ENCRYPTION AND VOTING SECRECY

SECRECY OF THE VOTE?

At EVoting we have developed our **own voting software**, which allows us to constantly update, perfect and adapt our security measures to the requirements that arise.

ENCRYPTED VOTING

Cryptography is the system we use to ensure the **secrecy of the vote**. We work with asymmetric cryptography, a mathematical technique that transforms a readable message into an unreadable one. When the voter marks his or her preference, an encryption process "locks" the vote, transforming it into an unreadable message and ensuring the secrecy of its content.

When the voter passes the different control stages - being on the voter's list, not having voted before and having authenticated his or her identity - the encrypted vote is deposited in the ballot box.

TOTAL SECRECY OF THE VOTE

The use of the homomorphic algorithm allows us to add up the encrypted votes and obtain an encrypted result. Once the voting is finished, the sum of the votes is decrypted, without the votes being opened individually and without being able to know the option marked on each one. Thus, we maintain the secrecy of the vote.

In cryptographic language we speak of "keys" to denote the inputs that allow the algorithm to perform the required encryption and decryption. The cryptographic keys define the **encryption scheme**. There are two types of keys: a **public key**, which encrypts, and a **private key,** which decrypts.

The final sum of votes - the result - is decrypted using the private keys held by the Electoral Commission.

ELECTORAL COMMISSION COMPOSITION

In each vote, EVoting works directly with the Electoral Commission, Supreme Court or Election Qualifying Court that the organization has defined, according to its internal rules. The Electoral Commission is the **only counterpart of EVoting** during the process. In this way, we ensure transparency and respect for pre-established protocols.

GENERATION OF CRYPTOGRAPHIC KEYS

In the "key generation" ceremony - EVoting's own process - the **public and private cryptographic keys are created** in the presence of the Electoral Commission or a **Minister of Faith**. The private key is divided into several parts, according to the number of members of the Electoral Commission. These are not copies of a key, but small pieces of the same key.

The size of the keys depends on the number of options on a ballot. Votes with a higher number of options require larger keys.

Cryptographic keys are **unique for each ballot and have no copies**. If most of these bits of private key are lost, the ballot cannot be counted and the vote must be repeated.

The idea is that the private key - hence access to the voting results - is divided into several pieces and that each piece responds to a member of the Electoral Commission, thus ensuring that access to the results **does not depend on a single person.**

SCRUTINY

This ceremony is carried out with the members of the Electoral Commission. Once the individual encrypted votes have been added up, each **member of the Commission** hands over his or her part of the key, which is loaded to **decrypt the results** (equivalent to opening the ballot box).

A **simple majority** of the private key bits is required for this procedure.

As a **transparency measure**, the results are automatically published on the voting website, allowing the Electoral Commission and any voter to have immediate access to this information.