote.

- Once voting has closed and all iVote voting activities are complete, the NSW Electoral Commission will undertake the decryption of the iVote votes.

7.2 Apply

Applications for iVote open, along with postal votes, three to six weeks prior to election day and close at 1pm on election day (see 8.1 Timelines for iVote timeline).

During the application process the elector has to confirm their enrolment details, create a password or PIN, provide an optional secondary confirmation of identity (passport, driver licence or Medicare number), and nominate their preferred manner of receiving their iVote Number (ie via SMS, email, post or phone). These steps are explained in more detail below.

- The elector has to provide their correct enrolment details (family name, address and date of birth) which are used to verify that they are enrolled to vote and also identifies their Legislative Assembly District[54].

- A check will be made against the NSW Electoral Commission Election Management Application (EMA) to ensure the elector has not already voted through another channel. If an elector has already voted their iVote application cannot proceed.

- Next the elector has to select the eligibility criteria they meet. They are presented with both iVote and Postal Vote eligibility criteria to choose from and based on their selection they proceed with their iVote or postal vote application.

- Silent electors are unable to apply for iVote online as the iVote Registration System that handles the application does not hold addresses for Silent Electors. They are directed to the iVote call centre to complete their application.

- NSW Electoral Commission requests iVote applicants to provide a secondary source of identification[55] which is used to check against the federal government's Document Verification Service (DVS)[56]. Electors who do not provide a second confirmation of identity will receive an acknowledgement letter at their enrolled address confirming that they have applied for iVote and how to proceed with their iVote application.

[54] An elector's Legislative Assembly District is based on their enrolled address
[55] Either Medicare number, passport number or driver license number
[56] https://www.dvs.gov.au/Pages/default.aspx

- iVote offers two separate voting channels either voting online or by using a DTMF phone[57]. If the voter chooses to vote using the iVote website they are required to create an alpha-numeric password, alternatively if they choose to use the phone channel they are required to create a ten digit numeric PIN.

- The elector needs to provide a method to receive their iVote number which they will need, along with their password\PIN, to cast their vote. The elector can select from a number of channels: SMS, e-mail, phone call or letter. If the elector chooses either SMS or email they are encouraged to confirm that the mobile phone number or email they enter is valid by triggering a test message.

- The final step is for the elector to submit their application.

7.3 Vote

Once the elector has successfully completed their application their iVote Number is generated and sent to them over the preferred communication channel which they provided during their application. On receipt of their iVote Number, the elector can cast their vote either online using the iVote voting website, or the iVote telephone service, depending on the channel they selected during their application. Alternatively electors who require assistance can call the iVote voting call centre and the call centre operator will enter the vote online on behalf of the voter. All actions by the call centre operators are recorded (video and audio) and are subsequently verified as accurate by another staff member.

The elector logs onto iVote using their iVote Number and either their password for the online channel or their PIN for the telephone channel and make a declaration that they have not already voted after which they are presented with their Legislative Assembly District ballot paper followed by the Legislative Council ballot paper. The iVote website is designed in such a way that ensures ballot paper formality as the elector “clicks” or “taps” against their preferred candidate\group (with each choice being automatically incremented) rather than entering their numeric preferences. The iVote system will still check the formality of each ballot paper and the elector will be warned if they are about to submit an informal ballot paper. The elector is also presented with a summary of their vote prior to submitting and they can go back and change their preferences. If the elector chooses to submit an informal ballot paper after the formality warnings then a blank ballot paper will be submitted marked by iVote as “informal”. On submission of their vote the elector receives an iVote Receipt[58] and for those electors using the iVote voting website they will also receive a QR code which they can use to verify their vote (as described below).

7.4 Verify

Once the elector has submitted their vote they have the option of verifying their vote. For electors who voted online, the verification step will be available to the elector immediately after the vote has been submitted. For electors using the telephone voting service the verification process is similar to that provided in 2015.

Electors who vote using the iVote voting website will need to download the iVote Verification Application, on to their mobile phone[59] — electors will be encouraged to do this prior to voting. On the submission of their vote iVote will display a QR code which the elector will then scan using the iVote Verification Application on their smartphone. They will then be required to enter their iVote Number and password and the iVote Verification Application retrieves and displays the elector’s vote. For electors who use the telephone service they can phone the iVote telephone verification service, provide their iVote Number and PIN and the service will repeat back their votes. In both cases if the votes are not as cast, the elector can phone the iVote call centre for assistance.

[57] This provides an alternative channel for those voters who are unable to vote using a website
[58] A “digital fingerprint” created from the encrypted vote received by iVote
[59] Available for both Android and iPhone iOS

7.5 Re-apply

In the following limited circumstances the elector can re-apply for iVote:

1. if the elector has forgotten their password\PIN their only option is to re-apply for iVote since the NSW Electoral Commission doesn't hold a record of the elector's password\PIN

2. if after verifying their vote the elector believes that vote is not as they had cast, then they can re-apply for iVote

3. if the elector has been coerced during the casting of their iVote then they can re-apply for iVote.

In all cases the elector will have to call the iVote call centre who will undertake the re-application process for the elector. The iVote call centre will process the re-application on the elector's behalf and at the same time the elector's original iVote will be automatically marked as no longer valid and will not be included into the final count. The elector will supply a password\PIN and be issued with a new iVote Number.

7.6 iVote call centre support

The NSW Electoral Commission operates two separate call centres to provide help and assistance to electors using iVote:

- the iVote call centre

- the iVote voting call centre.

The iVote call centre is able to process an elector's application on their behalf, answer enquiries and troubleshoot issues regarding iVote applications. In addition the call centre processes all elector re-applications.

The iVote voting call centre is operated separately to the iVote call centre and is intended to help blind or low vision electors, disabled electors, or electors who would find it difficult to use a computer or have weak or no internet connection to cast their vote. The process to take the votes on behalf of an elector has been designed to protect the privacy of the elector and maintain the secrecy of their vote. Calls to the iVote voting call centre are handled by two separate operators as described below:

- The operator who takes the call from the elector first instructs the elector not to identify themselves.

- Next the call centre operator access the iVote voting website and enters the elector's iVote number and password.

- The call centre operator will then talk the elector through the ballot paper and ask them for their preferences which are entered by the operator.

- On submission of the vote the call centre will repeat the iVote receipt back to the elector.

- Both the call and the screen actions of the first call centre operator are recorded and on completion the recordings are stored in the call centre system.

- The second operator accesses both the voice and screen recordings to verify that the elector's instructions have been followed correctly and the recording is erased afterwards.

The iVote system is available online 24 hours a day 7 days a week, however the call centres will only be available during extended business hours as published for each election.

7.7 Communication and stakeholder engagement

The NSW Electoral Commission will undertake a program of consultation and communication to raise awareness of iVote amongst eligible electors and ensure that it will effectively and appropriately address the needs of these electors.

Our goal is to make it easy for people to participate in the democratic process by engaging them in ways that work for them, including being available through people's preferred information platforms and formats. We have undertaken extensive customer research to understand the information needs of voters. What we learned has informed the development of our communications and stakeholder engagement strategies, the design of our new website and helped us create an evidence-based approach to communicating effectively with our audiences. Our integrated communications provide consistent, timely and accurate messaging. We have aligned the way we communicate across our channels including our call centre, website, social media, advertising and direct communications.

