TIVI Online Voting
Frequently Asked Questions

TIVI Powered by SMARTMATIC CYBERNETICA

How can I be sure that only eligible voters can cast their ballots?

Our online voting solution has been designed to support a variety of strong authentication methods, which only permit eligible voters to access the system and successfully cast their ballot.

Strong authentication methods include the use of multi-factor schemes (using out-of-band mobile phone verification) and can include biometric validation and or/integration with existing government authentication services to tightly control access and ensure that only eligible permitted voters can cast their ballots.

How do I securely cast my vote?

TIVI ensures the secure casting of ballots and maintains voter privacy and integrity at all times. Security is provided by means of multiple levels of physical, logical and procedural protection.

Ballot secrecy is protected by means of strong 'end-to-end' encryption and vote integrity is ensured through digital signatures and digital time stamping of votes.

By providing end-to-end encryption, digital signing along with secure transmission the system provides the strongest assurance of any internet voting solution globally, that votes cannot be intercepted, read or tampered (changed, deleted) and that absolute privacy and anonymity is maintained.

TIVI is the only online solution in the world that allows 100% universal digital verifiability to prove the integrity of the vote, from the point of casting to counting (cast as intended, stored as cast, counted as cast). It is the most technically advanced solution in terms of addressing security, secrecy and vote anonymity

How does the system maintain voter privacy?

Our online voting system is engineered to provide 100% voter privacy at every stage of the election process and at no stage can voter preferences ever be correlated with a voters' identity.

Our solution features a cryptographic "mixing" process, which decouples the voters identifying information from the still fully encrypted votes.

The anonymised encrypted votes are then taken to a 'clean', air-gapped decryption server which has never been connected to the internet where they are decrypted using a secret key-sharing process by a quorum of approved members of the electoral board.

The system features a secret-key sharing scheme that means that no single individual can decrypt and therefore delete, add or tamper with votes in the digital ballot box. The private key (used to decrypt the election) can only be formed by a collaborative process, in which the members of the electoral board combine their secret shares to recreate the private key.

There have been several large-scale SSL attacks/ compromises recently – How does the solution protect against SSL vulnerabilities?

Because we advocate the use specific voting applications (which are 'certified' by the relevant electoral body) rather than a standard web browser we can tightly control the implementation of 'transport layer security' (TLS) to only use the most up-to-date and secure version.

We therefore do not use older, often less secure SSL implementations, which have historically been vulnerable to well-documented, recent SSL attacks such as 'Heart bleed' or 'Poodle'.

In addition, we continuously update all software implementations to ensure that we mitigate the exposure to new software vulnerabilities and provide our customers with the absolute confidence and an assurance that our solution complies with the highest security standards.

If internet banking systems can be compromised, how can you guarantee the security of internet voting?

Both internet voting and internet banking are examples of useful and convenient e-services which have specific and high security requirements.

Anybody providing these services has to use a system designed to achieve these requirements, otherwise undesirable consequences arise - in case of internet banking somebody loses money, in case of internet voting the election result can be tampered with or the voter privacy is lost.

The underlying security problems for internet banking and internet voting are fundamentally different. In internet banking, both the bank and the customer can see all the transactions and charges on the account. In the case of internet voting the aim is to provide the correct aggregated voting result without revealing the choices of individual voters.

The challenges of internet voting can be effectively solved but require additional technologies and processes which offer a level of security and auditability (verifiability) which is far in excess of that required by online banking. We have defined the security requirements for such a system and we have rigorously designed a protocol to achieve these requirements.

We deal with issues such as ballot secrecy, vote integrity, safeguards against manipulations and man in the middle attacks by applying application level security measures on top of widely adopted internet security practices. Such additional measures are not typically seen in internet banking applications.

Our protocol is voter verifiable, enabling the voter to prove that their vote was cast correctly. All server-side operations can be audited by third parties, to ensure that the votes are correctly handled in the tabulation process.

How is internet voting protected against denial-of-service (DoS) attacks that slow down the servers, so voters can't vote and the entire process must either be delayed or cancelled.

