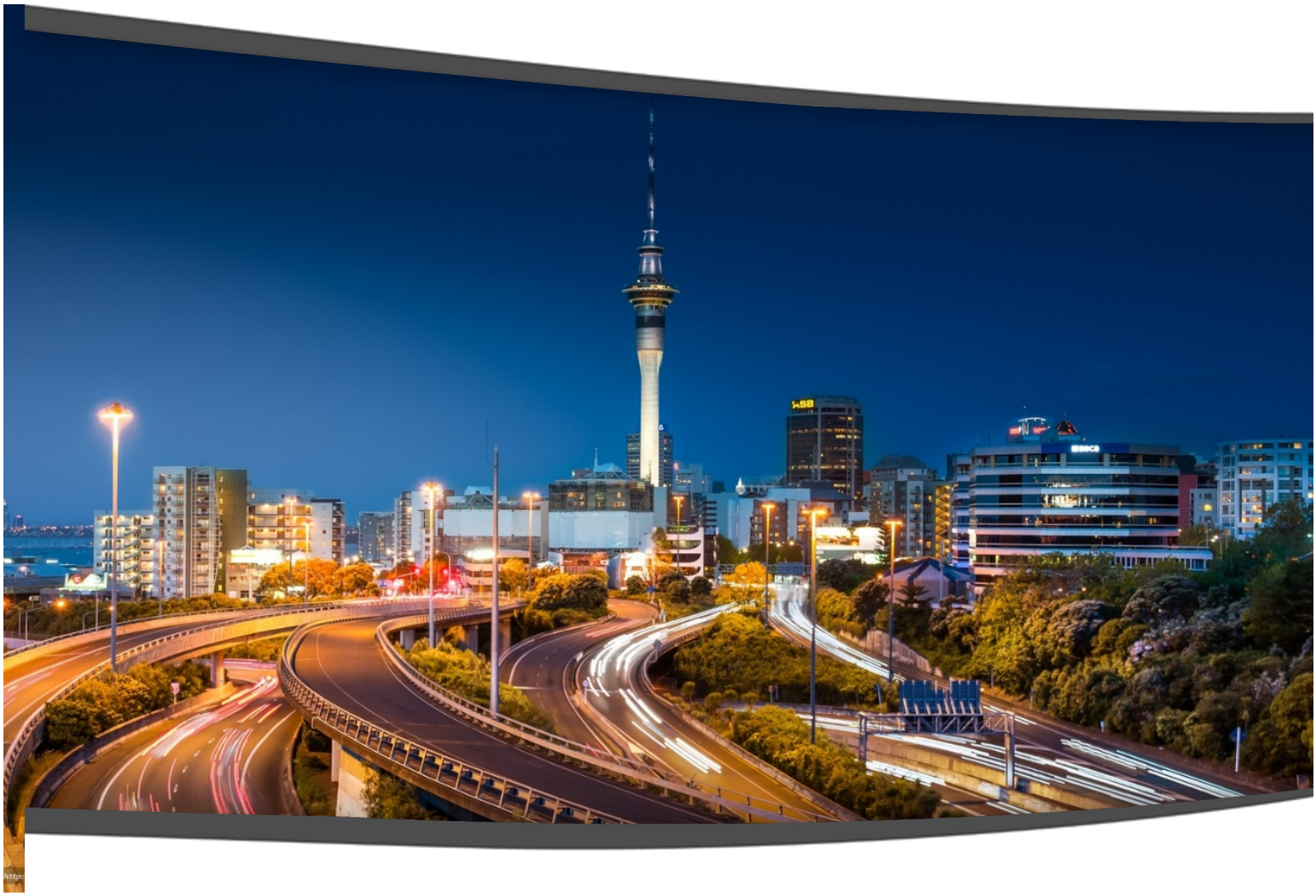

Submission to:

The NSW Electoral Commission for Call for submissions: Report on the iVote system.

Table of Contents

1 Executive Summary

Smartmatic Australia welcomes this opportunity to provide this submission to the NSW Electoral Commission for **Call for submissions: Report on the iVote system.**

Smartmatic is a multinational company that designs and deploys technological solutions aimed at helping governments fulfil, in the most efficient way, their commitments with their citizens. It is the largest cutting-edge technology supplier to Election Commissions (ECs) and Electoral Management Bodies (EMBs), with a wide and proven experience in the United States, Asia, Africa, Europe, Latin America and the Caribbean.

Online voting has evolved over the past 10 years from science-fiction to **viable** option for governments seeking to **enfranchise their citizens** in the democratic decision-making processes, regardless of where they are located.

