Eligo
Your way to vote

Eligo eVoting Platform

Technical Documentation

Document version: V.1.0
Platform Version: V.5.0
Date: 02/18/2024

Who we are

Company background and experience in the field of voting

Eligo is the online voting platform, verified by third-party legal entities: it guarantees the safe, secret and unambiguous vote, obtaining legally valid electoral results.

Since 2005 we are specialized in the field of electronic and online voting. We managed every kind of vote adapting and evolving the platform for the most varied types of Bodies, Associations, Social Security Funds, Municipalities, Universities and any type of Organization.

Electronic and online voting is increasingly seen and perceived as a technology of communication and involvement to make democracy effective in every area, public or private. Italy has already passed the testing phase and is entering the normalization phase: evoting is already normal and its adoption consolidated. Outside the political world, digital democracy is already a commodity. In some non-European countries, the use of digital voting systems has had immediate benefits on turnout, participation and a reduction in abstentionism.

Eligo
Your way to vote

ID_TECHNOLOGY

+24 YEARS IN THE FIELD

+20 MILIONS VOTERS

+45.000 CUSTOMERS

+55.000 ELECTIONS AND MEETINGS MANAGED

98,3% INDEX SATISFYING

+20 PROFESSIONALS

What we do

Main features of the platform

Eligo is a complete eVoting and iVoting system that has become the standard of the national market. Our platform is fully cloud-based, web-based, secure, legal and certified. It allows you to create and manage any type of voting and deliberative and elective assembly - provided for bylaws and Regulations - in hybrid, full-remote or at the seat. A computer system must ensure the security and confidentiality of data of its users. An evoting system, in particular, must guarantee its anonymity.

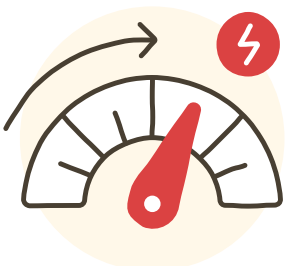
Both during and after a voting process, it should not be possible to associate the voting preference with users in order to make it secret. Fortunately, at the state of the art, platforms such as ELIGO are able to prevent - with the use of established and effective techniques of encryption and software engineering - any threats: DOS attacks, ie service interruption; spoofing, ie identity falsification; or sniffing, unauthorized interception of data.

All the infrastructure and application of Eligo is located on NextGen Cloud solution, in this case Azure with physical data residence in the datacenter in the Netherlands within the European Union. All data, back-ups and resiliency copies for business continuity are always located within the European space for GDPR compliance and protection of our customers' data.

Web-Based e full-responsive

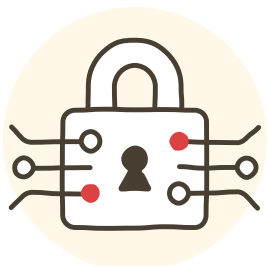
Click-n-Play configuration

Nextgen Cloud Solution



Highly performing

Secure multi-layers identification for the voters



Cryptographic communication at every level

Functionalities for every need

Feature Weighted Vote

With this module you can manage weighted voting cases regardless of its type. In the case of shareholders' meetings, the module allows to have all the data available in real time for constitutive and deliberative quorum both in terms of heads and weighted votes of the participants.

Feature Proxies Management

Thanks to this module, in its various declinations, you can manage all the types of proxies. Internal, external, Joint or Disjoint Proxies, Substitute or other specific needs. This module allows in any case to manage the need for the transfer of voting rights.

Feature 2FA

Strong authentication is the backbone of every digital process. At Eligo, we provide the ability for strong authentication with a second (or even third) authentication factor. We can send it by SMS, email, or using external SSO systems.

Feature Categories

The module allows you to divide the right to vote within the same assembly or electoral event. It allows to manage multiple concurrent assemblies or particular voting needs in which votes are diversified by electorate.

Professional services

Direct assistance to voters

We provide telephone and/or email switchboard service for direct support to voters during the open voting period. Sized according to the size of the electorate, we ensure that all voters get all the necessary support and quickly to cast their vote.

On-site assistance

Voting is an important and stressed moment. That's why we are always by your side. Eligo team will be there to provide all the procedural and technical support needed to better live the experience of a voting process.

Consulting on the voting project

Each voting project is different and each customer has their own needs. With our team of specialists and the experience of hundreds of voting projects we can provide advice and development on custom projects. We define together the essential elements taking into account all the necessary features.

