WHITE PAPER

Implementing End-to-End Verifiable Online Voting for Secure, Transparent and Tamper-Proof Elections

Sponsored by: Scytl

Fayaz Khaki
October 2014

INTRODUCTION

A citizen's vote is his right to express his democratic view. Elections are therefore a particularly emotional and personal affair for most citizens. However, being able to vote has not always been an easy process for some citizens such as those living overseas, military personnel, people with disabilities, and so on. These voter demographics have often been disenfranchised, having few options when it comes to exercising their right to vote: delegating their vote, voting by mail, or traveling to the nearest consulate or embassy and facing a multitude of hurdles in casting their ballots. These run from logistic difficulties, hefty administrative proceedings, long distances between the voters current residence place and the election office, inflexible voting opening hours and postal delays, all the way to privacy and security concerns.

To properly allow the complete demographic of voters to exercise their democratic and constitutional right, governments have to seek other methods by which to allow all citizens to vote.

Technology has changed dramatically over the past two decades. It has advanced and matured to the point at which the traditional form of voting can be partially, or in some instances, completely replaced with new technology. As a result of this technological advancement and maturity, online voting has emerged as a genuine solution to address the challenges faced by voter disenfranchisement and in addition help attract more young voters to exercise their democratic right.

However, the use of technology for online voting does come with its own security challenges that need to be overcome to safeguard the pillars of any free and fair election process, ensuring:

- Strong voter authentication
- Voter privacy
- Verifiability
- Election integrity

This paper focuses on how governments can implement the necessary information security controls that address those challenges.

CHALLENGES OF ONLINE VOTING

Breaches in the controlled environment of corporate infrastructures continue to be front page news. There has been a dramatic increase of over 200% in the number of significant (i.e., over one million records stolen) information security breaches in the first six months of 2014 alone when compared to the whole of 2013. Implementing the correct levels of information security control is a concern and priority for business.

These are also concerns that governments need to look into and address when seeking to implement online voting. Hacks steal records from organizations because there is money to be made from selling stolen records. Online voting is therefore a massive opportunity for hackers to make a lot of money not only by selling records but also crucially by potentially being able to influence and also directly manipulate election results.

Information security is a vital component in being able to address the challenges posed by online voting and particularly in ensuring strong voter authentication, voter privacy, and full verifiability, as well as preserving an election's integrity. It is important to understand that online voting can only be a success if the voters and other players involved in an election, such as political parties and observers, trust the technology that is being used to support the online voting process. The most important aspect in gaining that trust is being able to provide verifiability throughout the election process. This trust can be ensured through the implementation of end-to-end verifiable online voting, by using the most advanced levels of information security controls, thus safeguarding the four key pillars of a free and fair election.

Implementing Information Security For Online Voting

There is a clear distinction between basic and advanced information security. Standard encryption and decryption methods have proved to be more vulnerable to external and internal attacks, while advanced security measures (such as digital certificates, digital signatures, immutable logs, and end-to-end encryption) guarantee that voters are strongly authenticated, voter privacy is protected, and election results and votes cannot be manipulated by external hackers or even by internal technical staff with system privileges without these attempts being detected and impeded.

The latest advances in the field of applied security in online voting have enabled governments like Norway to implement end-to-end verifiable online voting, allowing voters to check for themselves that their votes have been cast-as-intended, recorded-as-cast, and counted-as-recorded.

To date the certification of online voting software has been the traditional method followed by governments to make sure that systems comply with a country's security and electoral standards. But implementing end-to-end verifiable online voting through the adoption of advanced information security could allow governments to go one step further and allow them to shift from simply certifying voting systems to certifying elections. This new paradigm allows for greater transparency and trust in election processes.

Implementing end-to-end verifiable online voting implies not only adopting advanced security standards, but also combining these standards in order to deploy multiple security layers and therefore ensure stronger protection against potential threats and greater transparency in the election process itself.

Table 1 depicts why advanced security should be used when implementing information security controls for online voting. It also provides an indication of the types of multilayered and in- depth security capabilities available when advanced security techniques are employed.