Several governments around the globe, including Estonia, Switzerland, Norway, Australia and Canada to name a few, have either implemented or 'piloted' forms of online voting. Modern online voting methods differ significantly from traditional paper based voting, but in coalition with traditional voting methods still support the same underlying key democratic principles: **universal suffrage, free suffrage, equal suffrage and secret ballot.**

The idea of online voting initially seems to be a straightforward application of Internet based technologies and practices into the field of elections. Providing online voting should not be harder than setting up a database system with a web front-end. At the very least, it should not be harder than running an Internet banking system.

Elections demand voting methods to accurately gather preferences of those eligible to vote and to produce an accepted voting result according to these preferences. The nature of the voting method defines how the preferences are gathered.

In the context of online voting, a combination of technological, procedural and organizational structures and protocols need to be aligned to successfully carry out the following core functions:

- Voter authorization – the operation of permitting access only to eligible voters; Voting – the process of marking and casting a ballot in accordance with the voters' preferences;
- Recording of the votes – the process of recording the cast vote;
- Storing votes for tally – the process of storing the cast votes after casting and before tallying;
- Tabulation of the voting result – the process of producing the correct result by tabulating valid, cast ballots in accordance with the election rules.

Huge strides in technical, operational, security aspects and auditability in the above areas are occurring every year.

To help EMB's with their challenge of having to deal with an increasingly mobile and dispersed electorate, increase participation rates and election credibility, online voting is the most effective method. It brings the ballot to the voter.

We believe that online voting should be one of the many channels available for voters to submit their voted ballots in a convenient and secure way. A robust voting system should comprise:

1. In-person voting, when voters are expected to show up at a special location to cast their ballots. This may take place in an electronic voting machine or on paper ballots that can be counted electronically.
2. Remote voting, when voters are allowed to cast their ballot from anywhere in the country or around the globe using a secure Internet voting platform.

With respect to the terms of reference, we have made a number of recommendations as part of this submission.

These include technical and architectural recommendations that we believe will need to be implemented to guarantee the security aspects of the iVote network into the future and also Legislative changes, which would allow all voters in NSW the ability to engage and vote online as an option.

2 Internet voting has passed the test

Internet voting has been in operations in other jurisdictions such for over 10 years.

The Estonian i-voting solution is the longest-standing, most technologically advanced, and highly trusted internet voting solution in existence. It has been used to support every binding, governmental election held since 2005. Such is the level of public trust in the system that nearly a third of all Estonian ballots are cast online. The 186,034 i-voters who used the system in the recent local elections (October 2017), represent an increase of 39% more votes since the previous local elections in 2013, and reaffirm the continued adoption of i-voting in Estonia.

Estonia Elections 2005 – 2017 Achievements:

- Used in 9 consecutive national elections
- 32% of the voters cast their ballot online
- 12% of i-voters used mobile phones to authenticate themselves
- 60% of advance voting was done online
- Enfranchised Estonians in 116 countries
- Overall turnout has risen since the introduction of i-voting,
- Universal digital verification

Election	LOCAL 2005	PARLIAMENT 2007	EU PARLIAMENT 2009	LOCAL 2009	PARLIAMENT 2011	LOCAL 2013	EU PARLIAMENT 2014	PARLIAMENT 2015	LOCAL 2017
Electorate size	1,059,292	897,243	909,628	1,094,317	913,346	1,086,935	902,873	899,793	1,100,647
Number of voters	502,504	555,463	399,181	662,813	580,264	630,050	329,766	577,910	586,519
Participation rate	**47%**	**62%**	**44%**	**61%**	**64%**	**58%**	**37%**	**64%**	**53%**
Number of online voters	9,317	30,275	58,669	104,413	140,846	133,808	103,151	176,491	186,034
Number of voters who voted online and in polling station	30	32	55	100	82	146	46	162	163
Number of unrevoked online ballots	9,287	30,243	58,614	104,313	140,764	133,662	103,105	176,329	185,871
Recast online ballots	364	789	910	2,373	4,384	3,045	2,019	4,593	4,527
Share of online voters to all voters	**1,9%**	**5,5%**	**14,7%**	**15,8%**	**24,3%**	**21,2%**	**31,3%**	**30,5%**	**31,7%**
Share of online voters to all early votes	7,2%	17,6%	45,4%	0.44	56,4%	50,5%	59,2%	59,6%	60,6%
Share of online votes cast abroad	–	2%	3%	2,8%	3,9%	4,2%	4,7%	5,7%	4,1%
Number of countries voted from using online voting		51	66	82	105	105	98	116	115
Length of online voting period (days)	3	3	7	7	7	7	7	7	7
Number of online voters using mobile ID	–	–	–	–	2 690	11 753	11 609	22 084	44 211
Share of online voters using mobile ID	–	–	–	–	1,9%	8,6%	11,0%	12,2%	23,8%
Share of votes verified using independent verification application	–	–	–	–	–	3,4%	4,0%	4,3%	4,0%

Verified votes - Individually verifiable online voting schemes provide voters with tools to verify that their votes were cast as intended and that they were correctly accepted by the voting system.

