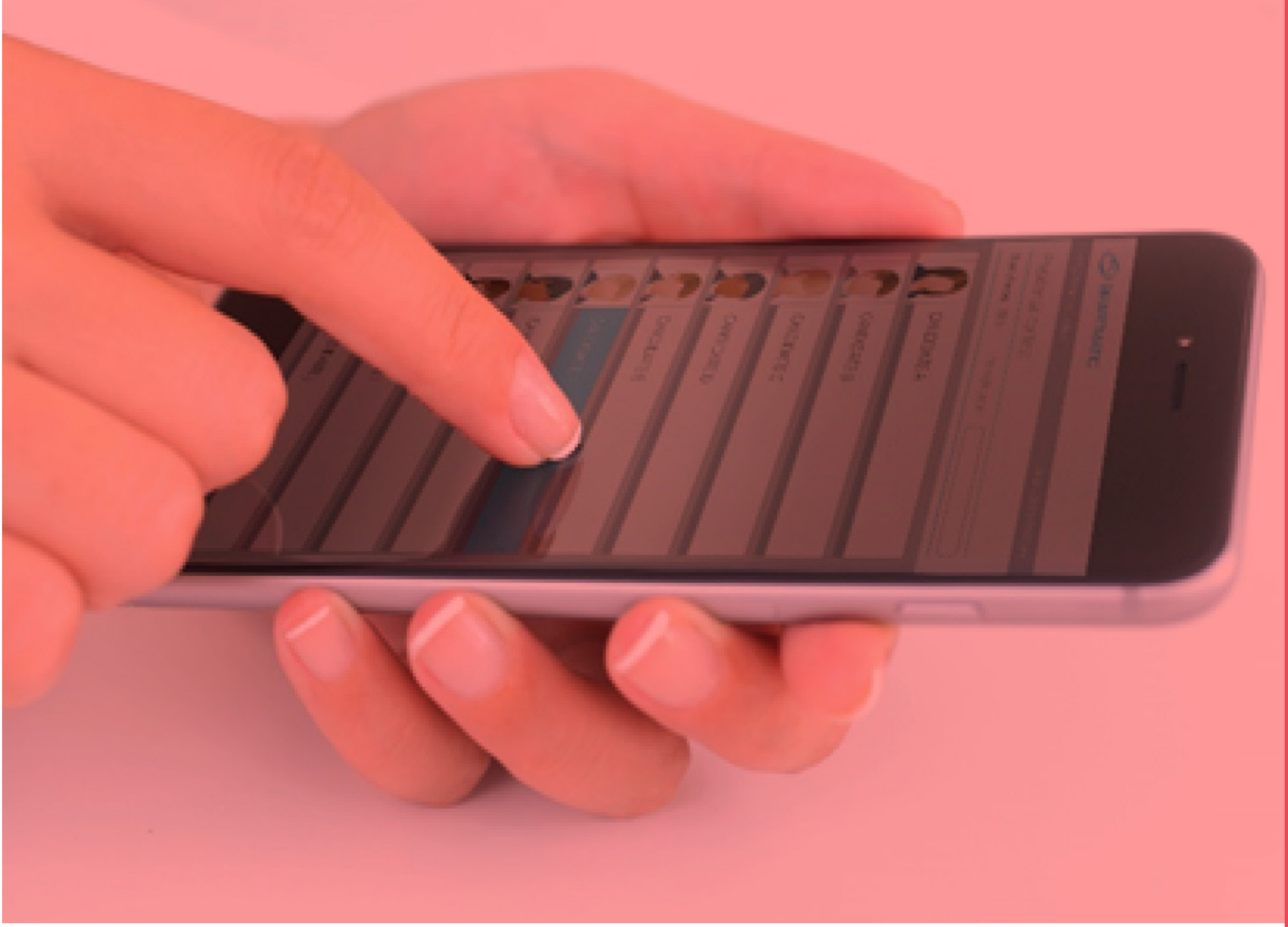
TIVI Powered by SMARTMATIC CYBERNETICA

Online Voting

Successfully Solving the Challenges

Table of Contents



Online Voting

No longer science fiction

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.