Denial of service (DoS) is a real threat that all web based systems need to consider in their design and architecture. However, there are new and sophisticated means to avoid denial of service attacks on computer systems and mitigate their impact. Extending the voting period for a number of days allows voters to try again at a different time in the unlikely event of a DoS outage. In Estonia, where online voting has been a success, internet voting is one of the options Estonians have to cast a ballot in advance. Voters can also cast their ballots by post prior to election day and also at designated polling stations.

It is important to note that denial of services is not an endemic vulnerability of digital world. In a broad sense, a worker strike in a foreign country can prevent a citizen to cast a ballot from arriving to its location on time.

Home computers are often infected with malware and are prone to hackers and cyber-attacks. How can I avoid this affecting my vote?

We apply tested and proven risk management and security testing processes in each election we undertake to ensure that we offer the highest level of security as the internet voting threat models change and evolve.

Malware is a common manifestation of the internet and vulnerabilities associated with client side malware are arguably the hardest security risk to mitigate. With this in mind, we have designed TIVI to strongly protect the security and privacy of the voting experience against eavesdropping and/or vote manipulating malware, but to still assume that the voters' computer may feature a malware infection. With this assumption the voter needs to have the ability to perform the following:

1) Vote in an environment which protects against malware infection
2) Detect the unlikely presence of vote tampering malware
3) Take remedial action in the unlikely event of a tampered vote

Voting in an environment which protects against malware infection

The overwhelming majority of malware infections can be detected and resolved by running up-to-date antivirus/malware software. As part of the voter outreach and communicate we strongly recommend that voters practice good internet/computer 'hygiene' and keep antivirus software up to date.

Detecting the unlikely presence of vote tampering malware

This is achieved by offering voter verifiability. TIVI allows voters to verify the contents of the cast vote using a separate device to the one they voted on. This is typically achieved through the use of a smartphone application which allows the voter to prove that the contents of their cast vote has not been altered. It would be virtually impossible to engineer a coordinated malware attack against the voters voting computer and smartphone given that there is no physical/logical connection between the two devices.

How can I be sure that no one can change my vote?

Our internet voting protocol is designed to guarantee the integrity of the vote throughout the process – from the point of casting until the point of tabulation.

The voter can use the verification application to make sure that the vote was sent to the system as intended. The server maintains a third-party verifiable audit trail for all votes, and is capable of proving up to the point of tabulation that all the votes were correctly handled according the rules.

This type of auditability together with cryptographic signatures eliminates all vote tampering possibilities, and provides a universal assurance that voter preferences will be captured, stored and tallied as the voter intended.

The implementation of a Blockchain based bulletin board provides additional proof of the integrity of all cast ballots, showing that no ballot preferences have been changed, no valid votes deleted or bogus votes inserted.

What safeguards does the system have to protect vote deletion or tampering by system administrators?

Our internet voting protocol is designed to guarantee the integrity of the vote throughout the process – from the point of casting until the point of tabulation.

The server maintains a third-party verifiable audit trail about the vote and is capable of proving up to the point of tabulation that all the votes were correctly handled according to the rules. This type of auditability together with cryptographic signatures excludes the tampering possibilities also by system administrators.

As mentioned previously, the system features a secret-key sharing scheme that means that no single individual can decrypt and therefore delete, add or tamper with votes in the digital ballot box.

The private key (used to decrypt the election) can only be formed by a collaborative process, in which the members of the electoral board combine their secret shares to recreate the private key.

In addition, the system features digital time stamping and daisy chaining of votes along with immutable system logs which mitigate against the insertion of bogus votes or the deletion of valid votes.

Surely online voting is a “black box” system – How do you support the principle of electoral transparency within internet voting?

Our solution features a unique auditability layer which despite the highest levels of security, offers ‘universal verifiability’ and the ability for stakeholders to audit the entire solution and end-to-end process. In particular, this includes tools to verify that votes were ‘recorded as cast, stored as cast and counted as intended’.

Not only do we provide a simple to use toolset for auditors, but also we provide a unique API, which enables any stakeholder to use their own audit/verification tools.

In addition, we fully disclose the system source code to official auditors to offer a level of transparency, which exceeds that of traditional paper based elections.

Is the source code open for review by independent authorities?

Yes – We 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.

How does the system protect against voter coercion?