As you can see from the table above, there are several key trends that online voting has enables after continual use within a country.

- Participation rates have increased year on year, indicating that online voting technology helps the voter engage and connect with the elections.
- The share of votes being received online also has increased exponentially.

3 Whether the security of the iVote system is appropriate and sufficient?

No cyber defence or information system can be regarded as 100 % secure. What is deemed safe today won't be tomorrow given the lucrative nature of cybercrime and the criminal's ingenuity to seek new methods of attack.

Online voting needs to ensure ballot secrecy. It is essential that during all stages of the election process, the vote contents remain secret and are protected from disclosure. Through the entire process it is essential that **no stakeholder can tell how a voter voted.**

Online voting must provide an accurate voting method, which captures the intent of the voter and protects the vote preferences from being tampered with (altered), deleted, and prevents bogus (ineligible) votes from being added. This is **critical to ensuring election integrity and creating trust** in the system.

We recommend that iVote implement two additional main technologies, which protect the integrity of the digital ballot box and individual votes kept inside;

1. Blockchain-based digital time stamping.
2. Minimising the use of external dependencies and services

3.1 Blockchain-based digital time stamping

Today if an attacker gains access to a blockchain network and the data, this does not necessarily mean the attacker can read or retrieve the information. Full encryption of the data blocks can be applied to data being transacted, effectively guaranteeing its confidentiality, considering the latest encryption standards are followed. The use of end-to-end encryption, where only those who have authorization to access the encrypted data i.e. through their private key, can decrypt and see the data. Using encryption keys in conjunction with PKI will provide NSWEC with a higher level of security.

Blockchains improve cyber defence as the platform can secure, prevent fraudulent activities through consensus mechanisms, and detect data tampering based on its underlying characteristics of immutability, transparency, auditability, data encryption & operational resilience (including no single point of failure).

Blockchain-based digital time stamping is a method of proving in an irrevocable manner that certain data existed at a given time point.

Online voting protocols, which utilize this, commit a cryptographic 'fingerprint' of every vote to an external time stamping service and receive a cryptographic timestamp in return. The timestamp is both stored and given to the voter. It can be used to verify that the vote was accepted to the voting system. Based on the timestamps it is later possible to verify, in cooperation of the voting system and time stamping service, that no votes were altered or removed from the system.

Digital signatures prevent vote alteration and ballot-box stuffing. Blockchain-based digital time stamping prevents vote alteration and deletion of the votes from storage. The cryptographic scheme ensures that it is possible to verify that the votes sent for tabulation were exactly the votes sent by the voters to ballot box.

3.2 Minimising the use of external dependencies and services

The security of online voting system requires that any potential attack vector be minimised. This, however, may be hard to control if system components or services are used, which have not been developed for the specific purposes of online voting or, are developed by vendors who do not/ cannot provide access to source code for review and / or certification, or services are used which reside outside the core i-voting infrastructure.

In this respect we strongly advocate minimising reliance on third party systems (including databases) and to ensure strict input validation on any external interfaces

4 Whether the transparency and provisions for auditing the iVote system are appropriate

4.1 Observing online voting

We believe that there can never be enough transparency in any election or any government process. The dilemma is – how do you provide complete transparency without compromising the security of the network or opening it up to cyber attack or manipulation?

Where human observation plays a large role in the trustworthiness of traditional paper-based voting methods. The remote nature of online voting is inherently unobservable by traditional means and therefore requires alternative techniques to verify the correct operation of the election protocol.

It is impossible to determine the incorrect operation of a computer system solely by the observation of the procedure. **Verifiable online voting schemes** make it possible to assure the stakeholders that the election has been performed correctly.

Individually verifiable online voting schemes provide voters with tools to verify that their votes were **cast as intended** and that they were correctly accepted by the voting system.

Auditable online voting schemes provide auditors with tools to verify that all accepted votes were **tabulated correctly.**

Auditing combined with individual voter verification provide effective observation techniques for online voting, which help improve transparency and enhance trust in the system.

4.2 Auditing

Online voting must provide an accurate voting method, which captures the intent of the voter and protects the vote preferences from being tampered with (altered), deleted, and prevents bogus (ineligible) votes from being added. This is critical to ensuring election integrity and creating trust in the system.

It is important for any organisation to have an audit trail to verify results. This will include a number of elements both technical and operational. The current iVote system obviously has a broad range of measures in this area.

We would recommend that the use of Blockchain would significantly improve the auditing capabilities of the iVote solution in the following areas.