Yet, the experiences of early adopters show that the reality is somewhat different. The scrutinized and mission critical nature of elections together with the inherent, connected properties of information technology give rise to concerns, such as voter privacy, election integrity and overall transparency.

How can voters ensure that their vote remains secret? How can voters or the election authority prove the system was not rigged? How can the system deal with ever evolving cyber threats? How can people observe an electronic tally?

It is not uncommon that well-respected experts in the field of computer science reject the idea of online voting. We do agree, that if a naïve and poorly considered approach is taken, then online voting is a bad idea. We have seen several instances of poorly designed online voting systems simply failing.

However, well designed and properly engineered systems, which consider all the possible risks associated with casting a ballot online from an uncontrolled environment, have proved to be a viable and effective method of reaching 'hard-to-reach' voters.

Furthermore, they provide a convenient and secure channel for voters in remote locations to engage in the democratic process in a verifiable manner.

The success of online voting at a larger national, provincial and municipal scale has demonstrated that it is possible to have a secure and transparent election by secret ballot cast from a remote location.

Why this whitepaper?

This white paper gives a short overview of the key issues, challenges and considerations associated with online voting. We present not only the key questions that should be answered by any government considering online voting, but also a variety of effective, practical and proven solutions to address these challenges.

Secure Online Voting

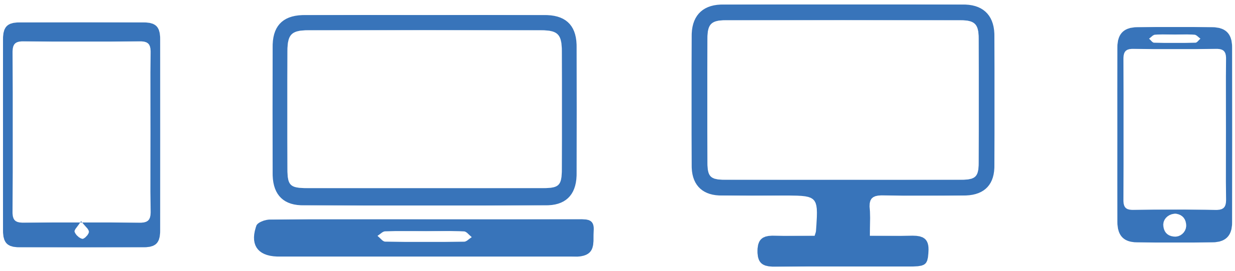
Online voting methods

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.

When we talk about online voting, in the overwhelming majority of cases we are describing an experience in which the votes are cast from a remote location on an Internet enabled device, using the Internet as a communication channel between the voter and the electronic ballot-box.



The most appealing way to apply online voting is to allow voters to participate in the election by using their own PC's, notebooks, tablets, smartphones as a voting device. This, and the fact that voting takes place in uncontrolled environments, which are outside the jurisdiction of the Election Management Body (EMB) raises the following questions:

- *How do we verify the eligibility of a voter in online voting?*
- *How is coercion-resistance achieved in the remote setting?*
- *What technology is available to support ballot secrecy and election integrity?*

Eligibility Assurance and Authentication

Online voting depends on the availability of a method for checking and verifying the eligibility of the voter from their remote location.

It is imperative that there is a **unique** way of identifying eligible voters and distinguishing them from those who are not eligible to vote. Also, there has to be a way for the voter to prove the claimed **identity** from that remote location.

1. The first part of the problem can be solved with the help of a coherent and up-to-date **voter registry.** The online voting system needs to interface with the registry and have a way of querying the eligibility of a voter.

2. The solution to the second part of the problem involves ensuring that methods of strong authentication are available to the electorate, which consider the following:

   - **Security aspect** – how fit for purpose the specific method is;
   - **Usability aspect** – what is the level of availability and usability for the end user; and
   - **Deployment aspect** – how complex is the distribution of necessary credentials/tokens to valid members of the electorate?

Strong authentication is a crucial part of determining the eligibility of the voters. Many countries operate electronic ID (e-ID) schemes, which allow citizens to access and interface with government services using personal e-ID cards, which have strong cryptographic properties. In these instances, voter eligibility can be ensured to prohibit ineligible voters from accessing the system.

This is the case is Estonia where online voting is one of many government services, which take advantage of the e-ID infrastructure.