Sviluppi Custom e Brand Identity

If requested, we make customizations especially related to process, technogy, brand identity. Over more than 20 years on the market we have developed techniques and integrations with the main technologies on the market.

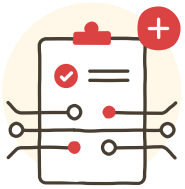
Voting process

Guarantee of safety, uniqueness and anonymity of the vote

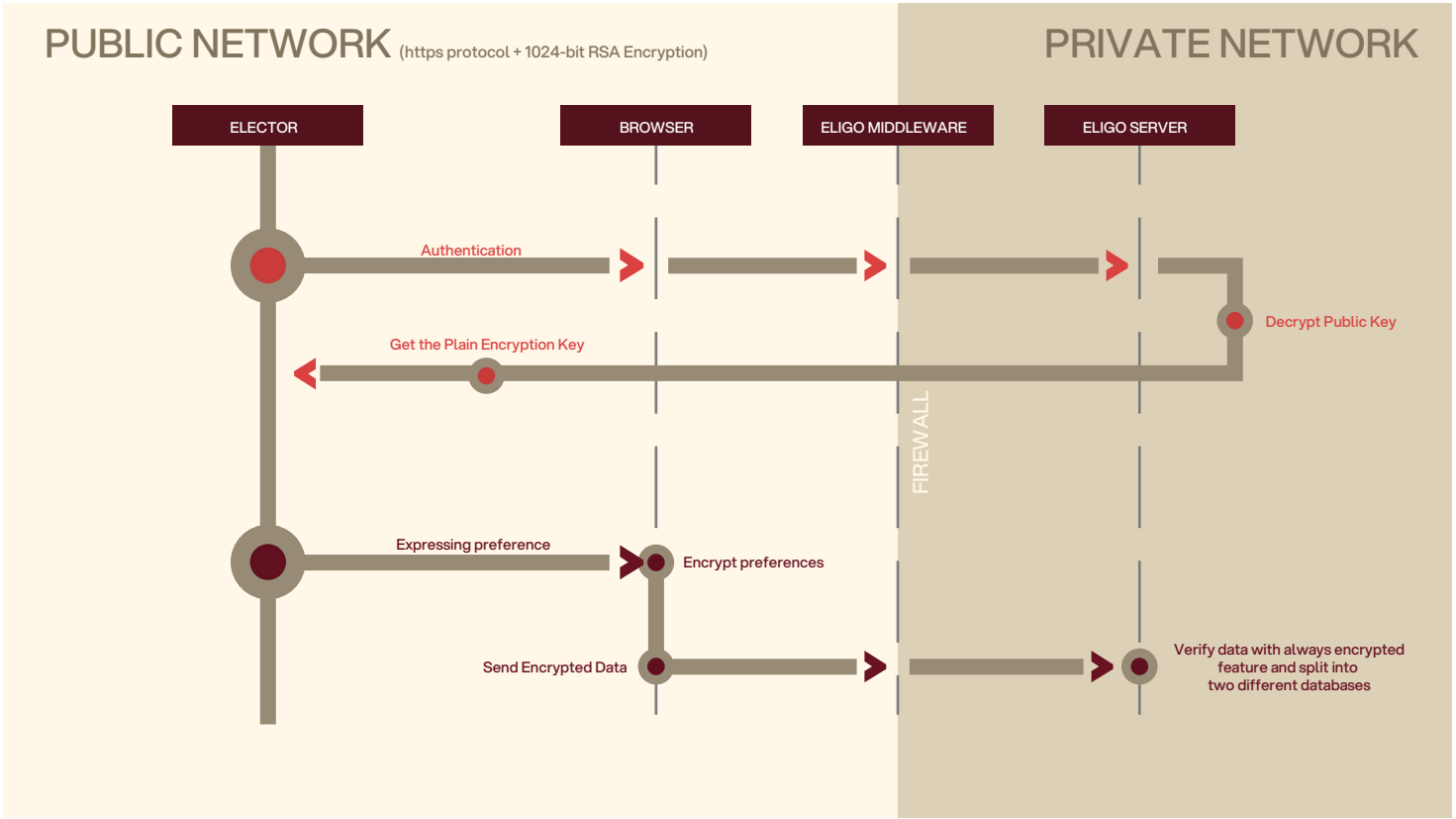
The Eligo voting and splitting process is the model on which the secrecy of the platform is based. Instead of protecting voting/voting information, it is immediately deleted without any physical and logical correlation.
Voting preference is a data that is totally anonymized and encrypted on the voting user's device (PC, mobile device, or physical seat).