8 Appendices

8.1 Timelines

Figure 8: iVote election operational timelines

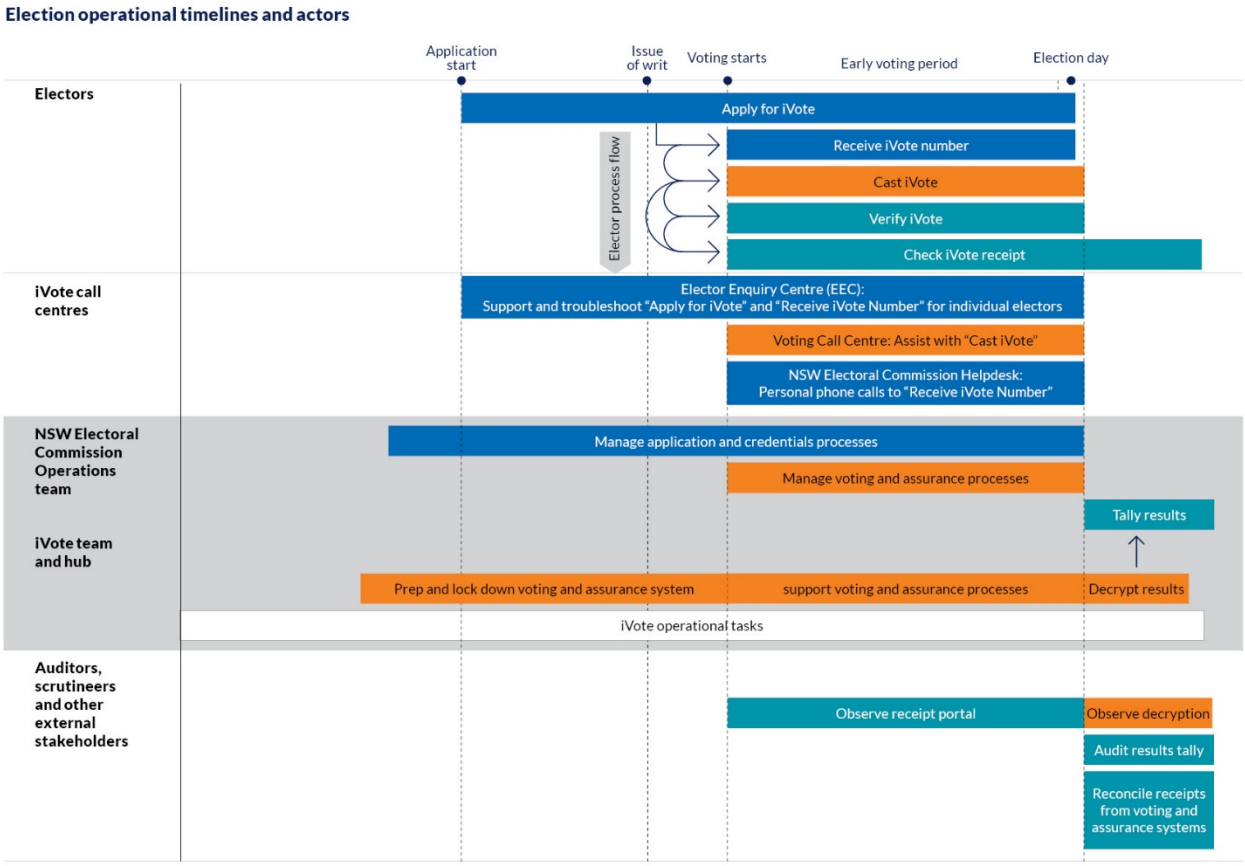
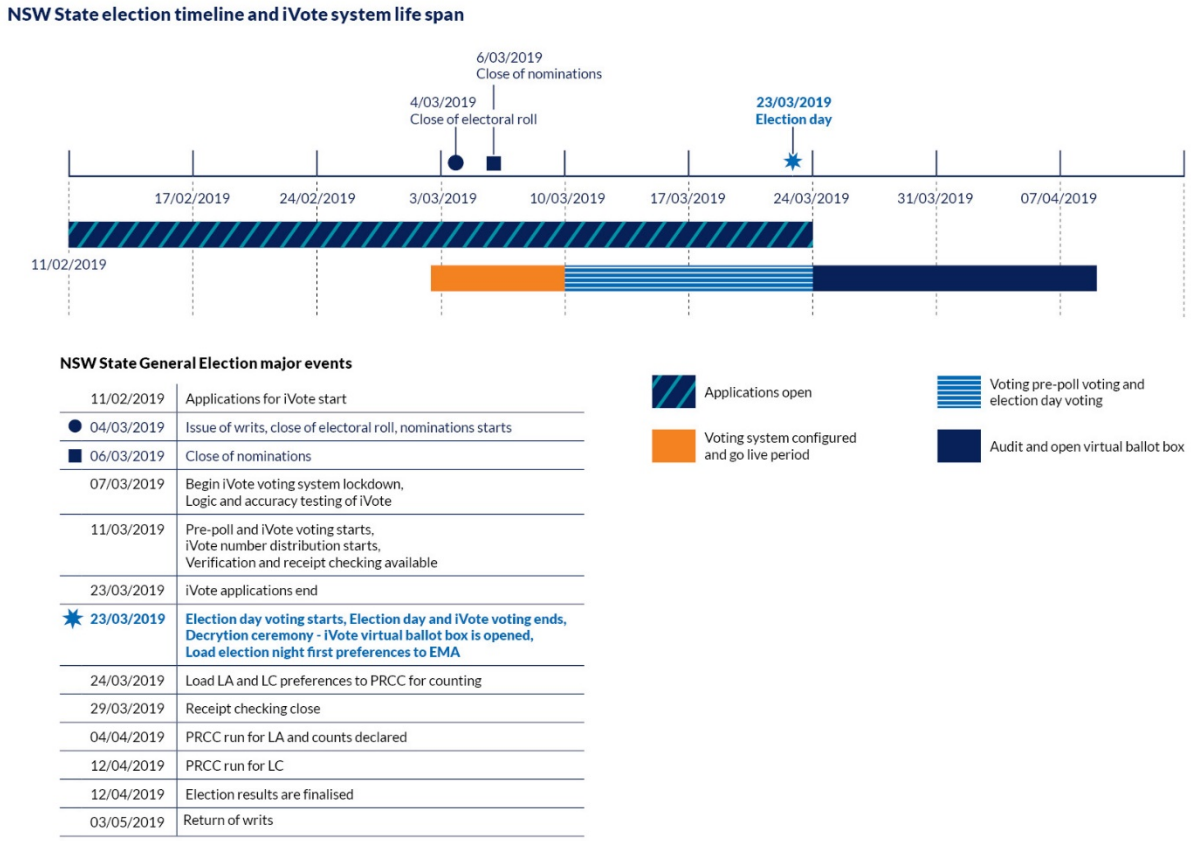


Figure 9: NSW State election timeline and iVote system life span



8.2 JSCEM iVote recommendations

No	Recommendation	Related paragraph in this report
6	The Committee recommends that: the NSW Government establishes an independent panel of experts to conduct a full inquiry into the iVote internet and telephone voting system to consider security, auditing and scrutineering issues prior to the 2019 State election; the panel contains members with expertise in at least the following areas of information technology: online voting; privacy; security; and cybercrime; iVote is only used for the 2019 State election if the security concerns highlighted by the Committee in this report have been addressed	2.8
7	The Committee recommends that the NSW Government makes the iVote source code publicly available	5.2.2
8	The Committee recommends that the Electoral Commission provides additional and targeted advertising about iVote to:	7.7

No	Recommendation	Related paragraph in this report
	people with disability to ensure they are aware of this voting option; and members from culturally and linguistically diverse communities in the same 24 languages that the Electoral Commission currently provides information in for other forms of voting	
9	The Committee recommends that political parties' 'how-to-vote' cards be made available for iVote users	6.5

8.3 ECANZ principles

Below is the detailed description of the 11 key principles for any Australian internet voting system.

Enfranchisement

1. Accessibility – as far as is practical, all eligible people should be able to access the Internet voting system.

   The Internet voting service shall be designed, as far as practicable, to enable eligible voters to vote independently regardless of disabilities, technology or geography. The Internet voting service will be an additional and optional service for specific eligible voters to use. It would be offered in conjunction with other pre-existing methods of voting.

2. Usability – the process of Internet voting should be sufficiently easy for eligible people to cast a vote.

   The user interface of the Internet voting service should be easy to understand, intuitive, and able to be used by all eligible voters on multiple technology platforms. Information provided may be presented differently depending on the differing technologies and channels which the service can be accessed on. For example, the electoral content presented on an electronic ballot paper will be the same as on the physical paper ballot paper (ensuring impartiality and equitably); however changes may be made in accordance with relevant legislative provisions while ensuring usability on each technology platform.

3. One person, one vote – the ability to ensure that each eligible elector receives only their voting entitlement.

   The Internet voting service should enable each eligible voter to be uniquely identified, ensuring that they are distinguishable from other voters. The service should cater for any legislative requirements around the presentation of identification documents. An eligible voter will only be able to use this channel if they can be uniquely identified this way. The service will check eligibility and only grant access to those that have been authenticated as an eligible voter. The service will have a process to ensure that only one vote per eligible voter is admitted to the count.

Integrity

4. Security – prevention of loss, corruption or tampering of votes.

   The Internet voting service and responsible Electoral Management Body shall protect authentication data so that unauthorised parties cannot misuse, intercept, modify, or otherwise gain knowledge of this data. The authenticity, availability and integrity of the electoral roll and lists of candidates shall be maintained. Only persons authorised by the electoral management body shall have access to the central infrastructure, the servers and the electoral event data.

The audit system should be able to detect voter fraud and provide proof that all counted votes are authentic. The audit system shall be open and comprehensive, and actively report on potential issues and threats. Where incidents that could threaten the integrity of the service occur, those responsible for operating the equipment shall immediately inform the electoral management body. Procedures shall be established to ensure regular installation of updated versions and corrections of all relevant software as the service will need to be continually evolved to meet and protect against potential and actual issues and threats. The service will encrypt votes if they are to be stored or communicated outside controlled environments. The electoral management body shall handle all cryptographic material securely. Votes shall be kept sealed[60] until after the close of polling.

5. Robustness – the system and processes are not subject to significant interruption or failure.

   Robustness applies to people, process and technology. The Internet voting service must be available, reliable and secure to ensure that it can function on its own, irrespective of shortcomings in the hardware or software. The technical solution for the service will be peer-reviewed to help ensure availability, reliability, usability and security. The service shall identify votes that are affected by an irregularity so that necessary measures are taken and stakeholders are informed. The electoral management body administering the service will ultimately be responsible for compliance with the above even in the case of failure.

6. Transparency – the system and processes be designed to enable scrutiny, to provide stakeholder confidence.

   The Internet voting service and accompanying processes will be established with a focus on transparency. The service will ensure that the way in which eligible voters are guided through the Internet voting process shall not lead them to vote without due diligence or without confirmation. The service should be designed to allow the voter to express his or her true will. A voter will be allowed sufficient time to consider their choices and will be under no obligation to commit their vote without time for reflection on their choices. Upon casting their vote, the service will verify to the voter that his or her intention is accurately represented and that the vote has been submitted. Any alteration to the voter's vote should be detected by the service.

   Voters and third parties should be able to observe the count of the votes and check that only eligible voters' votes are included in the results. The service will provide evidence that only eligible voters' votes have been included and this evidence will be auditable.

   Clear and unambiguous information about the Internet voting service should be available to the public explaining how to use the service and how the service operates.

   The service should be open for verification, assurance and scrutiny purposes. Observers, to the extent permitted by law, shall be enabled to observe, comment on and scrutinise the Internet voting component of an election, including the compilation of the results.

7. Independence – full control of the system and processes shall rest with the Electoral Management Body.

   The electoral management body will be accountable for the Internet voting service of an electoral event. The electoral management body must be able to put into place assurances that maintain their electoral integrity and independence.

8. Impartiality – The voter's intention should not be affected by the voting system.

   An eligible voter's intent should not be affected by the Internet voting service. The service will ensure that the way in which voters are guided through the process and the information displayed will not influence their vote.

[60] Sealed is an analogy to the seal on a physical ballot box. This is the term used in the European standards

The service should be structured to ensure that voters do not miss anything during the voting process. It should provide a means for informal voting by allowing a blank vote to be cast, however advising the voter they would be casting an informal vote and providing them with the option to change their vote if they wish. This provides an equitable approach across channels enabling voters to cast an informal vote via both the service and the paper-based option. Other than a blank ballot paper, all formality rules will be enforced by the service.

9. Accuracy – the system should accurately capture, store and export the voters intention

   The Internet voting service shall provide sound evidence that only votes from eligible voters are included in the final result while de-identifying a completed ballot paper from its voter. The service shall support the voter in marking the ballot paper and accurately store, capture, verify, and export the vote cast. Before an event, the electoral management body administering the service shall satisfy itself that the service is genuine and operates correctly.

   The service shall allow and support evaluation regarding the compliance of the service and its related components. This should occur upon introduction, periodically and after significant change to the service has been made.