Most 'government grade' online voting systems are **authentication agnostic,** meaning that eligible voters may use a choice of strong authentication methods to access the system. Well-designed protocols guarantee that it is possible to adjust to any authentication/identification scheme including, eID, biometric based systems and distributed multi-factor schemes.

Where e-ID schemes are not present, other **authentication options** may be used. Biometric information (such as fingerprint or facial information), often combined with biographical data taken from a government issued ID can be used to create a digital identity or profile of the voter. Modern smartphones possess superior quality cameras, allowing the capture of facial images, which can be compared with passport or driver license photos and cross referenced with a central citizen database. This provides a robust method for demonstrating eligibility and an assurance that the person who is voting really is the stated person who is eligible to access the system at the time of

Protecting ballot secrecy

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.**

The standard tool to ensure ballot secrecy is strong encryption. Most online voting protocols take advantage of public key encryption to protect ballot secrecy. This operates as follows:

- The EMB generates the election key-pair comprising the election private key and election public key. The election public key is distributed to the eligible voters.

- The voters use the election public key to encrypt their ballot beforecasting on the device from which they are accessing the online voting system. These ballots can only be decrypted with the election private key.

- The EMB uses the election private key to decrypt the ballots before tabulating the voting result.

- Online voting systems have to store the voter identification together with the encrypted ballot. It is therefore necessary to identify ballots to ensure that each eligible voter casts at most one vote that counts. A potential consequence is that anybody who has control over the election private key can theoretically decrypt individual ballots and determine who voted for who, which clearly violates ballot secrecy. **To protect against this, accountable election private key management is used to counter the threat.**

Accountable election private key management is necessary to ensure that the private key is only used in the appropriate manner to decrypt the ballots before tabulating the election result. There are two viable scenarios for key-management technologies:

1. Key management with hardware security modules;
2. Key management using threshold decryption schemes.

Key management with hardware security modules

A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys. The election private key is generated inside the HSM and the technology guarantees that the key can only be used in a specially protected area of the module. Modern HSM's are tamper evident and resistant, and such devices are commonly certified according to applicable standards (such as FIPS 140-2 or Common Criteria protection profiles).

For accountable key management, HSM's provide M-of-N key activation schemes, where security tokens are given out to the authorized personnel (typically members of the election authority, opposing political parties and even the media), and only a quorum of these people can jointly activate the private key operations and ultimately decrypt the votes.

A HSM is a standard solution for private key protection in other verticals including Internet banking. However, from the perspective of online voting there are some downsides to this technology.