TABLE 1

Basic Security Versus Advanced Security

Domain	Basic Security	Control Provision (Basic Security)	Advanced Security	Control Provision (Advanced Security)
Authentication	Username and password	Usernames and passwords are stored on the servers, which can be stolen by attackers or brute force techniques applied to steal bulk credentials.	Digital certificates	Digital certificates provide robustness to the authentication process as voter credentials are not stored on the server.
End-to-end voter privacy	Encrypting the network transmission channel	Encrypting the network channel is not enough to provide end-to-end secrecy as the votes remain encrypted only when being transmitted. Even when the votes are encrypted in the server, clear text votes could be intercepted before being ciphered on the server.	Encrypting the votes on the voter's device.	Encrypting the votes on the voters' device provides end-to-end encryption and ensures votes are not passed in clear text mode in any stage of the voting process, also ensuring that votes are only decrypted by the proper election authorities at the counting stage.
Voter privacy during vote decryption	Basic decryption	Allows for clear text votes to be easily correlated to the encrypted votes, therefore not ensuring voter privacy.	Cryptographic mixnets and secret sharing	Cryptographic mixnets shuffle and re-encrypt/ decrypt the votes several times before obtaining the clear text votes. This breaks the correlation of the vote to the original voting order ensuring voter privacy. Secret sharing breaks the decryption key into several parts and ensures no single electoral board member can decrypt a ballot box.
Vote integrity and authenticity	Message authentication codes (MAC) / server digital signatures	The key has to be shared between the voter and the server (MAC) or is stored on the server (digital signature). Therefore, the server is able to generate a MAC code or digital signature of any vote.	Voter digital signatures	Votes are digitally signed by the voter after they have been encrypted. Therefore the server can validate and verify the signature as authentic and cannot manipulate it.

Election monitoring	Standard log generation	Logs can be maliciously modified without any indication proving the logs have been tampered with.	Immutable logs	Immutable logs use cryptographic processes to ensure the logs cannot be changed and thus prevent tampering as well as highlighting any unfruitful attempt at tampering.
Election verifiability	Standard receipts	Confirms that the vote has been cast, but does not provide proof that the vote has been cast as originally selected.	Individual voter verification Universal verification	Voters are able to verify the vote recorded has been recorded correctly and in accordance with the voting options originally selected by the voter. Universal auditability provides voters, observers, and independent auditors assurance over the decryption / counting process. It guarantees the vote has been: ▪ Cast-as-intended ▪ Recorded-as-cast ▪ Counted-as-recorded

Source: IDC, 2014

Ensuring Voter Authenticity

Any online voting process needs to ensure that the citizen's identity is genuine (i.e., not false or fraudulent) and that the citizen voting is eligible to vote.

How to Ensure Voter Authenticity

Voter authenticity needs to be maintained from the very start of the voting process – even before the voter logs in to the voting application.

Basic security controls such as usernames and passwords do not fulfill the required information security principles for online voting. Usernames and password can be easily compromised via brute force attacks or even guessing. In addition, given that usernames and passwords need to be stored on servers, if the server is compromised it potentially exposes all the citizens who are eligible to vote.

To ensure voter authenticity, advanced security controls are required. Advanced security techniques leverage technologies such as digital certificates or national electronic ID cards (e-ID). In order for a voter to obtain a digital certificate or an e-ID card they will need to prove they are who they say they are. Digital certificates – provided that they are issued specifically for an election and not reused in other elections – or e-ID cards cannot be obtained by brute force or guessed by an attacker. Furthermore, digital certificates and e-ID cards are held by the individual voters and are not stored on a central server, resulting in the central server not being a potential single point of failure.

Protecting Voter Privacy

Maintaining citizens' privacy throughout the voting process is also critical when implementing online voting as it provides confidence to the voter that his vote will remain private, ensuring the voter cannot be subject to any coercion.

How to Ensure Voter Privacy

Ensuring privacy is a multistep process that needs to be maintained throughout the voting process: during the voting process, during the transmission of the vote to the server and during the decryption process.

Privacy ought to be maintained from the point at which the citizen marks his ballot through to the point in which the ballot is counted. Using basic security techniques such as encrypting the transmission channel is not enough as the votes remain encrypted only during transport. At either end of the transmission channel the votes are in clear text. Clear text votes can easily be read by unauthorized users in breach of privacy, and can also be tampered with or manipulated without any evidence being left that the vote has been altered. This is also possible when votes are encrypted in the server, because votes are vulnerable to eavesdropping and/or manipulation in the server before being encrypted.