Privacy

10. Privacy – The system and processes shall maintain the privacy of personal information.

    The Internet voting service shall process and store, as long as necessary, only the personal data needed for the conduct of the electoral event. The electoral management body administering the service will determine what information is deemed necessary to keep and dispose in accordance with relevant legislative obligations. Any information retained will be secure and any information not required to be retained will be securely disposed of.

11. Secrecy – the system and processes shall maintain the secrecy of the votes cast.

    The Internet voting service shall be organised in such a way as to ensure that the secrecy of the vote is respected at all stages of the voting process – from pre-polling through to counting of the votes. Votes shall remain sealed until the counting process commences. During completion of the ballot paper, the service will protect the secrecy of the voter's choice. The service should not provide a proof of vote preferences that would facilitate coercion or vote buying.

    The service will be able to de-identify a voter from their completed ballot paper to preserve the secrecy of the ballot. The order in which votes are cast shall be mixed[61] so as to deny reconstruction of the order of votes submitted.

    It is acknowledged that a tension can arise in giving effect to some of these principles. For example, an appropriate balance needs to be struck between usability and security. Such decisions also need to take into account legislative electoral requirements and the current technological environment.

[61] In electronic voting, the concept of mixing is used to remove all links that may exist between the voter and their ballot paper so that it becomes infeasible to re-construct any such links once the votes have been mixed

8.4 ECANZ principles and Council of Europe mapping

Table 4: Showing how the CoE standards cover the ECANZ principles

Council of Europe standards		ECANZ principles										
		Enfranchisement			Integrity						Privacy	
Heading	Standard	Accessibility	Usability	One person, one vote	Security	Robustness	Transparency	Independence	Impartiality	Accuracy	Secrecy of cast vote	Privacy of personal information
Universal suffrage	1. The voter interface of an e-voting system shall be easy to understand and use by all voters.		X									
Universal suffrage	2. The e-voting system shall be designed, as far as is practicable, to enable persons with disabilities and special needs to vote independently.	X	X									
Universal suffrage	3. Unless channels of remote e-voting are universally accessible, they shall be only an additional and optional means of voting.	X										
Universal suffrage	4. Before casting a vote using a remote e-voting system, voters' attention shall be explicitly drawn to the fact that the e-election in which they are submitting their decision by electronic means is a real election or referendum.	X										

Council of Europe standards		ECANZ principles										
		Enfranchisement			Integrity						Privacy	
Heading	Standard	Accessibility	Usability	One person, one vote	Security	Robustness	Transparency	Independence	Impartiality	Accuracy	Secrecy of cast vote	Privacy of personal information
Equal suffrage	5. All official voting information shall be presented in an equal way, within and across voting channels.		X									
Equal suffrage	6. Where electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the result.					X					X	
Equal suffrage	7. Unique identification of voters in a way that they can unmistakably be distinguished from other persons shall be ensured.			X	X							
Equal suffrage	8. The e-voting system shall only grant a user access after authenticating her/him as a person with the right to vote.				X							
Equal suffrage	9. The e-voting system shall ensure that only the appropriate number of votes per voter is cast, stored in the electronic ballot box and included in the election result.			X								
Free suffrage	10. The voter's intention shall not be affected by the voting system, or by any undue influence.	X			X				X			

Council of Europe standards		ECANZ principles										
		Enfranchisement			Integrity						Privacy	
Heading	Standard	Accessibility	Usability	One person, one vote	Security	Robustness	Transparency	Independence	Impartiality	Accuracy	Secrecy of cast vote	Privacy of personal information
Free suffrage	11. It shall be ensured that the e-voting system presents an authentic ballot and authentic information to the voter.					X						
Free suffrage	12. The way in which voters are guided through the e-voting process shall not lead them to vote precipitately or without confirmation.		X									
Free suffrage	13. The e-voting system shall provide the voter with a means of participating in an election or referendum without the voter exercising a preference for any of the voting options.		X									
Free suffrage	14. The e-voting system shall advise the voter if he or she casts an invalid e-vote.		X									
Free suffrage	15. The voter shall be able to verify that his or her intention is accurately represented in the vote and that the sealed vote has entered the electronic ballot box without being altered. Any undue influence that has modified the vote shall be detectable.						X					
Free suffrage	16. The voter shall receive confirmation by the system that the vote has been cast successfully and that the whole voting procedure has been completed.		X									

Council of Europe standards		ECANZ principles										
		Enfranchisement			Integrity						Privacy	
Heading	Standard	Accessibility	Usability	One person, one vote	Security	Robustness	Transparency	Independence	Impartiality	Accuracy	Secrecy of cast vote	Privacy of personal information
Free suffrage	17. The e-voting system shall provide sound evidence that each authentic vote is accurately included in the respective election results. The evidence should be verifiable by means that are independent from the e-voting system.						X					
Free suffrage	18. The system shall provide sound evidence that only eligible voters' votes have been included in the respective final result. The evidence should be verifiable by means that are independent from the e-voting system.						X					
Secret suffrage	19. E-voting shall be organised in such a way as to ensure that the secrecy of the vote is respected at all stages of the voting procedure.										X	
Secret suffrage	20. The e-voting system shall process and store, as long as necessary, only the personal data needed for the conduct of the e-election.											X
Secret suffrage	21. The e-voting system and any authorised party shall protect authentication data so that unauthorised parties cannot misuse,			X	X							

Council of Europe standards		ECANZ principles										
		Enfranchisement			Integrity						Privacy	
Heading	Standard	Accessibility	Usability	One person, one vote	Security	Robustness	Transparency	Independence	Impartiality	Accuracy	Secrecy of cast vote	Privacy of personal information
	intercept, modify, or otherwise gain knowledge of this data.											
Secret suffrage	22. Voters' registers stored in or communicated by the e-voting system shall be accessible only to authorised parties.				X							
Secret suffrage	23. An e-voting system shall not provide the voter with proof of the content of the vote cast for use by third parties.										X	
Secret suffrage	24. The e-voting system shall not allow the disclosure to anyone of the number of votes cast for any voting option until after the closure of the electronic ballot box. This information shall not be disclosed to the public until after the end of the voting period.								X			
Secret suffrage	25. E-voting shall ensure that the secrecy of previous choices recorded and erased by the voter before issuing his or her final vote is respected.										X	
Secret suffrage	26. The e-voting process, in particular the counting stage, shall be organised in such a way that it is not possible to reconstruct a link between the unsealed vote and the voter. Votes are, and remain, anonymous.										X	

Council of Europe standards		ECANZ principles										
		Enfranchisement			Integrity						Privacy	
Heading	Standard	Accessibility	Usability	One person, one vote	Security	Robustness	Transparency	Independence	Impartiality	Accuracy	Secrecy of cast vote	Privacy of personal information
Regulatory and organisational requirements	27. Member States that introduce e-voting shall do so in a gradual and progressive manner.					X						
Regulatory and organisational requirements	28. Before introducing e-voting, member States shall introduce the required changes to the relevant legislation.					X						
Regulatory and organisational requirements	29. The relevant legislation shall regulate the responsibilities for the functioning of e-voting systems and ensure that the electoral management body has control over them.							X				
Regulatory and organisational requirements	30. Any observer shall be able to observe the count of the votes. The electoral management body shall be responsible for the counting process.						X					
Transparency and observation	31. Member States shall be transparent in all aspects of e-voting.						X					

Council of Europe standards		ECANZ principles										
		Enfranchisement			Integrity						Privacy	
Heading	Standard	Accessibility	Usability	One person, one vote	Security	Robustness	Transparency	Independence	Impartiality	Accuracy	Secrecy of cast vote	Privacy of personal information
Transparency and observation	32. The public, in particular voters, shall be informed, well in advance of the start of voting, in clear and simple language, about: - any steps a voter may have to take in order to participate and vote; - the correct use and functioning of an e-voting system; - the e-voting timetable, including all stages.						X					
Transparency and observation	33. The components of the e-voting system shall be disclosed for verification and certification purposes.						X					
Transparency and observation	34. Any observer, to the extent permitted by law, shall be enabled to observe and comment on the e-elections, including the compilation of the results.						X					
Transparency and observation	35. Open standards shall be used to enable various technical components or services, possibly derived from a variety of sources, to inter-operate.						X					
Accountability	36. Member States shall develop technical, evaluation and certification requirements and shall ascertain that they fully reflect the relevant legal and democratic principles.							X				

Council of Europe standards		ECANZ principles										
		Enfranchisement			Integrity						Privacy	
Heading	Standard	Accessibility	Usability	One person, one vote	Security	Robustness	Transparency	Independence	Impartiality	Accuracy	Secrecy of cast vote	Privacy of personal information
	Member States shall keep the requirements up to date.											
Accountability	37. Before an e-voting system is introduced and at appropriate intervals thereafter, and in particular after any significant changes are made to the system, an independent and competent body shall evaluate the compliance of the e-voting system and of any information and communication technology (ICT) component with the technical requirements. This may take the form of formal certification or other appropriate control.									X		
Accountability	38. The certificate, or any other appropriate document issued, shall clearly identify the subject of evaluation and shall include safeguards to prevent its being secretly or inadvertently modified.									X		
Accountability	39. The e-voting system shall be auditable. The audit system shall be open and comprehensive, and actively report on potential issues and threats.				X		X					

Council of Europe standards		ECANZ principles										
		Enfranchisement			Integrity						Privacy	
Heading	Standard	Accessibility	Usability	One person, one vote	Security	Robustness	Transparency	Independence	Impartiality	Accuracy	Secrecy of cast vote	Privacy of personal information
Reliability and security of the system	40. The electoral management body shall be responsible for the respect for and compliance with all requirements even in the case of failures and attacks. The electoral management body shall be responsible for the availability, reliability, usability and security of the e-voting system.				X							
Reliability and security of the system	41. Only persons authorised by the electoral management body shall have access to the central infrastructure, the servers and the election data. Appointments of persons authorised to deal with e-voting shall be clearly regulated.				X							
Reliability and security of the system	42. Before any e-election takes place, the electoral management body shall satisfy itself that the e-voting system is genuine and operates correctly.					X						
Reliability and security of the system	43. A procedure shall be established for regularly installing updated versions and corrections of all relevant software.				X		X					