Disadvantages

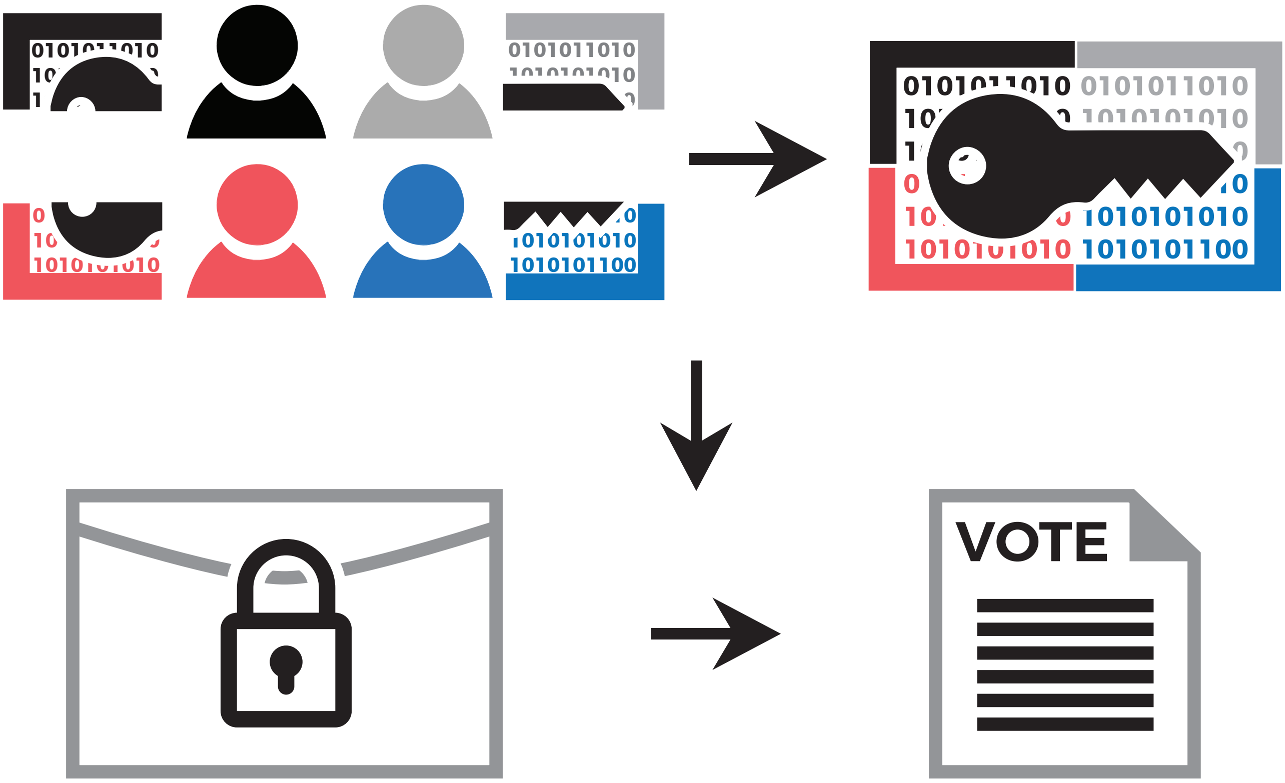
- HSM's can be expensive devices, and it may not be cost effective to purchase a HSM to use it once in two years for election key management.

- HSM's have restricted functionality in terms of available encryption schemes and it is complex and challenging to extend these devices to support more elaborate tabulation protocols that provide transparency and auditing capabilities in addition to the tabulated result.

Key management using threshold decryption schemes

Threshold decryption schemes implement tabulation protocols on ‘off-the-shelf’ hardware tokens, such as smart-cards or PIN-protected USB drives for accountable key management.

With this scenario, a M-of-N threshold decryption scheme generates the election public key and N private election key shares, which are distributed to the hardware tokens, with one unique share being stored on each of the tokens. The tokens are then distributed to members of the authorized election personnel. A quorum of M tokens must be present in order to reconstruct the election private key and ultimately decrypt the ballots.



Threshold decryption schemes provide accountable election key management, which is suitable for online voting at l**ower cost and with higher flexibility** than HSM technology. ‘Government grade’ online voting systems base ballot secrecy on the public key encryption and accountable key management. Either of these two scenarios for key-management are suitable for governmental online voting and may be considered.

When used in conjunction with standard Transport Layer Security (TLS) for communication between the voting device and the server, these mechanisms provide **highly effective methods of ensuring voter privacy.**

Ensuring Election Integrity

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.

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

1 Digital signatures

2 Blockchain-based digital time stamping.

Digital Signatures

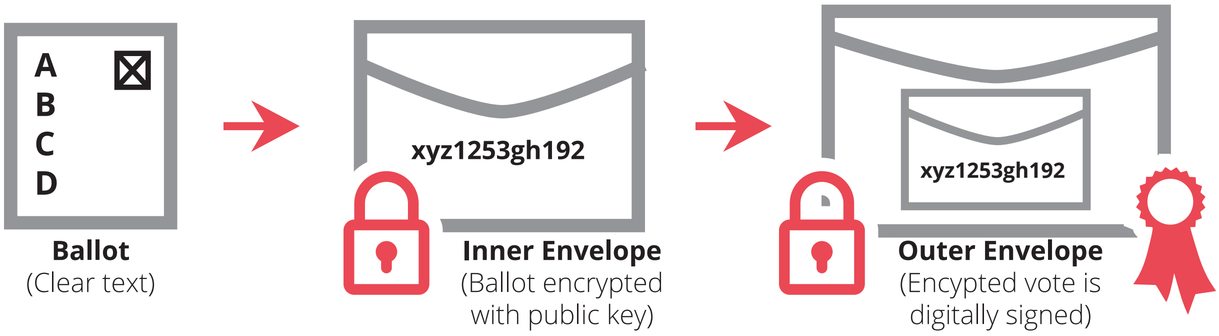
Digital signatures provide a method for **ensuring the authenticity and protecting the integrity of a digital message.**

Common digital signature methods are based on public key cryptography and rely on the voter being in possession of a private key that can be attributed only to that voter. In those countries where there is e-ID in place, this e-ID often has digital signing capabilities and can be used to confirm and protect the votes in an online voting protocol.