Encryption is applied using asymmetric key encryption. Applying this model, the vote becomes secret even for the system itself. In no way, and in no part of the system, it is possible to reconstruct the link between voting preference and voting user.

E2E Encryption



Voting Preferences Anonymized



Uniqueness and Inalterability of the Vote

The Eligo secret voting system guarantees the uniqueness and inalterability of the voting preference. A voting user may express a single time each voting preference for which they are entitled. In addition to ensuring the complete anonymity of the voting preference (no link between the vote and the voter), the system records the voting happened.
It is therefore not possible for a voter to express several times, and then change, the same voting preference.

The system also provides a protection mechanism against simultaneous voting scenarios; it can happen, by mistake or a fraudulent attempt to alter a vote, that the credentials of a voting user are used simultaneously to express the same voting preference.

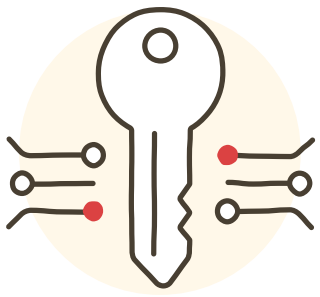
Eligo guarantees, through a distributed locking mechanism, that the process of expressing voting preference for a single user is mutually exclusive. In no way, by mistake or deliberately, a user can vote simultaneously from multiple locations or browser sessions.

Counting Process

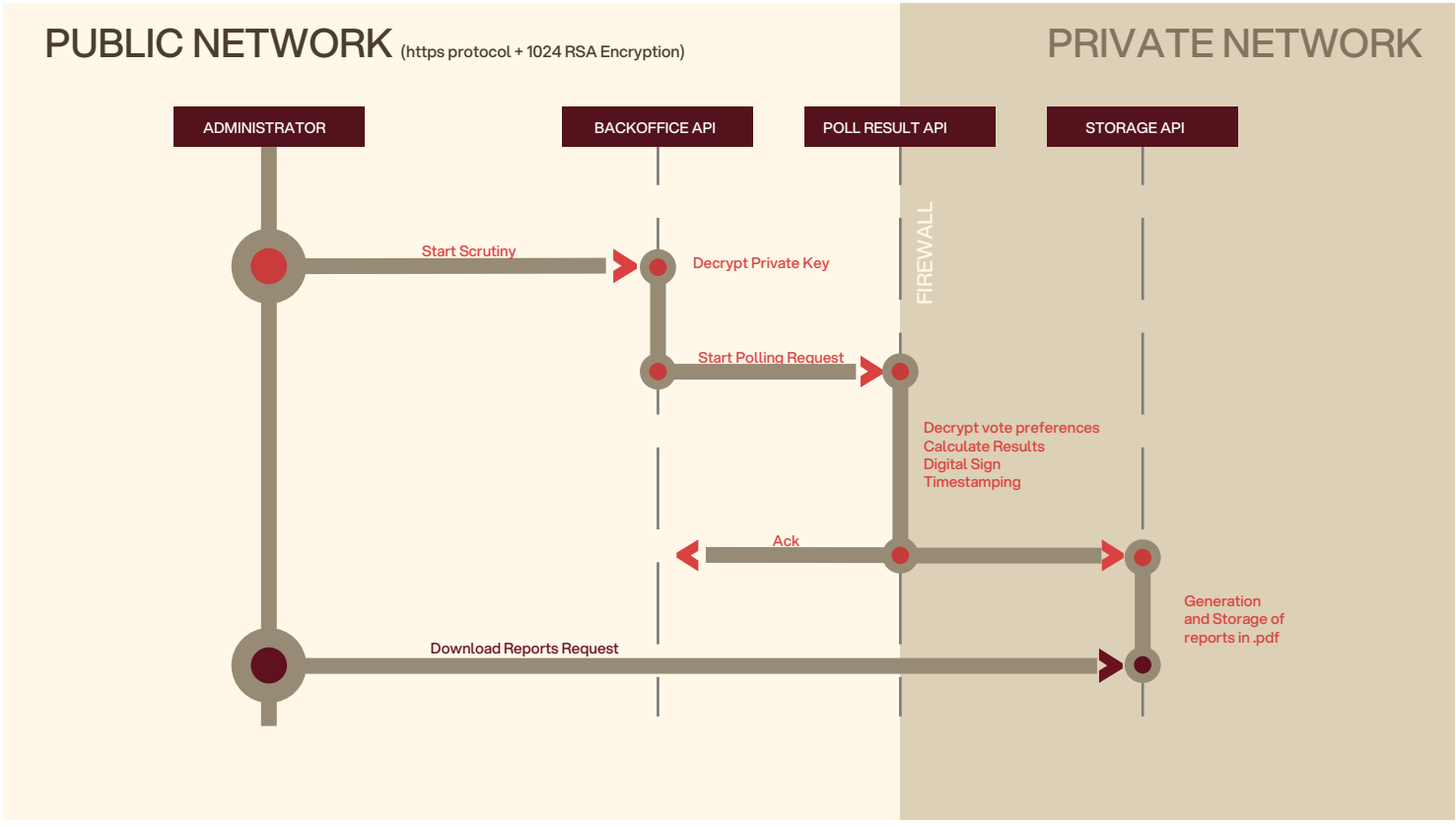
Digital counting flow, mode and management