Council of Europe standards		ECANZ principles										
		Enfranchisement			Integrity						Privacy	
Heading	Standard	Accessibility	Usability	One person, one vote	Security	Robustness	Transparency	Independence	Impartiality	Accuracy	Secrecy of cast vote	Privacy of personal information
Reliability and security of the system	44. If stored or communicated outside controlled environments, the votes shall be encrypted.				X							
Reliability and security of the system	45. Votes and voter information shall be kept sealed until the counting process commences.				X							
Reliability and security of the system	46. The electoral management body shall handle all cryptographic material securely.				X							
Reliability and security of the system	47. Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment shall immediately inform the electoral management body.				X							
Reliability and security of the system	48. The authenticity, availability and integrity of the voters' registers and lists of candidates shall be maintained. The source of the data shall be authenticated. Provisions on data protection shall be respected.				X							

Council of Europe standards		ECANZ principles										
		Enfranchisement			Integrity						Privacy	
Heading	Standard	Accessibility	Usability	One person, one vote	Security	Robustness	Transparency	Independence	Impartiality	Accuracy	Secrecy of cast vote	Privacy of personal information
Reliability and security of the system	49. The e-voting system shall identify votes that are affected by an irregularity.					X						

8.5 iVote mapping to Council of Europe standards

Heading	Standard	iVote
Universal suffrage	The voter interface of an e-voting system shall be easy to understand and use by all voters.	• The system will be tested by potential electors for the purposes of improving the elector experience and gauging the level of trust prior to the election • The iVote IVR telephone system will allow the elector to save a partially completed vote and exit the system. Electors will be able to access their ballot paper again and continue to complete and submit their vote.[62] • iVote voting website will be provided in English plus three additional languages • The iVote telephone voting system will be implemented in compliance with the Australian Electoral Industry Standard "Automated Telephone Voting"
Universal suffrage	The e-voting system shall be designed, as far as is practicable, to enable persons with disabilities and special needs to vote independently.	• The web based iVote system will meet WCAG 2.0 (Web Content Accessibility Guidelines) Level AA standards
Universal suffrage	Unless channels of remote e-voting are universally accessible, they shall be only an additional and optional means of voting.	• iVote is offered alongside all other voting channels both during the early voting period and on election day
Universal suffrage	Before casting a vote using a remote e-voting system, voters' attention shall be explicitly drawn to the fact that the e-election in which they are submitting their decision by electronic means is a real election or referendum.	• The Apply and Vote websites are designed to ensure the elector clearly understand that they are applying\voting in the NSW State election. • The Apply and Vote web sites require the elector to make declarations in relation to both their application and their vote with regard to the State election • The iVote demonstration voting system is clearly labelled
Equal suffrage	All official voting information shall be presented in an equal way, within and across voting channels.	• Information regarding iVote on the NSW Electoral Commission websites will be provided in the context of other voting options. This includes information on voting channels in community languages

[62] This feature is not available votes cast using the iVote website

Heading	Standard	iVote
		• Both the Legislative Council (LC) and Legislative Assembly (LA) ballot papers are presented in accordance with the legislation\approved procedures
Equal suffrage	Where electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the result.	• All votes cast using iVote are securely mixed and decrypted after the close of voting • Once decrypted, we will process and provide all iVote 1st preference and TCP results alongside other voting channels • LC and LA votes from all voting channels including iVote are input into the NSW Electoral Commission's PRCC for calculation of results • iVote uses zero-knowledge proof to ensure the secure & correct transfer of results from decryption process to the counting system • Decrypted votes imported into PRCC will have a ballot sequence ID to ensure proper importation of the iVote ballot papers • There is a reconciliation process in place to ensure the votes provided by iVote have been processed correctly in EMA and PRCC • The NSW Electoral Commission will publish iVote receipts of all votes included in the count
Equal suffrage	Unique identification of voters in a way that they can unmistakably be distinguished from other persons shall be ensured.	• Each elector has to provide a password\PIN on application and are then provided with a unique iVote number by the system. • At the same time the iVote system creates a unique credential hash of the elector's hashed password\PIN and iVote number and links this to the elector's Virtual Ballot Paper. • When the elector votes they have to provide their password\PIN plus iVote number which is used to compute the iVote credential hash and present their virtual ballot paper. • The password\PIN and iVote Number combination can only be used once to successfully cast a vote

Heading	Standard	iVote
Equal suffrage	The e-voting system shall only grant a user access after authenticating her/him as a person with the right to vote.	• Only after the elector has successfully applied will iVote create their electronic\virtual ballot papers for the correct State district • iVote generates and sends the electors their unique iVote Number • An elector can only cast their vote with the iVote Number and their password\PIN created by the elector when applying
Equal suffrage	The e-voting system shall ensure that only the appropriate number of votes per voter is cast, stored in the electronic ballot box and included in the election result.	• Once the elector has applied for iVote, they will not be able to apply for another iVote for the same election event • Once the elector has cast their vote, the scrutiny process ensures that any additional votes cast, via iVote or another early voting channel, are rejected and only one is admitted to the count • NSW Electoral Commission allows an elector to verify their vote and to re-apply for another iVote should they believe their vote isn't correct • Their initial vote is set aside and not admitted to the count. • The re-application can only be done by calling the NSW Electoral Commission call centre • Prior to decrypting the votes NSW Electoral Commission remove any rejected / set aside iVotes, leaving only the appropriate number of votes per elector for inclusion in the count
Free suffrage	The voter's intention shall not be affected by the voting system, or by any undue influence.	• iVote is presented alongside all other channels of voting • The iVote registration system allows the elector to choose a postal vote or vote using iVote • The LA and LC ballot papers show the correct candidates in correct order and are presented in accordance with the legislation and approved procedures • Due to the size of the Council paper the initial display will be randomised so there is no bias towards groups on the left hand side of the paper

Heading	Standard	iVote
		• iVote provides the elector with the chance to verify their vote on a medium other than that which they cast their vote to ensure their vote is cast as intended • NSW Electoral Commission offers the elector with the opportunity to recast their iVote if they believe that the vote is incorrect or their vote was cast under duress
Free suffrage	It shall be ensured that the e-voting system presents an authentic ballot and authentic information to the voter.	• Once nominations have closed and the ballot draw is complete, the NSW Electoral Commission conducts extensive logic and accuracy testing to ensure iVote works correctly for all scenarios • NSW Electoral Commission conducts extensive quality assurance on iVote ballot papers to ensure correctness of all ballot papers • Logic and accuracy testing is conducted in front of scrutineers as part of the NSW Electoral Commission's transparency approach • Once the logic and accuracy tests are complete the ballot box is confirmed as empty and voting can start • Instructions to the elector are presented in accordance with the legislation and approved procedures
Free suffrage	The way in which voters are guided through the e-voting process shall not lead them to vote precipitately or without confirmation.	• Electors are provided with information on how to use iVote to enter their preferences • Electors are always presented their LA ballot papers first along with information on how to complete a valid\formal ballot paper • iVote validates that each paper has been completed correctly and presents the elector with details of their entered preferences prior to submitting their vote • Electors are given the opportunity to correct or change their vote prior to submitting • Electors are able to submit a blank vote but are warned prior to submitting that their vote will not count

Heading	Standard	iVote
Free suffrage	The e-voting system shall provide the voter with a means of participating in an election or referendum without the voter exercising a preference for any of the voting options.	• Electors are able to submit a blank vote for either the LA or LC elections but are warned prior to submitting that their vote will not count
Free suffrage	The e-voting system shall advise the voter if he or she casts an invalid e-vote.	• The iVote voting system interface is designed so the elector enters their vote by double clicking on the square next to the candidate(s) of their choice in descending order of preference. This approach ensures that a elector can only submit a formal vote • The elector can submit a blank vote if they choose to do so. The vote is marked as "Informal" in the voting system.
Free suffrage	The voter shall be able to verify that his or her intention is accurately represented in the vote and that the sealed vote has entered the electronic ballot box without being altered. Any undue influence that has modified the vote shall be detectable.	• iVote offers two forms of Cast as Intended verification for electors • For those electors who vote over the Internet using a browser they will able to verify their vote on completion of voting using a mobile phone application to scan a QR code that is presented on the browser. • For those who vote using the iVote telephone voting services, they will be able to verify their vote by using the phone verification vote • The elector is provided with an iVote Receipt on the submission of the vote. • iVote provides a receipting checking portal from the start of voting for electors to check their vote has been received and is in the ballot box • The encryption of the vote includes an integrity hash which remains with the vote to check for any changes to the vote • The iVote system uses a mixnet to anonymise the vote which includes the use of mathematical proofs to ensure no changes to the vote during decryption • The decrypted votes are loaded into the NSW Electoral Commission's PRCC with a ballot paper Sequence ID to track correct loading into PRCC.

Heading	Standard	iVote
Free suffrage	The voter shall receive confirmation by the system that the vote has been cast successfully and that the whole voting procedure has been completed.	• On completion of the ballot papers and submitting their vote the elector receives a receipt which can be used to later confirm that the vote was received and is in the virtual ballot box • On receipt of the vote the iVote system provides the elector with a QR which can be used to verify the vote has been cast as intended • The elector is first shown their LA ballot paper and if the elector moves to the LC without selecting any preferences they are warned & have to affirm their action. • Before seeing the LC ballot paper the LA summary screen shows that no votes have been cast • Similarly if the elector chooses to cast an incomplete LC ballot paper they are warned and have to affirm their actions • iVote presents the ballot to be submitted for checking before it is actually submitted. • The elector receives a warning if they try to submit before sufficient preferences for a formal vote are recorded.
Free suffrage	The e-voting system shall provide sound evidence that each authentic vote is accurately included in the respective election results. The evidence should be verifiable by means that are independent from the e-voting system.	• When an elector submits their vote iVote generates a receipt • The receipt of each vote that is included into the counting process is published on the iVote receipt checking website where electors can check their vote was included in the count. • Electors who cannot find their receipt on the web site can contact the call centre to inquire the reasons why their vote was not admitted to the count • The iVote system uses a mixnet to anonymise the vote which includes the use of mathematical proofs to ensure no changes to the vote during decryption • The decrypted votes are loaded into the NSW Electoral Commission PRCC with a ballot paper Sequence ID to track correct loading into PRCC.