Decrypting the votes themselves using basic cryptographic techniques also falls short when maintaining voter privacy. Once the votes are decrypted they can easily be associated with the voter as the correlation between the encrypted vote and the decrypted vote has not been broken, and can easily be matched. To ensure voter privacy and to prevent encrypted and decrypted votes being easily matched, advanced cryptographic techniques and systems need to be employed.

To warrant complete confidentiality and privacy, the votes ought to be encrypted through the stack (on the voting device), guaranteeing votes are never actually sent in clear text and are not restricted to being encrypted only through the transmission channel or in the server by privileged actors. This ensures that votes can only be decrypted by the proper election authorities (i.e., the electoral board) during the counting period.

In addition, during the decryption process standard decryption methods are not sufficient to ensure voter privacy as clear text votes could easily be correlated to the encrypted votes and therefore to the voter (even if the voter identity is detached from the vote). To further reinforce the security during the decryption process, cryptographic mixnets and secret sharing techniques should be used to ensure the votes cannot be correlated back to the voter and voter privacy is maintained.

Cryptographic mixnets shuffle and re-encrypt/decrypt the votes several times before obtaining the clear text votes. This breaks the correlation of the vote to the original voting order (encrypted votes) and therefore, indirectly to the voter.

Meanwhile, secret sharing breaks the decryption key into several parts and distributes those parts to the election authorities, protecting the secrecy of the election (i.e., electoral board). The decryption key is therefore not stored anywhere (it is not vulnerable to being stolen) and is only retrieved when reconstructed by the election authorities before decrypting the ballot box. This ensures that no single electoral board member can decrypt a ballot box and that the key is not vulnerable to being stolen.

Providing Election Verifiability

Vote verifiability in online voting provides many added benefits that a voter wouldn't otherwise obtain when using traditional voting methods. The objective of vote verifiability is to provide the voter and election observers with a level of comfort (and transparency) that the vote has been cast as he intended, that his vote has been recorded as he cast it, and that the vote has been counted as it was previously recorded. Put another way, the voter has the confidence that the vote has not been interfered or tampered with and has been included in the final tally of the election results as the voter originally intended.

Online voting has many verifiability advantages over traditional voting. With traditional voting, for example, the only verification a voter gets is cast-as-intended and recorded-as-cast, i.e. the voter marks the ballot paper and submits that ballot paper into the ballot box. However, from then on, the voter does not receive any verification that the vote has been counted-as-recorded. With online voting end-to-end verifiability, however, a voter will receive a verification of the counting of his vote through the voting process. This provides the voter with confidence that the vote has been included – correctly – in the final results tally.

In addition, counted-as-recorded verification allows any electoral observer and independent auditor to audit the counting process without requiring special privileges to the system or being an eligible voter, achieving universal verifiability. This allows the public certification of the accuracy and integrity of an election process regardless of the voting system being certified.

How to Ensure Election Verifiability

Providing the voter with verifiability while maintaining voter privacy is a difficult objective to meet. However, this is possible if advanced cryptographic techniques are used, as these techniques utilize verifiable mechanisms to ensure these objectives are met. As previously mentioned, there are effectively three phases during which a voter will require verification to ensure the vote has not been tampered or interfered with. These three key voter verification pillars are:

- Cast-as-intended: Previous to the election day, voters receive individual codes corresponding to each candidate. These codes are privately generated (by the election officers) and are known only to the voter. Once the voter has cast his vote online, he will receive return codes confirming his voting options. These return codes will have to match the original candidate codes previously received by the voter. The return codes are generated by the voting server over the encrypted vote to maintain voter privacy (i.e., the vote is never decrypted) and sent to the voter. If the return codes do not match, the voter can assume that his vote has been tampered with or manipulated.
- Recorded-as-cast: After confirming the return codes are correct, voters receive a voting receipt based on a fingerprint of the encrypted vote. During the voting process, the servers publish the fingerprints of the encrypted votes stored in the ballot box. The voting receipt will allow the voter to check that his vote has been recorded properly. The voting receipt, together with the return code, provides the voter with the confidence that his vote has been recorded as originally cast.
- Counted-as-recorded: This verification is based on generating irrefutable mathematical proofs of the cryptographic processes: mixing and decrypting the votes. Using standard mathematical operations, observers can check that no vote has been manipulated when the contents of the encrypted votes are obtained. These proofs do not contain any information that could allow any correlation between the votes and the voters. They are therefore known as Zero Knowledge Proofs.