Digital signatures are used in combination with strong encryption (described earlier) to achieve ballot secrecy and vote integrity simultaneously. This so called "double-envelope" scheme is analogous to postal voting in which the anonymous ballot is encrypted with the election key (ballot secrecy envelope) and the encrypted ballot is digitally signed (outer envelope).

Strong encryption and digital signing of the vote in an online voting protocol offer far greater protection than the physical (paper based) protections of postal votes. In an online voting system, the votes are stored in an encrypted and digitally signed form, within physically, logically and procedurally secured redundant infrastructure.

Vote encryption using "double envelope" scheme



Blockchain-based digital time stamping

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 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. In combination, these methods offer a **high-level of protection against all threats to election integrity.** 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.

‘Government grade’ online voting systems take advantage of digital signature and Blockchain-based digital time stamping technologies.

Coercion resistant voting

Online voting usually takes place in an uncontrolled environment, where the threat of coercion may be higher than in polling stations. A reasonable level of protection must be provided to the voter, so that they cannot be coerced to vote in a specific way.

Coercion is not a technological problem and **cannot be solved by purely technical means.** Protocols exist that propose the use of both fake and valid credentials for voting. Fake credentials are used at the time of coercion; valid credentials are used at the time of actual voting. This type of scheme makes online voting cumbersome for voters and can create usability issues.

A more practical and effective approach to coercion-resistance involves multiple session and paper precedence voting. This operates as follows:

- Voters can vote several times - only the last vote is sent to the tabulation and ultimately counted;
- Voters can vote both on paper and online - in these cases the paper vote takes precedence and priority over any vote cast online.
- These measures ensure that the coercer cannot be sure, whether the coercion was successful or not, and eliminates the market for vote buying and vote selling.

Government grade online voting systems can handle multiple session voting and precedence-votes from other voting methods.

Distributed Denial of Service (DDoS) attacks

Distributed Denial of Service (DDoS) attacks are cyber-attacks in which a perpetrator seeks to make a network resource or service unavailable to its intended user, such as to temporarily or indefinitely suspend or interrupt services.

A DDoS attack is normally accomplished by overwhelming the target resource with superfluous traffic or network requests, which overload the target service and prevent it from fulfilling legitimate requests and processing valid requests.

DDoS attacks can affect any Internet based system and are a consequence of the fundamental architecture of the internet. This therefore potentially extends to online voting systems also. That said, it is possible to take steps to minimize the likelihood and impact of a DDoS attack on an online voting system and any governmental online voting system should feature appropriate and reasonable DDoS protection measures required to mitigate such attacks.

Defense techniques not only include the application of specific (intelligent) hardware or services, which are placed on the network before traffic reaches the servers. These devices analyze data packets as they enter the network, and identify them as priority, regular or dangerous, and route them appropriately. In addition to intelligent hardware, the voting solution itself has to have the potential to be **scaled out and seamlessly integrate** with distributed highly available infrastructural services, such as DNS.

The impact of any potential DDoS attack can also be minimized by offering online voting over an extended polling period. One of the advantages of online voting is the ability of deploy it in an environment where it can be offered to voters in a pre-poll period, typically 7 to 10 days before the election day, which provides the voter with a significant time period to vote.

It is mandatory for any modern online voting solution to make sure that the integrity, confidentiality and availability of already accepted votes is not undermined by any potential DDoS attack.

Transparent Online Voting

Observing Online Voting

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

Voter Verifiability

Individually verifiable voting methods provide the voter with the means to verify that certain properties such as 'cast as intended, accepted as cast and tallied as recorded' can be assured for the cast vote.

An example of individually verifiable voting was applied in **Norway** for online voting pilots in 2011 and 2013. This method takes advantage of two additional communication channels; a pre-channel implemented by the traditional postal system and post-channel implemented by cell-phones.