Heading	Standard	iVote
Free suffrage	The system shall provide sound evidence that only eligible voters' votes have been included in the respective final result. The evidence should be verifiable by means that are independent from the e-voting system.	• During the iVote application the elector will need to find themselves on the electoral roll, including providing a secondary form of identification • The elector has to make a declaration that they meet one of the legislated eligibility criteria • Only electors who reside within a NSW Electoral Commission LA District that contains addresses that are more than 20kms from a voting centre are able to claim this eligibility • Any elector who is a "silent elector" will automatically be eligible to use iVote • Checks are made against the NSW Electoral Commission's EMA to ensure a elector hasn't already voted through another channel • As part of the decryption process final checks are made to ensure that the elector hasn't voted by another channel
Secret suffrage	E-voting shall be organised in such a way as to ensure that the secrecy of the vote is respected at all stages of the voting procedure.	• Voting sessions and cast ballots are encrypted and securely transmitted to the iVote system • The NSW Electoral Commission has designed the infrastructure to generally accepted security principles and practices • iVote systems that contain links to the elector's hashed credentials and their electoral ID (SPID) are separate from the iVote voting system • No single user will have access to all systems • Ballots are anonymised prior to decryption
Secret suffrage	The e-voting system shall process and store, as long as necessary, only the personal data needed for the conduct of the e-election.	• The only iVote system that has access to elector's personal information is the Registration System which has a copy of the electoral roll. • The only additional personal information held is contact details (eg mobile phone number, e-mail) supplied by the elector

Heading	Standard	iVote
		• iVote doesn't hold details of the secondary identification data • All data is discarded after the declaration of the election and the period in which an election may be challenged
Secret suffrage	The e-voting system and any authorised party shall protect authentication data so that unauthorised parties cannot misuse, intercept, modify, or otherwise gain knowledge of this data.	• The NSW Electoral Commission is responsible for the operation of the Registration System which relies on the electoral roll for the authentication of the elector • The iVote Registration System is operated on infrastructure under the control of the NSW Electoral Commission • When the elector applies to use iVote they create their own password\PIN which is not stored within the iVote systems
Secret suffrage	Voters' registers stored in or communicated by the e-voting system shall be accessible only to authorised parties.	• The NSW Electoral Commission records that an elector has voted using the iVote channel which is held in EMA • The NSW Electoral Commission provide voting statistics to authorised parties and in their reports following elections • The statistics and information regarding the iVote channel is de-personalised • If there is a risk of identifying an elector due to a data set being too small, the practice is to combine with another voting channel
Secret suffrage	An e-voting system shall not provide the voter with proof of the content of the vote cast for use by third parties.	• The iVote voting system provides the elector with a receipt to confirm the vote has been received and stored by the iVote voting system • The receipt cannot be used to determine the elector's preferences • iVote maintains receipts for all votes cast even if an elector re-applies and casts a second vote • If the elector has been coerced they can show the coercer the receipt of the original vote cast although it will not be counted

Heading	Standard	iVote
		• The verification process allows the elector to check their vote after submitting their vote. This is done using a mobile phone, with the iVote Verification Application installed, to scan the QR code presented to the elector • The elector has to enter their password and iVote Number and their vote will be shown to them for verification • Electors who voted using the iVote telephone voting system will be able to verify their vote using the iVote telephone verification system • There is a time limit after submitting a vote for verification which limits the ability for the elector to reveal their elector to others
Secret suffrage	The e-voting system shall not allow the disclosure to anyone of the number of votes cast for any voting option until after the closure of the electronic ballot box. This information shall not be disclosed to the public until after the end of the voting period.	• The iVote captures and encrypts votes in the electronic ballot box. • The votes cannot be decrypted until after voting closes – 6pm on election day • De-encryption of the votes requires a quorum of the NSW Electoral Commission Electoral Board to recreate the decryption key
Secret suffrage	E-voting shall ensure that the secrecy of previous choices recorded and erased by the voter before issuing his or her final vote is respected.	• iVote doesn't allow the elector to delete their votes and recast • Electors can only recast their vote by contacting the call centre who will mark the previous vote as no longer valid • This is then removed from the final count and only the last vote cast will be counted
Secret suffrage	The e-voting process, in particular the counting stage, shall be organised in such a way that it is not possible to reconstruct a link between the unsealed vote and the voter. Votes are, and remain, anonymous.	• As part of the decryption of the votes iVote implements a mixing process that breaks any correlation between the elector and their votes in the ballot box • All votes to be decrypted are shuffled • At the same time the iVote operations will remove the links between the Credential Hashes and the elector's SPID in the iVote Credential Management system

Heading	Standard	iVote
		• The mixing also produces proofs to provide surety that the mixing did not manipulate any of the contents of the votes • The file of decrypted votes will have a ballot paper sequence ID to ensure the votes are loaded correctly into the NSW Electoral Commission PRCC
Regulatory & organisational requirements	Member States that introduce e-voting shall do so in a gradual and progressive manner.	• iVote was introduced by the NSW Electoral Commission at the 2011 State election. Usage has increased for subsequent by-elections and the 2015 State election • NSW Electoral Commission has sought to continually improve iVote for each State election • The NSW Electoral Commission is a member of the ECANZ E-Voting Working Group and is working towards the establishment of an Australian e-voting system
Regulatory & organisational requirements	Before introducing e-voting, member States shall introduce the required changes to the relevant legislation.	• iVote was introduced after the relevant framework was created by the *Parliamentary Electorates and Elections Act 1912*, since updated under the *Electoral Act 2017* • The Electoral Commissioner publishes Approved Procedures under the Act in relation to the use and conduct of the iVote channel
Regulatory & organisational requirements	The relevant legislation shall regulate the responsibilities for the functioning of e-voting systems and ensure that the electoral management body has control over them.	• The NSW Electoral Commission is responsible under the legislation for the delivery and functioning of iVote
Regulatory & organisational requirements	Any observer shall be able to observe the count of the votes. The electoral management body shall be responsible for the counting process.	• NSW Electoral Commission officials perform the decryption of the iVote ballot papers and the transfer of those ballots to the counting systems in the presence of appointed scrutineers and other independent observers • The NSW Electoral Commission developed, owns and operates the system that is used to count the results of both LA and LC elections • Votes cast through iVote are included in the counting system along with votes cast through all other channels

Heading	Standard	iVote
Transparency & observation	Member States shall be transparent in all aspects of e-voting.	• The NSW Electoral Commission works to provide as much information regarding the operation of iVote as possible • As part of the iVote refresh project for the 2019 State election, particular emphasis has been placed on the transparent operation of iVote – see paragraph 5.2 of this document for details
Transparency & observation	The public, in particular voters, shall be informed, well in advance of the start of voting, in clear and simple language, about: any steps a voter may have to take in order to participate and vote; the correct use and functioning of an e-voting system; the e-voting timetable, including all stages.	• For each electoral event the NSW Electoral Commission implements a comprehensive communication strategy to raise awareness and inform electors on all aspects of iVote
Transparency & observation	The components of the e-voting system shall be disclosed for verification and certification purposes.	• Critical software elements of the iVote system are available for independent review 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 • NSW Electoral Commission engages the services of an independent panel of experts to review and verify critical components of iVote • NSW Electoral Commission engages an independent auditor to report on critical aspects of the iVote project and the conduct of the iVote operations during an election • Formalised certification of iVote will be put in place as standards become agreed and stabilised
Transparency & observation	Any observer, to the extent permitted by law, shall be enabled to observe and comment on the e-elections, including the compilation of the results.	• NSW Electoral Commission allows appointed scrutineers, invited observers and auditors to observe the critical aspects of the iVote operations such sealing the electronic ballot box and the decryption of votes
Transparency & observation	Open standards shall be used to enable various technical components or services, possibly derived from a variety of sources, to inter-operate.	• See 8.8 for list of applicable standards

Heading	Standard	iVote
Accountability	Member States shall develop technical, evaluation and certification requirements and shall ascertain that they fully reflect the relevant legal and democratic principles. Member States shall keep the requirements up to date.	• ECANZ has developed and approved the eleven principles of an Internet voting system. • These have been mapped to the CoE recommendations • The Approved Procedures align with the requirements of the *Electoral Act 2017*
Accountability	Before an e-voting system is introduced and at appropriate intervals thereafter, and in particular after any significant changes are made to the system, an independent and competent body shall evaluate the compliance of the e-voting system and of any information and communication technology (ICT) component with the technical requirements. This may take the form of formal certification or other appropriate control.	• The NSW Electoral Commission has engaged an external auditor to test against the defined set of controls for iVote. • The NSW Electoral Commission has engaged an expert panel to provide review and comments on critical aspects of the project in addition to the external auditor. • The NSW Electoral Commission has developed a comprehensive test plan that covers all elements of the iVote systems including security readiness and penetration testing
Accountability	The certificate, or any other appropriate document issued, shall clearly identify the subject of evaluation and shall include safeguards to prevent its being secretly or inadvertently modified.	• The NSW Electoral Commission uses the services of an independent technical advisory group to review and advise on all aspects of the iVote systems • NSW Electoral Commission engages the services of an external auditor to develop a comprehensive audit and control plan
Accountability	The e-voting system shall be auditable. The audit system shall be open and comprehensive, and actively report on potential issues and threats.	• The iVote system maintains a comprehensive set of system logs and monitors all relevant system activities and configuration changes. • The logs do not capture information which will allow a vote's preferences to be explicitly associated with a given elector.
Reliability & security of the system	The electoral management body shall be responsible for the respect for and compliance with all requirements even in the case of failures and attacks. The electoral management body shall be responsible for the availability, reliability, usability and security of the e-voting system.	• The NSW Electoral Commission is solely responsible for operating all aspects of the iVote systems including ensuring the security and availability of all parts of the iVote systems including the infrastructure. • The NSW Electoral Commission has in place disaster recovery and security response plans

Heading	Standard	iVote
Reliability & security of the system	Only persons authorised by the electoral management body shall have access to the central infrastructure, the servers and the election data. Appointments of persons authorised to deal with e-voting shall be clearly regulated.	• Access to the infrastructure that runs the iVote systems will be strictly controlled and operates on the principles of separation of environments and least privilege user access
Reliability & security of the system	Before any e-election takes place, the electoral management body shall satisfy itself that the e-voting system is genuine and operates correctly.	• Prior to the start of voting, the NSW Electoral Commission conducts a Logic & Accuracy test on the live iVote system to verify the correct operation of the systems • Once the test is completed the live ballot box is 'sealed' ready to start taking votes • 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 • iVote has in place a configuration management regime that ensures the correct and approved versions of the iVote systems are deployed • iVote systems are constantly monitored to alert for any unauthorised changes
Reliability & security of the system	A procedure shall be established for regularly installing updated versions and corrections of all relevant software.	• Once iVote has been certified as ready the systems will be locked down and a change moratorium imposed. • During this period only critical changes can be made to the iVote systems • There will be strict change control processes and procedures in place • A patching policy will be part of the normal operation, although patching during lock down will be by exception • Updated versions of the voting software will be validated versions as advised by the supplier
Reliability & security of the system	If stored or communicated outside controlled environments, the votes shall be encrypted.	• The iVote voting system seals and encrypts the vote throughout its transmission from elector to ballot box.