Guaranteeing Election Integrity

The objective of election integrity is to ensure a transparent process that enables a free and fair election to be conducted in line with democratic values. Election integrity is provided through the culmination of all the advanced security techniques discussed above being implemented and operated correctly to provide the voter with the confidence required.

Transparency and independent verification of results and the fairness of the election process is also required. In order to achieve this, additional advanced security mechanisms need to be in place for online voting.

How to Ensure Election Integrity

In addition to the mechanisms described under voter authenticity, voter privacy, and vote verification, a means for the election process to be audited by an independent body is required. For this, encrypted votes need to be digitally signed by voters before they are cast. This prevents the manipulation of the votes after being cast and also ensures the eligibility of the votes stored in the ballot box by means of verification of the digital signatures. Digitally signing the votes in the servers does not fully ensure integrity, because if the server key is compromised, votes could be manipulated or added without being detected.

To ensure election integrity, logs also need to be generated and stored to facilitate election monitoring. These logs are used to record activity which can then be audited and reviewed to ensure election integrity has been maintained – i.e., the election has been transparent and hasn't been manipulated. Given the importance of the logs in providing assurance, basic security mechanisms will not provide the level of assurance required, as logs generated via basic security mechanisms can easily be tampered with or even deleted.

Logs generated and protected using cryptographic systems made available under advanced security will ensure the logs are immutable and cannot be tampered with. This will enable observers and independent auditors to provide a high level of assurance of the election process such as the authentication of voters and casting of votes and also ensuring the votes have not been interfered with in any way.

Voter verifiability (both individual and universal – discussed above) is vital to ensuring election integrity. Voters need to be provided with individual verification that their votes have been cast as they intended and included in the final tally of results as they, the voters, cast their vote; the tallying process should also be universally verifiable, not only by voters, but by any other independent authority or observers to ensure the maximum level of transparency. All these verifiability

processes should ensure voter privacy and not disclose any details that could be used to coerce the vote or facilitate vote selling practices.

Implementing advanced security mechanisms to enforce the information security principles within voter authenticity and privacy, vote verifiability, and election integrity, will provide governments and voters with the layered security that is required to certify the election process as opposed to just the voting devices, ensuring a free, fair, and transparent election.

CONCLUSION

The advantages of online voting include cost savings, electoral process efficiency, and voting convenience. However, to ensure online voting is a true success the voter needs to be able to trust the technology that is being used for the election process. Advanced security techniques described above make online voting a viable option.

Some of the key areas that need to be addressed to ensure this trust when implementing online voting technology are:

- Encryption: End-to-end encryption should be implemented to ensure the confidentiality of the voting process is maintained throughout the election process, despite the presence of technological privileged actors (i.e., IT infrastructure managers) or new technological risks (i.e., malicious hackers).
- Anonymity and privacy: Protecting a voter's privacy is key to ensuring online voting maintains the same level of voter anonymity as is offered by manual voting on ballot papers.
- Verifiability: Providing voting process transparency in an online voting environment is a challenge; the technology exists to ensure a voter can verify his vote has been cast and counted correctly. Verifiability is vital to provide usable means to the voter to check that his vote hasn't been tampered with. In addition, universal verifiability is crucial for observers and independent auditors to verify the accuracy of the election process.
- Technology independence: Online voting using end-to-end verifiable techniques allows the auditing of the election process regardless of the software and technology used by the voting platform or voter's device. Therefore, it does not require voters to use specific certified voting devices to cast their votes.
- Proven technology: Considering the critical aspect of election processes, online voting needs to utilize technology that has been proven, tested, and implemented across different election processes and countries.

To date, a variety of countries across the globe have successfully implemented online voting in binding political elections, including France, Switzerland, Norway, Australia, the U.S., Canada, Mexico, India, the UAE, and Peru.

Norway has pioneered the implementation of end-to-end verifiable online voting processes, and other countries are following its example. Most recently, the Swiss Federal Council allowed the deployment of online voting on a larger scale provided that Cantons ensure end-to-end verifiable online voting. In addition, various initiatives across the globe are being implemented to enable a more convenient voting process for both persons with disabilities and those overseas.