- Before the election each voter receives a printed check-list of (candidate, return-code) pairs on their polling card.
- Although the candidates are the same, return codes differ from voter to voter.
- The voter uses a voting application to cast their vote.
- After the vote has been received by the voting system, a SMS is sent to the voter with the return-code calculated from the encrypted vote.
- If the return-code matches the printed code relating to the voter's actual choice on the poll card, then the voter can be sure that the ballot was accepted by the server and the voter's choice was correctly encoded.
- If malicious software has modified the voter's choice, the return-code will indicate a different candidate.

A more accessible way of individual verifiability is used in Estonia. Voters have access to a smartphone application that can be used to verify that the vote cast with the voting application, was accepted as cast by the online voting system, and cast as intended by the voting application.

It operates as follows:

- A cryptographic receipt is displayed by the voting application on the voter's computer in the form of a QR code, which comprises a unique random token and a unique voting session code.
- The camera of the smartphone is used to capture the receipt and the session code is sent to the vote server.
- The vote server identifies the vote being verified and returns the digitally signed, encrypted vote to the verification application.

- The vote server then sends the list of candidates in that contest to the verification application.

- The verification application cannot decrypt the vote, but it knows the random token and the public key which were used to encrypt the vote, therefore it can create cryptograms for all the candidates on the ballot using the token.

- The verification application searches for the cryptogram that matches the vote received from the server.

- The matching cryptogram is shown to the voter on the verification application allowing the voter to verify that their vote was cast as intended and received by the server correctly.

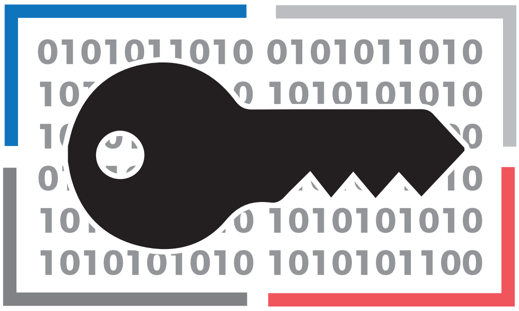
Using this technique, the voter is **assured that there was no manipulation** of his/her vote on their computer or whilst being transmitted to the vote server. The usage of the vote verification application is optional and does not require any materials distributed over the postal channel.

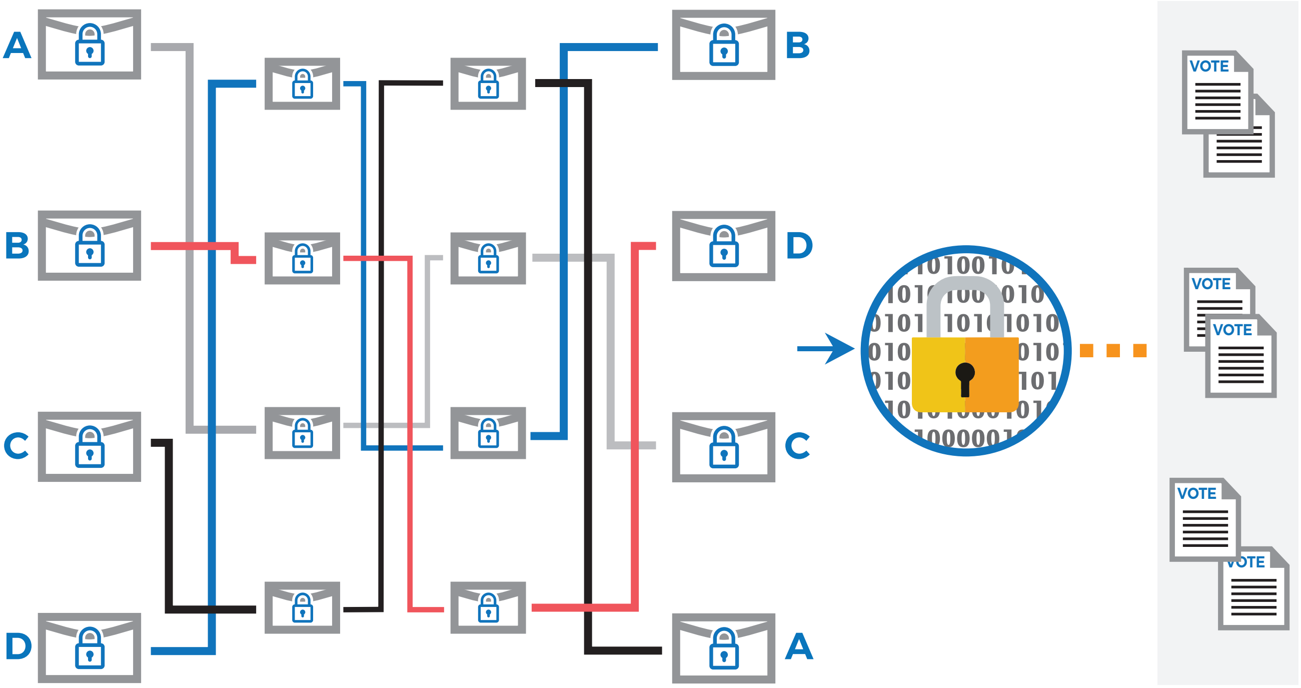
In summary, 'government grade' online voting systems provide voters with tools for individual verifiability. Different approaches to verifiability have different cost, accessibility and level of assurance, but some form of individual verifiability should be a baseline requirement for online voting in government elections.