Heading	Standard	iVote
		• All network packets are encrypted in transit
Reliability & security of the system	Votes and voter information shall be kept sealed until the counting process commences.	• Once iVote is live and for the duration of the voting period the votes cast are held encrypted within the iVote ballot box. • The ballot box can only be accessed following the close of voting – after 6pm on Election day
Reliability & security of the system	The electoral management body shall handle all cryptographic material securely.	• The iVote election keys are generated on an "air gapped" computer which is not connected to any network at any time • The generation of the election keys requires at least six members of an Electoral Board • The decryption of the votes requires a quorum of the electoral board as decided by the Electoral Commissioner • The decryption of the votes is undertaken on the same "air gapped" computer which has remained in a sealed container for the period of the election
Reliability & security of the system	Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment shall immediately inform the electoral management body.	• The NSW Electoral Commission operates all aspects of the iVote systems. In the case of issues during the conduct of an electoral event the iVote project team will escalate problems within the NSW Electoral Commission in accordance with the response plans
Reliability & security of the system	The authenticity, availability and integrity of the voters' registers and lists of candidates shall be maintained. The source of the data shall be authenticated. Provisions on data protection shall be respected.	• The electoral roll (*voters register*) is held within the Registration System and is loaded from the NSW Electoral Commission electoral roll system • Only members of the NSW Electoral Commission iVote team will have access to this system • The list of candidates is loaded from the nominations module of EMA once the nominations process is complete • NSW Electoral Commission is required to protect electors' personal information as required by the *Electoral Act 2017* and the *Privacy and Personal Information Protection Act 1998*

Heading	Standard	iVote
Reliability & security of the system	The e-voting system shall identify votes that are affected by an irregularity.	• The iVote systems maintain audit logs that will identify any problems or issues across the systems • During the decryption of the votes there is a process to verify the integrity of the ballot box and removing those votes that the NSW Electoral Commission identify as invalid e.g. electors who have also voted by another method

8.6 Global trends in electronic voting

As part of the iVote evaluation, we reviewed internet voting systems in other jurisdictions, in particular Switzerland, Estonia, France, Norway and Canada.

The experience of electronic voting in these countries has provided useful background and input into the iVote project for the 2019 State election as well as helping to frame our longer-term roadmap for iVote.

8.6.1 Switzerland

Switzerland has seen a gradual introduction of online voting since 2003, with small trials by the canton of Geneva followed by the municipalities of Neuchâtel and Zurich. Switzerland holds regular elections and referenda for all three levels of government with up to four elections held each year. Electronic voting is seen as a way to improve voter convenience and overall voter turnout. It is also important to note that "unsupervised" voting is commonplace in Switzerland with about 90% of all votes cast by post.

There are two different systems, one developed by government[63] (also known as the Geneva system) and the other developed and run by Swiss Post[64]. Both systems make use of return codes as a form of verification. Electors are sent, by mail, their personal voter's card that contains a unique code to access the system and series of random four-digit codes aligned to each candidate and referendum question. The elector logs onto the website with the unique code and cast their vote. When the votes have been received by the server it displays to the elector their voting choices along with a four-digit return code. The elector then checks the code displayed against the card that was mailed to them to confirm the system has processed the vote correctly[65,66,67]

8.6.2 Estonia

Estonia became the first country to use internet-based voting for government elections when they used it for the first time in 2005 for local government elections and it has since been used for all its local, parliamentary and European elections. All voters are permitted to use the Estonian I-vote system and the overall usage is relatively high (between 20% and 30% across all elections). All Estonians have a government electronic ID which is used to access all forms of Estonian government services and is also used in the casting of votes. The electronic ID has two PINs. The first is used to authenticate access to government services (eg to view health records). The second PIN is required if the citizen needs to digitally sign a government transaction (eg to submit a tax return).

To vote, the elector has to download and install the I-vote application on to their internet-connected device. They are required to present their electronic ID and enter their first PIN to authenticate themselves. After

[63] https://www.ge.ch/document/evoting-chvote/telecharger
[64] https://www.evoting.ch/en
[65] https://www.post.ch/-/media/post/evoting/dokumente/swiss-post-online-voting-protocol-explained.pdf?la=de
[66] https://www.ge.ch/document/evoting-chvote/telecharger
[67] https://www.coe.int/t/dgap/goodgovernance/activities/e-voting/evoting_documentation/passport_evoting2010.pdf

completing their ballot paper and submitting their vote, they are required to enter their second PIN which digitally signs the vote. The encrypted and signed vote is then submitted to the voting server. Once submitted the elector is presented with a QR verification code, which they can scan to undertake "cast as intended" verification.

8.6.3 France

In 2012, the French Parliament introduced 11 new seats representing French citizens living abroad. During the two-week election period, overseas electors could vote at either a limited number of overseas polling sites, by post or over the internet. More than 240,000 of the approximately 700,000 entitled voters cast an online vote.

Despite the successes of the 2012 election, the French government decided that internet voting would not be permitted for its parliamentary elections in 2017 following the advice of its information security agency ANSSI (Agence nationale de la sécurité des systèmes d'information), which believed there was an extremely high risk of cyber attacks.

8.6.4 Norway

Norway successfully implemented trails of internet voting at their 2011 local and the 2013 general elections. The trials were popular with the internet voting used in 10 to 15 municipalities with 26 per cent of the total votes cast in 2011, and between 33 per cent and 37 per cent in 2013. The system provided the "cast as intended/recorded as cast" verification using a system of return codes similar to those used in Switzerland. Norway largely discontinued internet voting in 2014, due to the lack of political consensus (the government that introduced the trials was defeated at the 2013 election).

8.6.5 Canada[68]

Canada has three levels of government – federal, provincial and municipal. Internet voting was first used in 2003 at the local government level in the provinces of Ontario and Nova Scotia. The number of municipalities offering internet voting has grown, with 97 of the 414 Ontario municipalities in 2014 and 23 of the 51 Nova Scotia municipalities in 2016 offering internet voting. There is no standardised approach governing internet voting nor the systems or protocols used, with each municipality tendering for the provision of its own systems.

8.6.6 Conclusion

Internet voting throughout the world covers the full range of elections from surveys and non-governmental elections[69] through to the various levels of government[70]. To successfully use internet voting for government elections, it is important that the electoral authorities operate all aspects of the voting channel. Components of an internet voting system may be provided by third-party suppliers, however, the electoral authority needs to have overall control and responsibility for the entire operation and conduct of the election.

[68]1. Online Voting: A Path Forward for Federal Elections, report prepared by Nicole Goodman, Director of the Centre for e-Democracy, for the Privy Council Office, Government of Canada
https://www.canada.ca/en/democratic-institutions/services/reports/online-voting-path-forward-federal-elections.html
2. The Patchwork of Internet Voting in Canada, Nicole Goodman Munk School of Global Affairs, University of Toronto & Jon H. Pammett, Department of Political Science, Carleton University, Ottawa
[69] Eg Shareholder, clubs and associations, board elections
[70] Municipal, state or regional, federal

8.7 Analysis of verification options

Table 5: An update to the analysis published with the iVote initiation brief[71]

Solution options	Advantages	Disadvantages	Comment	To be implemented for 2019
1 Cast as intended and Recorded as cast (Individual verification)				
	• Provides the means for the elector to be able to verify the vote. • Improves transparency and elector confidence in the system. • Protects against the effects of malware on voting device or man-in-the-middle attacks.	• Additional steps for the elector in the voting processes. • Potentially allows coercer or vote buyer to verify that vote was cast as instructed. • Implementations could unintentionally 'leak' elector preference information.	• Verification is important for election assurance. • Must not compromise ease of use for the elector and should be usable by electors with disabilities. • A study[72] concluded that coercion and vote buying are not significant risks in the Australian context, which needs to be taken into account when evaluating verification approaches.	• Yes
1.1 Cast as intended and Recorded as cast, protection against votes being cast from an insecure platform[73]				
Use a different device for voting and verification	• Both devices have to be compromised, which is less	• More complex for elector.	• Preferred approach but needs to address usability in the way implemented.	• Yes • For votes cast by

[71] https://www.elections.nsw.gov.au/NSWEC/media/NSWEC/Reports/iVote%20reports/iVote-Refresh-Project-initiation-brief-171117-(PDF-908kB).pdf
[72] https://www.elections.nsw.gov.au/NSWEC/media/NSWEC/Reports/Commissioned%20reports/Internet-voting-and-voter-interference-report-2013-(PDF-437kB).pdf
[73] Cannot prevent malware on a voter's device.

