DETERMINE THE REQUIREMENTS

TEAM ID	NM2023TMID04404
PROJECT NAME	ELECTRONIC VOTING MACHINE

Online voting has to meet a number of requirements in order to achieve the same or higher security than that of traditional paper-based voting. These requirements can be organized into four main groups: authentication, integrity, privacy and verifiability.

Authentication requires voters to be uniquely identified in a way that unmistakably distinguishes them from other people. Authentication can be implemented by several mechanisms, such as: pairs of usernames and passwords securely delivered to the voters before the election; pre-existing citizen authentication credentials, like those used for government web portals; or electronic identification cards, like national IDs.

Also, these mechanisms can be combined with additional authentication factors, such as login confirmation through a secondary device (an SMS code sent to the voter's mobile phone, for example) or biometric authentication (fingerprints or face scans). Thanks to these authentication mechanisms, the e-voting system can verify a voter's eligibility and will only grant access to citizens who have the right to vote.

Integrity means that a voter's intention shall not be affected by the voting system, or by any undue influence. In an online voting system, integrity is protected at different levels and stages throughout the election. At the beginning, during the voting period, each ballot is digitally signed with a key unique to each voter, ensuring that the ballot cannot be altered by anyone other than the voter themself. Later, during the counting process, when the votes are anonymized and decrypted, digital signatures are used to protect the intermediate data exchanged during these processes and, depending on the type of election, mathematical proofs are also done to ensure the integrity of the processes themselves. Other sensitive information that is susceptible to manipulation is also digitally signed to prevent manipulation, such as election configuration files.

While many of these security features are indeed complex and sophisticated, this does not translate to the usability of an online voting system. Any qualified provider should have these measures built in and automatically applied when possible, simplifying the entire process election organizers and voters alike.

They should also offer the necessary support to ensure that the election runs smoothly and securely. To learn more about the different security measures mentioned in this article, you can find in-depth descriptions in our Security Table of Online Voting, available in our resource center.

Counted-as-Recorded verifiability, on the other hand, enables anybody with the data used and produced by the counting process to check that each authentic and authorized vote is accurately included in the respective election results. The evidence should be verifiable by means independent from the system. Usually mathematical proofs, known as Zero Knowledge Proofs, are generated by several of the counting processes and can be externally verified. In this manner it can be proven that the process was correct, and that no manipulation of the votes was produced during counting.