Public perspective

Auditable voting methods give means to official observers and auditors to verify that the voting result was tabulated correctly according to the contents of the digital ballot-box. When used in combination with advanced cryptographic techniques to ensure ballot-secrecy, auditability can provide a higher level of transparency than current traditional voting methods.

In ‘government grade’ online voting systems, all system components that directly handle votes, are capable of generating proofs for auditing. These proofs are based on cryptographic protocols and provide a high-level of assurance that the election has not been tampered with and that the end-to-end election process operated as expected.





As in any government election, the **privacy of the voter is paramount.** At no stage should it be possible to correlate clear vote preferences with the identity of the voter who cast the ballot. Within the context of online voting, cryptographic verifiable shuffling of the votes – e.g. mixing – provides a highly effective way of ensuring voter privacy and ensuring that at no stage the vote preferences are linked with the identity of the voter. Mixing plays a crucial role in anonymizing the data that is provided to the auditor.

The auditing can use the data provided by the election system, published protocols and open source tauditing tools to effectively audit the end to end election. Without sacrificing ballot secrecy or voter privacy, the auditors can prove that votes stored in the voting system were handled correctly.

The auditors should audit the following aspects of the election:

- All votes were digitally signed and the signatures verified correctly;
- All stored votes were correctly sent to tabulation;
- All encrypted votes were correctly decrypted in the tabulation.

Conclusion

In summary, state-of-the-art, 'governmental-grade' online voting systems have to support the key democratic principles of franchisement, privacy and integrity. To support these objectives, online voting systems need to optimally balance accessibility, security and transparency, which are critical in creating public trust in the system and legitimacy, credibility of the election process.

The underlying technology must support transparent online voting, allow for auditability by officially appointed external parties and individually by voters. Only then is it possible to prove to stakeholders that the online voting system performed its task correctly and that the voting result is legitimate.

Therefore;

- Transparency must co-exist with voter privacy and coercion resistance – nobody should find out how a specific voter voted.
- Ballot secrecy can be achieved with strong encryption and accountable key management.
- Coercion-resistance is supported by multi-session voting and paper voting precedence.
- Election integrity has to be achieved by protecting the integrity of the votes and the ballot-box by appropriate means, such as digital signatures and Blockchain-based digital time stamping.
- Digital double envelope schemes combine integrity proving and secrecy assuring technologies supported by strong authentication and eligibility assurance technology, such as governmentally issued ID-cards, biometric systems or multi-factor credential schemes.
- The likelihood of a DDoS attack on an online voting system can be minimized by the application of specific (intelligent) hardware or services, by having a seamless integration with highly available infrastructural services and by offering online voting over an extended polling period.

These technologies form the foundation of secure and practical online voting for governments.

Curious to learn more?

For more details, webinars and information, please have a look at the TIVI web site, or send us an email: **hello@tivi.io.**

tivi.io.
hello@tivi.io.