- Time-stamping stored votes using blockchain
- Zero-knowledge cryptographic proofs of mixing
- Zero-knowledge cryptographic proofs of decryption
- End to end verifiable - Every vote can be irrefutably traced to its source without sacrificing a **voter's vote anonymity.** End to end verifiable voting systems will give the voter the ability to verify if their vote is correctly recorded and correctly counted, for instance, if a ballot is missing, in transit or modified, it can even be detected by the voter and caught before the election is over.

4.3 Source code

Should the source code open for review by independent authorities?

Disclose the source code to approved independent authorities to audit the solution to ensure that it complies the highest levels of security and accuracy.

We strongly advocate the use of third party independent authorities as a mechanism of enhancing public trust in any automated election.

4.4 4.4 Formal verification of protocol

We strongly advocate the formal review and verification of the chosen online voting protocol. At Smartmatic we seek to engage with expert academics to validate our design decision and in particular the cryptographic protocols which underpin our online voting technologies. Not only can this be used to identify any potential weaknesses or vulnerabilities, but the public, peer-reviewed forum of openness can be used to foster additional trust in the system by validating its integrity.

5 Whether adequate opportunity for scrutineering of the iVote system is provided to candidates and political parties.

To provide the opportunity for the candidates and parties, the implementation, data structures and procedures must be well documented. To ease implementing independent auditing software, reference implementations should be made public.

6 What improvements to the iVote system would be appropriate before its use at the 2019 State General Election?

As with any technology and any market, this is an evolving area. The answer today will not be the same as the answer tomorrow or the answer 12 months ago. It is important to continuously improve and stay ahead of any possible threats.

At a high level, we believe that the iVote network should strive to drive continuous improvements in the following key areas.

6.1 Recommendation 1) Improved protection against TLS vulnerabilities

iVote should enforce the use of the strongest, most up to date version TLS protocols to eliminate the risk of TLS/SSL downgrade attacks.

6.2 Recommendation 2) Improved protection against Distributed Denial of-service (DDoS) attacks

iVote should deploy a range of provisions to ensure the highest availability and minimise the risk of service outage by Distributed Denial of service (DDoS) attacks.

These would include:

- Load balancing (Network, DNS and applications levels) to ensure efficient uses of available service resources.
- Horizontal scalability to seamlessly add new servers if the monitoring detects an overload of existing services.
- Vertical scalability to add additional processing performance to existing services
- Distributed storage to ensure ballot box integrity and availability.
- Extensive benchmarking to understand and model exact thresholds for service degradation and failure and appropriate resource modelling.
- Network level routing restrictions in collaboration with ISP's to define rules for handling network traffic.
- Third party prevention services (where applicable and controllable)

In addition, extending the online voting period for a number of days limits the potential affects of a successful DDOS attack by allowing voters to try voting again at a different time in the unlikely event of a DDoS outage.

6.3 Recommendation 3) Improved security and traceability

There are two main technologies, already discussed, which protect the integrity of the digital ballot box and individual votes kept inside;

1. Blockchain-based digital time stamping
2. Minimising the use of external dependencies and services

It can be argued that Blockchain technology will become the biggest enabler in the adoption and credibility of online voting systems globally.

It provides a solution for all of the characteristics you would want in a platform that is arguably the most important part of a democratic society;

- It is absolutely fault-tolerant,
- You cannot change any events in the past,
- You cannot hack the present and manipulate results,
- You cannot alter the access to the system,
- Every node with access can see the exact same results, and
- End to end verifiable

6.4 Recommendation 4) Improved scrutiny – Open Source code

Should the source code open for review by independent authorities?

Disclose the source code to approved independent authorities to audit the solution to ensure that it complies the highest levels of security and accuracy.

We strongly advocate the use of third party independent authorities as a mechanism of enhancing public trust in any automated election.

6.5 Recommendation 5) Offer universal, legally binding Internet voting as an option to all voters.

Engage your voters, engage your youth.

Citizens are becoming more mobile in term of their lifestyles, there are increasing pressures on governments and Election Management Bodies (EMB's) to offer improved methods to allow voters to vote remotely, thereby effectively bringing the ballot to the voter rather than relying on the voter to travel to a specific voting location.

We do not see online voting as the only answer but as a one of the options available to the voter. Online voting should be one of the many channels available for voters to submit their voted ballots in a convenient and secure way.

A robust voting system should comprise:

- In-person voting, when voters are expected to show up at a special location to cast their ballots. This may take place in an electronic voting machine or on paper ballots that can be counted electronically.
- Remote voting, when voters are allowed to cast their ballot from anywhere in the country or around the globe using a secure Internet voting platform.

We would recommend that legislation is changed ate that all voters would be eligible for voting online in 2019.