Scytl
Innovating Democracy

Scytl
Online Voting

The Pillars of End-to-End Online Voting Security and Verifiability

Thanks to technology advances and maturity, online voting has emerged as a genuine solution to address the challenges faced by disenfranchised voters, help attract more voters to exercise their democratic right and make elections more secure, transparent, auditable and efficient.

In order to safeguard the pillars of free and fair elections, online voting technology needs to address key security aspects, and ensure:

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

This mini guide will help you comprehend the advanced security framework that Scytl provides (vs. Basic security measures implemented by other technology vendors) that address those challenges and helps safeguard the pillars of any free and fair election process.

The Pillars of End-to-End Online Voting Security and Verifiability

Security area	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 hackers 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 transported. 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. This also ensurs 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 in 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	The 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 with the voting options originally selected by the voter. Universal auditability allows voters, observers and independent auditors to provide assurance over the decryption / counting process. It guarantees the vote has been: - Cast-as-intended - Recorded-as-cast - Counted-as-recorded