Remote voting outside of a controlled environment offers a different set of challenges. One of these is potential voter coercion. However, our solution mitigates this risk by offering the voter the opportunity to ‘re-vote’ or re-cast their ballot as many times as they wish.

The system still maintains the principle of ‘one voter, one vote’ and any previously cast ballots are discarded in favour of the last cast vote.

In this respect, if a voter is coerced into voting a certain way, they can access the system at a later time and re-vote in a coercion free environment.

Has the solution ever experienced any security breaches?

No – The solution has been used for eight nationwide elections in ten years in Estonia. At no time has there ever been a single documented security breach.

We apply tested and proven risk management and security testing processes in each election we undertake to ensure that this record is maintained and that we continue to offer the highest level of security as the internet voting threat models change and evolve.

Surely online voting is only appealing to younger, technologically savvy voters?

More and more citizens today engage using the internet on digital devices in all age groups and demographics.

In Estonia, the age group of 55+ are the largest users of internet voting constituting around 25% of all Internet voters. Internet voting offers greater accessibility for voters with disabilities and our solution has been designed to support the highest accessibility standards including the use of screen readers (such as JAWS, NVDA) and accessible hardware devices such as switches, paddles and ‘sip & puff’ tubes.

In this respect, we see internet voting as a solution, which appeals to voters of all ages and demographics not simply to younger technology aware voters.

Does Internet voting increase participation/ turnout?

Online voting offers a convenient and simple platform to bring the ballot to the voter in a more accessible and secure way than other remote voting methods (postal voting).

The following empirical evidence of increased turnout from online voting in USA, Estonia and Australia is presented below:

USA

The introduction of electronic means for remote voting UOCAVA voters (Uniformed and Overseas Citizens Absentee Voting Act) in various US jurisdictions resulted in significant improvements in turnout.

- In Cook County (one of the largest electoral jurisdictions in the US), the provision of online voting for Uniformed and Overseas Citizens increased turnout from 11% to 53% after the introduction of Internet voting in 2012. Also in Cook County, overall accuracy increased, going from 92% of ballots counted in 2008 to 99% in 2012.
- In the 2010 Primary, General and Special elections in West Virginia, absentee ballot return rates increased from 58% to 92.5%.

Estonia

In the case of Estonia, several studies have provided evidence that as many as 10% of Internet voters would not have voted if they hadn't had the internet as a voting channel (which results in an approximate 2.5% increase in turnout).

Australia
In the New South Wales State Elections in 2011, online voting (iVote) was made available for voters with disabilities and those who lived more than 20km away from the polling stations.
The post election report summarized that “usage of iVote greatly exceeded expectations by three-fold with almost 50,000 electors using it. We estimate that access to iVote enfranchised around 30,000 electors who were unlikely to vote had iVote not been available”.

Switzerland
For many years now, various Cantons in Switzerland have used on-line voting to support their own particular form of representative democracy, using on-line voting methods to supplement polling based voting in referenda.
In this respect, we believe that online voting if implemented correctly, in conjunction with a robust voter education initiative, is able to have a marked positive effect on voter turnout.

Surely online voting is more expensive that paper voting?

It is actually possible to reduce the overall cost of elections through the use of internet voting. With an online voting system, the number of polling stations can be radically reduced and the requirement to print ballot papers and postal votes can also be reduced. Electronic poll cards delivered through email or SMS can offer additional cost savings.

Counting ballots electronically would also reduce the need to hiring count centres to count ballots, eliminate transport and other logistical costs associated with the transfer of ballot boxes to central count venues. Staffing costs would also be dramatically reduced to deliver additional cost savings.

There exists the misconception that online voting is costlier than postal voting because of the cost of technology. While some internet voting experiments have been very costly (such as the case of Norway), the best enduring example in the world of internet voting is the case of Estonia, a system that has remained in operation for almost 10 years.

Even after going through two generations of the system in 8 national elections over the past 10 years, the government of Estonia has spent less on internet voting than on the provision of postal voting.
In this regard, with the appropriate solution, efficient procurement process and long term vision and commitment, online voting offers governments the opportunity to radically reduce the cost of elections as well as delivering the previously described benefits.

tivi.io
hello@tivi.io