A safe and reliable election result starts with an equally safe and reliable vote.
Eligo guarantees data security and confidentiality by applying the latest End to End asymmetric encryption techniques that make it impossible to decipher the voting preferences expressed. The system also guarantees that at no time during the election and in no case, fortuitous or fraudulent, a user can change his voting preference.

In addition, the ballot process is only carried out by a user with a private encryption key. Not even the service provider can carry out an independent scrutiny. The generated reports and their originality are identified and guaranteed by the affixing of valid digital signature and time stamp. Finally, this process leaves no "trace", as it does not use any intermediate database, and is repeatable at any time after the end of the election.



Signing and marking temporal



Certifications

Certified results and guarantees provided by the Eligo system

The ELIGO system has been certified by important third parties during its almost twenty years of existence on the market. In addition to these important entities, the platform undergoes regular penetration tests and vulnerability detection every two years and performed by relevant market players. From the point of view of information security and its management in the entire enterprise ecosystem, the developer IDTechnology and owner of the ELIGO platform, has achieved the ISO ISO 27001, 27017, 27018 e 9001 certifications in order to guarantee to its customers the highest quality and safety in the management of their data and their electoral voting event.

STRIPE OLT

Vulnerability Assessment e Penetration Test (2023)

ISO 27001:2022

ISO 27017:2015

ISO 27018:2019

Certifications

A vote of legal value

DATA PROTECTION AUTHORITY - 2011

In 2011, during the online voting of an important Social Security Fund, is
the intervention of the Guarantor of Privacy regarding the verification of the secrecy of the vote on the e-voting platform provided by IDTechnology srl. In force and according to the content of the then D.Lgs. 196/2003, the Guarantor for the protection of personal data expressed himself in the final measure of the investigation:

"the possible relationship between voters and expressed voting preferences is not recorded in any table, nor can be reconstructed from the information stored in the databases".
[...]" Electronic communication takes place through cryptographic protocols".
[...]"the measures described by ID Technology are considered appropriate to prevent direct identification
of the voters and of the votes cast, with the consequence that they can be considered as

COURT OF ROME - Sez. XVI - 2021

In 2021, the Judgment of the Ordinary Court of Rome on the adoption of the platform Eligo evoting:

"Documents have been filed [...] showing that the electronic voting platform set up by Eligo Evoting & Consulting is suitable to guarantee the personality, freedom and secrecy of the vote. [...] Moreover, the risk of possible password subtraction or possible accesses of "Hackers" in the electronic system is in the abstract possible, but it would be part of pathological hypotheses that can not be completely eliminated even in the case of a vote exclusively cataceous, as demonstrated by the cases of contests of electoral fraud even in electoral comptements of greater importance".

COURT OF ROME - Sez. I - 2014

In 2015, the Judgment of the Ordinary Court of Rome on the adoption of the platform Eligo evoting:

"A series of technological precautions have been prepared to prevent an incorrect or improper use of the vote and to offer the greatest guarantees of confidentiality, secrecy and freedom of expression of the vote".

Data security

PROTOCOL

All communication to and from the system uses the HTTPS protocol with valid SSL certificates. An additional layer of security is a 1024-bit RSA cryptographic algorithm.

IN TRANSIT

Voting preference data, as well as voter registration data, are encrypted at the application level; encryption keys are not known to the Database engine, nor to the cloud provider.

AT REST

An additional layer of security is applied to databases, backup and log files; Transparend Data Encryption (TDE) techniques are applied at the file level protecting the data contained in them from unauthorized access.