Solution options	Advantages	Disadvantages	Comment	To be implemented for 2019
	likely than one device being infected. • Different device could be a different channel, e.g. phone vs web • Since verification is offered immediately after the vote is cast more likely to get a high level of verification increasing assurance of the total votes cast	• Might be difficult to be sure elector does use a different device. • If abroad, access to a different device may be a barrier		iVote voting website
Use hardware token device	Isolated therefore relatively more resilient to compromise	• Not viable for the voting group: • Unlikely to be accessible for electors who are blind, have low vision or other disabilities. • Unlikely to be able to send token to electors outside of NSW especially electors who are overseas • High costs per elector • High overhead to manage & support logistics for large number of electors	• Not considered in the NSW context since the disadvantages significantly outweigh the advantages.	• No

Solution options	Advantages	Disadvantages	Comment	To be implemented for 2019
Use telephone verification (IVR)	• System understood and was used in 2011 • Different platforms for voting and verification therefore no chance of compromised verification platform • Accessible for electors who are blind, have low vision or other disabilities. • Provides a method of verification for electors who vote using the iVote telephone service	• Requires elector to enter 10 digit PIN and 8 digit iVoteID which can cause elector error to appear as verification failure • Requires the elector to verify after voting & therefore less likely to undertake verification • Low levels of elector verification does not provide the strong levels of assurance of the overall votes cast • Requires electors ballot paper to be decrypted on the IVR server which is not ideal as the server (or any intruder or suborned insider) knows the content of the vote when it is decrypted, so elector privacy could be compromised	• Will need to be used alongside other forms of verification.	• Yes • Only for votes cast by iVote telephone voting
1.2 Cast as intended and Recorded as cast, Decryption of vote				
	• Simpler for the elector as the vote cast is not obscured.	• Could be used as proof of vote to a coercer or vote buyer, however proving your vote in other voting channels is not easily prevented (e.g. taking a	• Prefer decrypting the vote for verification because ease of use is important and coercion risk is low.	• Yes

Solution options	Advantages	Disadvantages	Comment	To be implemented for 2019
		photo in the polling place) so not necessarily weakening the current state when compared against other voting channels		
1.2.1 Cast as intended and Recorded as cast, Decryption of vote, Location of decryption				
Server	• All processing is done on the server and the requirements on the client side are minimum.	• Decryption of the vote on the server could provide the means of an insider learning how a particular elector has voted. • If the server is compromised then the attacker could learn how to decrypt the entire ballot box	• Server-side decryption is not ideal. • If IVR verification is necessary for electors with a disability, then this is an implementation option.	• Yes • Only for votes cast using the iVote telephone service
Device	• Could increase the security by ensuring that the vote is decrypted on the elector's device and the server does not learn the key to decrypt.	• Requires the elector's device, which may not be secure, to be able to perform the decryption process.	• Decryption on elector's device is preferable to server-side decryption, assuming that usability is not significantly compromised. •	• Yes • Only for votes cast using the iVote website
1.2.2 Cast as intended and Recorded as cast, Decryption of vote, Key for decryption				

Solution options	Advantages	Disadvantages	Comment	To be implemented for 2019
Receipts	• Ease of use • Provides the means for the elector to be able to verify the vote. • Dependent on the design of the Voting Protocol it could be used to mislead coercer.	• If malware corrupts a voting session then it could also corrupt the receipt • Receipt could be obtained by a coercer or provided to a vote buyer as proof of vote	• The current iVote system uses a receipt number for vote decryption but other approaches are likely to offer improvements. (It also uses the receipt number for counted/tallied as recorded.)	• No
Token generated when vote encrypted (a receipt or otherwise) that can be used for verification - either for immediate use or can be saved.	• Generated and used on device at time of vote encryption. • Used immediately afterwards for verification • Not saved on device afterwards	• If malware corrupts a voting session then it could also corrupt delivery of the token, unless delivered to alternate device. • Token could be obtained by a coercer or provided to a vote buyer as proof of vote.	• Variations on the current receipt number approach may offer significant improvements and NSW Electoral Commission does not have a preferred approach, but is open to innovative proposals.	• Yes
Private key	• A digital certificate on elector's device (like digital Driver Licence) would be used to decrypt the vote and could be seamless for the elector.	• Delivery (prior to voting session) and security of the certificate would need to be resolved.	• Could offer the best solution but NSW Electoral Commission does not have a preferred approach and is open to innovative proposals. • Digital Transformation Office's Trusted Digital Identity efforts; might become the basis for a	• No

Solution options	Advantages	Disadvantages	Comment	To be implemented for 2019
			future voting certificate if successful	
1.3 Other forms of verification				
1.3.1 Use of Return Codes	• Allows verification on same device as used to vote by using a set of secret, unique 'return codes' for each elector. • Randomised codes for each elector allow vote preferences to be obscured during voting and verification to maintain secrecy of the vote. • Return codes allow mandatory verification as the system can enforce checking the codes as part of vote submission steps. • Has been used successfully in Norwegian and Swiss elections	• Preparation and distribution of personalised return codes may be high cost with significant risk of errors occurring. • More complex for electors to understand and potentially use especially if the elector has to enter a large number of preferences • Provision of the elector's unique codes to a coercer or vote buyer destroys any benefits to vote secrecy. • The 3 day time frame from candidates being finalised to start of voting to deliver codes via an alternative, safe channel may make this impossible.	• A suitable approach, though concerns over usability and elector understanding need to be addressed as well as secure delivery of return codes within available timeframe. This could be a good option for NSW if all concerns are addressed.	• No

Solution options	Advantages	Disadvantages	Comment	To be implemented for 2019
1.3.4 Trial Vote Credentials (To use for verification. The voting system cannot distinguish between actual and test votes)	• Allows elector to confirm system via a 'test vote' then make their actual vote. • Could be integrated with use of test votes prior to start of voting. • Test votes can be published on bulletin board.	• Potential confusion between test vote and real vote. • It is uncertain whether sufficient electors will bother to cast a test vote	• Extra effort and potential confusion, plus the likelihood that few electors will bother with a test vote mean this is not viewed as a suitable approach for electors. However, it could be an approach for operational testing (Logic and Accuracy) prior to go live.	• No
1.3.5 Cut-and-choose **An approach (generic 'Benaloh challenge[74]') whereby a vote can be tested (similar to with trial credentials) by the elector.**	• Here a elector can choose to test a vote after casting it. This verifies the vote was as cast, but then destroys the vote and the elector casts a new vote, which can also be tested or left as the submitted vote.	• Potential confusion to electors who might challenge and then not recast the vote. • Uncertain that many electors will bother to challenge a vote. • Limited protection for elector's insecure platform.	• Extra effort and potential confusion, plus the likelihood that few electors will bother to challenge a vote mean this is not viewed as a suitable approach.	• No
1.3.6 Encrypt vote a second time on a different device (Estonia 2013[75]) with vote	• No need to decrypt the vote for verification	• Accessibility issues. • Potential performance implications for NSW State	• As it stands, not suitable for a key cohort of iVote (voters with a disability) due to accessibility issues.	• No

[74] https://www.usenix.net/legacy/events/evt06/tech/full_papers/benaloh/benaloh.pdf
[75] http://www.vvk.ee/public/Verification_of_I-Votes.pdf

Solution options	Advantages	Disadvantages	Comment	To be implemented for 2019
encryption parameters sent via camera		General Elections with 300+ candidates below-the-line		
• **1.4 Other considerations**				
1.4.1 Mandatory or Optional Verification	• Mandatory verification theoretically ensures a higher degree of assurance for the election. • Optional allows the elector a simpler process, like paper voting, if they are not interested in verifying their vote.	• Mandatory forces electors to perform additional steps that are not part of paper voting. Additional mechanisms required to be able to debunk false claims of verification failure. • Optional may not achieve enough verifications to gain desired statistical confidence level. The profile of those that choose to verify is likely to represent those who are less likely to be affected by malware.	• Ideally, the objectives of assurance can be obtained without compromising usability for electors.	• Optional
• **2 Verification, Counted as recorded**				
	• Assurance that there was no tampering with the votes cast.	• Requires additional processes.	• Verification is important for election assurance	• Yes

Solution options	Advantages	Disadvantages	Comment	To be implemented for 2019
	• Reassures electors that votes were counted as cast.	• Complexity and cost of implementation.		
2.1 Mixing	• After mixing, no vote can be linked to the elector. • Increases trust in the vote secrecy of the system.	• Requires additional processing power. • Mixing process could corrupt or exclude valid votes.	• Stripping elector identifying information from votes without then mixing them is inadequate.	• Yes
2.1.1 Verifiable With Mathematical proofs	• Mathematically provable mix-nets exist that allow proof of the mixing with all votes being correctly emitted from the process.	• Need to ensure that the mixing performance is sufficient for the post-election timeline • Proof relies on specialised mathematical and cryptographic knowledge to confirm.	• Assurance of the mixing process is worthwhile, assuming it introduces no other significant risks or delays to the election results.	• Yes
2.2 Decryption proofs	• Mathematical proofs of correct decryption of votes can be achieved with certain cryptographic schemes.	• Computationally heavy for the large number of votes that NSW will process. • Proof relies on specialised mathematical and cryptographic knowledge to confirm.	• Assurance of the decryption process is worthwhile, assuming it introduces no other significant risks or delays to the election results or weakens vote secrecy protections.	• Yes

Solution options	Advantages	Disadvantages	Comment	To be implemented for 2019
2.3 Use of Bulletin Board (BB)	• Increases transparency and trust in the system through scrutiny. • Supports end-to-end verifiability.	• Increases the complexity and cost of implementation. • May expose election data to external attack. • Requires additional security implementations.	• Publishing the vote in the clear would allow a running count and is not permissible under NSW law. • Publishing other vote data is permissible and could enhance transparency and scrutiny of the system.	• Yes
2.3.1 Publish hash of encrypted vote	• The fingerprint of the vote can prove no subsequent tampering. • Content of the vote cannot be determined from the hash.	• Decryption of the vote for verification is separate from BB.	• A hash or similar derivative of the vote being saved on a public bulletin board could be a useful assurance measure for the system.	• Yes
2.3.2 Publish the encrypted vote	• Elector can verify the vote on the BB matches the vote cast. • The encrypted vote can prove no subsequent tampering.	• For the elector to verify the encrypted vote on the BB it must be stored with a connection to the elector. • Votes encrypted with current algorithms could be vulnerable to attack in the future and once all encrypted votes are published, not all copies can be destroyed after the election.	• The encrypted votes being saved on a public bulletin board could be a useful assurance measure for the system, but would need to be achieved in a way that doesn't compromise secrecy of the votes, either during the election or in subsequent years.	• No