CASE STUDY — ONLINE VOTING IN NORWAY

Norway has a long history with online voting. With initial studies beginning back in 2004, Norway has travelled a long and successful road to its latest deployment of online elections in 2013.

The latest election where Norway leveraged online voting was in the 2013 Parliamentary Elections. As part of the country´s strategy for online voting rollout, the online voting channel was only deployed in a series of pre-selected municipalities. Upon the conclusion of the election and the use of online voting in 12 municipalities, feedback from the trial was a success with high support from the electorate for online voting with 75% expressing a positive opinion about the process. Overall, 30% of all votes were cast via the online voting system.

The process for including online voting as an additional channel in Norway began in 2004. The initial discussions which began in 2004 were centered on evoting (i.e., electronic voting at the polling stations). However, the cost and complexity of implementing an infrastructure specifically for evoting dissuaded the government at the time.

In 2006, discussions progressed to online voting and were mainly driven by the government's Election Ministry. The primary driving factors for online voting, particularly for the Norwegian government, were:

- Make voting accessible to the whole electorate, particularly those living overseas, the disabled, or those unable to get to polling stations on the day of the election.
- Cost/benefit of online voting in controlled (supervised) versus the cost/ benefit in uncontrolled (unsupervised) environments. Enabling voters to cast their vote from home allows the government to continue to use existing election infrastructure (unlike the scenario where new poll stations would be required for evoting).
- Online voting ensures the creation of efficiencies and speed in the election process.

To ensure the solution not only addressed efficiencies and cost/benefits, the Norwegian government thoroughly reviewed and addressed all concerns around online voting. The key and critical concern was on ensuring electoral information security, transparency and privacy. All these issues were addressed in the procurement process managed by the Election Ministry, which followed the Competitive Dialogue procurement process when interviewing and assessing potential vendors. The process, due to the level of detail required around security and privacy concerns, took just under six months from May 2009 to September 2009.

At the end of the procurement process, the most qualified and best resourced vendor was selected to deliver the online voting project, which started in 2010. Given the scope and newness of the process in Norway, the implementation of the online voting system, along with its corresponding election administrative system, was a difficult process that was duly addressed by all parties involved in the project. Some of the difficulties overcome included:

- The software vendors were geographically separated (Oslo and Barcelona), while developing two highly integrated modules – more or less from scratch.
- High security requirements made it difficult for the ministry to perform detailed software functionality testing, though security testing was in-depth and fully audited.

- Differences between development and operating environments made the delivery process time-consuming and error prone and requiring additional testing to ensure full functionality.
- For the Election Ministry, it was vital for the selected vendor to have the capability and skilled resources to be able to support the implementation, even if this meant resources were remotely located.

Throughout the 2010 implementation of the online voting system a number of rigorous attack and penetration tests were used on the system. These tests were conducted by third parties not affiliated with the vendor delivering the online voting system and also included academic institutions. They were conducted to ensure the online voting system was implemented correctly and that there were no vulnerabilities or potential weaknesses within the process.

After the rigorous testing and trialing of the process to ensure information security and privacy controls were maintained, in 2011 the online voting system was used for the first time in local elections across 10 municipalities. To provide assurances to the electorate that their safety and privacy would be maintained via the online voting process, the Norwegian government embarked on a number of initiatives:

- Personal letters were sent to the electorate explaining online voting and how information security and privacy will be maintained.
- Radio interviews explaining the voting process and security and privacy features were conducted.
- A dedicated website was setup to ensure not only clear information about the process but to ensure the entire procurement and implementation processes were completely transparent.

  http://www.regjeringen.no/en/dep/kmd/prosjekter/e-vote-trial/about-the-e-vote-project.html?id=597724

- The government set up technical working groups which included opponents of online voting and allowed them to test the system to give them confidence in the information security and privacy controls that had been implemented.

After successfully rolling out online voting during the local elections, the Norwegian government extended online voting to include the 2013 parliamentary elections. All in all, both from the security, transparency, privacy and electorate uptake, the Norwegian online voting experience has proven a success on all fronts and is a reference for other countries looking to implement fully verifiable online voting solutions.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com