Solution options	Advantages	Disadvantages	Comment	To be implemented for 2019
2.4 Vote comparison	• For the current iVote system, a comparison of votes to be counted with the votes in the verification system provides assurance that votes being counted match votes as cast. Means an attacker must synchronously corrupt both pools of votes, whilst avoiding detection of changes through elector verifications.	• Level of assurance depends on percentage of votes verified by electors. • Needs to be done in a way that prevents linking the decrypted vote with the elector.	• The current approach of comparing two separate pools of votes at the close of the election is a valuable assurance mechanism and a version of this may be a feature in future versions of iVote. (in the new system this is substituted by the comparison of Receipts)	• No
2.5 Post votes in the clear after the election with privacy preserving tracker id (e.g. Selene protocol[76])	• Allows verification after voting closes, which may improve assurance of the results.	• Verifying after the election closes means that nothing can be done by a elector who discovers their vote was corrupted by malware, however publishing the vote in the clear before voting closes would allow a running count and is not permissible under NSW law	• This might add value as part of a protocol that also allows elector verification before the close of voting, though it is unlikely that electors would adopt such a complex process.	• No

[76] https://eprint.iacr.org/2015/1105.pdf

8.8 List of standards

AS/NZS ISO 9001:2016 Quality management systems

AS/NZS ISO/IEC 27001:2015 Information technology - Security techniques - Information security management systems

Australian Government Information Security Manual (ISM)[77]

NSW Government Digital Information Security Policy (2015)

ISO/IEC 21827:2008 Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model (SSE-CMM) / CMMI

ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model

ISO/IEC 15408-2:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components

ISO/IEC 15408-3:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components

Secure Development Lifecycle (BSIMM/OpenSAMM)

Microsoft Security Development Lifecycle[78]

CERT Secure Coding[79]

Australian Government Information Security Manual (ISM)[80] - CONTROLS

NIST Computer Security Division's (CSD) Security Technology Group (STG Cryptographic Toolkit[81]

NIST Special Publication 800-38D, Nov-07, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC

NIST SP 800-44 Version 2, Sep-07, Guidelines on Securing Public Web Servers

NIST SP 800-57 Part 1, Jan-16, Recommendation for Key Management: Part 1: General (Revision 3)

NIST SP 800-57 Part 2, Aug-05, Recommendation for Key Management: Part 2: Best Practices for Key Management Organization

NIST SP 800-57 Part 3 Rev.1, Jan-15, Recommendation for Key Management, Part 3 Application-Specific Key Management Guidance

[77] http://www.asd.gov.au/infosec/ism/index.htm
[78] https://www.microsoft.com/en-us/SDL
[79] http://www.cert.org/secure-coding/
[80] http://www.asd.gov.au/infosec/ism/index.htm
[81] http://csrc.nist.gov/groups/ST/toolkit/index.html

NIST SP 800-63-3 Digital Identity Guidelines

NIST SP 800-63B (June 2017) Authentication and Lifecycle Management

NIST SP 800-63C Federation and Assertions

NIST SP 800-64 Rev. 2, Oct-08, Security Considerations in the System Development Life Cycle

NIST SP 800-67 Rev. 2, July 2017, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher

NIST SP 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators

NIST SP 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation

NIST SP 800-90C, Recommendation for Random Bit Generator (RBG) Constructions

NIST SP 800-131A Revision 1, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, November 2015,

NIST SP 800-133 Recommendation for Cryptographic Key Generation

FIPS 140-2, Security Requirements for Cryptographic Modules

FIPS 186-4: (2013): Digital Signature Standard (DSS)

FIPS 180-4: (2012): Secure Hash Standard (SHS)

FIPS 197: (2001): Advanced Encryption Standard (AES)

FIPS 198-1: (2008): The Keyed-Hash Message Authentication Code (HMAC)

FIPS 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions.

RSA Laboratories - Public-Key Cryptography Standards (PKCS)

9 Glossary

Term	Explanation
Approved procedures	The procedures approved by the Electoral Commissioner under section 155 of the *Electoral Act 2017*
By-election	An election held to fill a casual vacancy in the Legislative Assembly
Cast as intended verification	The method by which an elector can verify that iVote has correctly captured and stored their preferences
Completed virtual ballot paper	A virtual ballot paper containing the preferences as submitted by an elector on completion of the iVote voting process
Council of Europe	An international organisation whose stated aim is to uphold human rights, democracy and the rule of law in Europe.
Counted as recorded verification	The method by which an elector can check that their stored vote has been successfully included into the count
Credential hash	A unique number generated by combining the elector's iVote number and password\PIN and Salt using a hashing formula
Credentials	Information used to identify an individual accessing the system. In the iVote system, for an elector this includes a password or PIN known only to the elector and an iVote number generated by the system
Declaration vote	A vote cast by an elector where the elector is required to complete a declaration before they are able to vote. Declaration votes include postal votes, absent votes and enrolment votes
District	Geographical regions containing approximately equal numbers of electors. Each district is represented by one of the 93 members of the Legislative Assembly. The district for the Legislative Council is the whole state
Dual-tone multi-frequency signalling (DTMF)	A method used to issue commands over the telephone network
Document verification service (DVS)	A national online system that allows us to compare an elector's identifying information with a government record. The DVS is a secure system that operates 24/7 and matches key details contained on Australian-issued identifying credentials, providing a 'yes' or 'no' answer. The DVS provides greater confidence in the elector's identity
Early vote	Electors who cannot vote on election day can vote at an early voting centre. Eligible electors can also vote prior to election day using iVote or postal voting

Term	Explanation
Election Management Application (EMA)	A computer system developed by the NSW Electoral Commission to undertake administrative tasks including nominations, processing declaration votes and election results
Elector	A person who is entitled to vote at an election
Electoral Board	The body appointed by the Electoral Commissioner to control the iVote system encryption/decryption process
Electoral Commissioner	The Electoral Commissioner for NSW appointed under the *Electoral Act 2017*.
Eligible elector	An elector who meets any of the eligibility requirements for technology-assisted voting under section 152 of the *Electoral Act 2017*.
Electoral Council of Australia and New Zealand (ECANZ)	A forum where the Australian national, State and territory electoral commissions, and the New Zealand electoral commission, meet to discuss all aspects of electoral administration, encourage mutual cooperation, and consider contemporary electoral challenges aimed at improving access and equality for all eligible electors
Hashed password or PIN	The result of applying a one-way cryptographic hash function to a password or PIN, plus Salt. Only the hashed password or PIN is transferred between iVote systems
iVote system	The NSW Electoral Commission electronic voting system comprises the software components, hardware, networking, procedures and protocols required to deliver remote electronic voting services for eligible NSW electors
iVote ecosystem	The systems, infrastructure, process and procedures that together support the three functions of iVote: apply, vote and verify
iVote number	A unique eight-digit number for each elector who applies to use the iVote system
iVote receipt website	Allows electors to verify that their vote is stored correctly in iVote by searching for their iVote receipt
iVote telephone voting	Electors who need to use a telephone to cast their vote can use the iVote telephone voting system. This allows electors to log in and cast their vote using a telephone with DTMF.
iVote verification application	A smartphone app that the elector has to install onto their device to verify that iVote has correctly captured and stored their vote unaltered
iVote voting website	The interface the elector uses to cast their vote using iVote. The website is part of the iVote voting system

Term	Explanation
Joint Standing Committee on Electoral Matters (JSCEM)	A NSW joint parliamentary committee that conducts inquiries into, and reports on, electoral laws and practices and the spending and public funding of political parties
Legislative Assembly (LA)	The Lower House of the NSW Parliament. It has 93 members, with one elected member for each district
Legislative Council (LC)	The Upper House of the NSW Parliament. It has 42 members elected for an eight-year term, half (21) of whom are elected at each general election
Nomination(s)	The process by which a person is nominated to become a candidate for a State or local government election
Optional preferential (voting)	A voting system in which an elector numbers their preferences for individual or groups of candidates but need not show a preference for every candidate or group listed
Password	A password of at least 10 characters, as chosen by an eligible elector when applying to use iVote
Password dictionary attack	A dictionary attack is a method of breaking a password by systematically trying every word in a dictionary as a password
PIN	Personal identification number. This can only be numeric
Postal voting	A voting channel offered together with the iVote channel for electors who will be unable to attend at a voting centre on election day
Proportional representation computer count (PRCC)	A system used by the NSW Electoral Commission to calculate the results of each of the Legislative Assembly Districts as well as the Legislative Council
Recorded as cast verification	The method by which an elector can check that iVote has stored their vote and that it hasn't been changed once stored
Recovery point objective (RPO)	The NSW Electoral Commission's iVote data and loss tolerance. RPO is determined by looking at the time between data backups and the amount of data that could be lost in between backups
Recovery time objective (RTO)	The target time for the recovery of iVote if a disaster occurs
Salt	A secret number combined with the password or PIN and iVote number to make breaking the Credential Hash difficult using brute force approaches.
Silent elector	An elector who has satisfied the Electoral Commissioner that their residential address should be omitted from any authorised roll or list of electors on the grounds that having that address on a roll or

Term	Explanation
	list of electors places or would place the personal safety of the person or of members of the person's family at risk.
SmartRoll person ID (SPID)	A unique voter electoral identifier (held in the electoral roll)
Technology assisted voting (TAV)	A method of voting where an eligible elector votes by means of an electronic device (whether networked or not), such as by a telephone or by a computer
Two candidate preferred count (TCP)	Before election day, the NSW Electoral Commission selects the two candidates in each electoral district who are likely to be the eventual two remaining candidates in the count for that district. This is done to give candidates, registered political parties and the media, an indication of the potential election outcome
Virtual ballot box (VBB) or electronic ballot box	A data base corresponding to a physical ballot box in which the votes cast using iVote are accumulated
Virtual ballot paper (VBP)	A blank or empty electronic ballot paper unique to each application by an elector which is associated with their credential hash and available in the iVote voting system for electors to cast their vote
Voluntary Voting System Guidelines (VVSG)	Guidelines developed by the US Assistance Commission to provide a set of specifications and requirements against which voting systems can be tested.
Voting centre	A venue appointed by the Electoral Commission for the purpose of taking ‘in person’ votes
Voting channel	A voting channel is method which electors can choose to cast their vote. During elections, the NSW Electoral Commission will provide multiple voting channels, for example, postal voting, early voting, absent voting and iVote
Voting protocol	All the steps and controls that are in place to enable an elector to correctly cast their vote. Protocols often describe the interactions between systems as part of the voting process