ASSEMBLY VOTING X

The Digital Polling Station

A fully-documented, End-to-End verifiable online voting system.

Assembly Voting

AN ELECTION RESULT BEYOND ANY DOUBT

In a democracy, it is the votes that count and the voters who decide. Whether it is a general election, a collective agreement ballots, or an election for a membership organisation or professional body, everyone expects a fair election and an election result that is beyond all doubt.

Trust in elections is based on compliance with the fundamental democratic principles of transparency, anonymity, shared responsibility and the ability to control all parts of the election. This applies not only at polling stations but also in digital elections.

Assembly Voting X provides you with a digital polling station, based on the same democratic principles and with the same high level of security as a physical polling station. Assembly Voting X is a secure digital polling station that is suitable for all types of elections.

Assembly Voting X gives you

An End-to-End (E2E) verifiable online voting system

All elements of the election before, during and after the voting can be checked and verified by independent parties.

A secure and fully-documented online voting system

A secure, mathematically-proven online voting system that deploys cryptographic algorithms to ensure full anonymity and integrity in the voting process.

An easy-to-use online voting system

A complete online voting system that can easily be set up to statutory requirements, and is also easy for voters, election officials and administrators to operate.

A financially viable online voting system

So far, this type of election technology has been financially and practically unfeasible for the majority of elections. Assembly Voting X makes the same high level security as in general elections available to all elections, no matter type of election, organisation or scale.

A COMPLETE ONLINE ELECTION SOLUTION

Assembly Voting X comes as a complete online election solution, in which all activities and processes are included and taken into account from start to finish. Based on experience from 4,000 legislative and statutory elections, Assembly Voting X is the optimisation of both technical and administrative solutions, brought together to provide a proven, secure, End-to-End verifiable electoral solution to accommodate the vast majority of needs.

Assembly Voting X can be supplemented by a number of other systems, which, in their different ways, can contribute to a proven secure and easy-to-use democratic electoral process. For example, we can provide candidate registration systems, support systems and election list systems. All our systems come with full service or self-service SaaS (Software as a Service), with the option of local hosting.

Assembly Voting systems and data management processes are documented in accordance with the ISAE3000 standard, ensuring that all processes are transparent and in full compliance with the EU General Data Protection Regulation.

Configuration options

Types of elections

- Candidate elections
- Candidate and list elections
- Referendums
- Collective agreement ballots
- Multiple ballots

Voting media

- PC and computer
- Tablet
- Smartphone
- Postal votes (hybrid elections)

Voting access

- Digital signatures: e.g. 3rd party authentication credentials
- Voting codes
- Voting codes and User ID

Voting principles

- Required number of votes
- Maximum number of votes
- Weighted votes
- Write-in votes (digital postal votes)
- Overwriting votes
- Ranking of votes

ABOUT ASSEMBLY VOTING

Assembly Voting was the first provider of electronic elections in Denmark (2001) and is today the market's most widely used provider of digital election solutions in Northern Europe.

Assembly Voting is based on the idea of strengthening democratic participation in society and associations, through the integration of fundamental democratic processes with documented secure and user-friendly technologies.

Assembly Voting provides mathematically proven and fully documented election solutions for ministries, municipalities, professional organisations, companies, associations, etc.

Primary systems

Assembly Voting X

The digital polling station - Proven secure online voting systems.

Assembly Conference Voting

System for "live" elections independent of physical presence.

Assembly Votes

Flexible and complete election solution for statutory and non-statutory elections.

Assembly Candidacy

Registration, validation and presentation of candidates.

Facts

- First digital legislative and statutory elections in Denmark (2001)
- 4,000+ elections
- 25 million+ voters
- 35,000+ candidate registrations
- Full service, partner and self-service solutions

For further information on our solution for your next election, please contact us

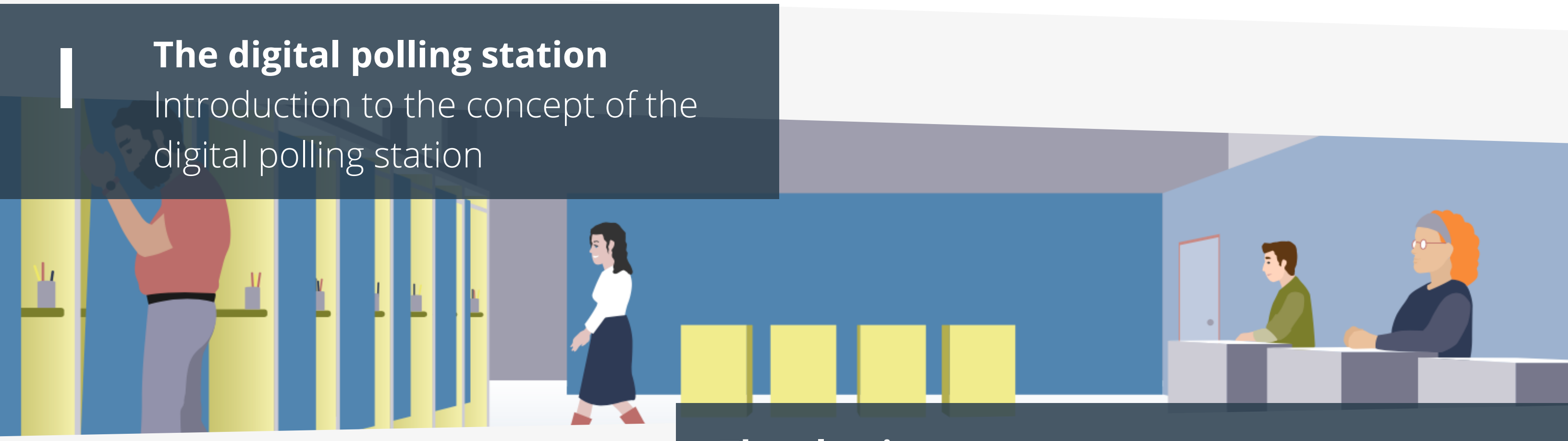
☎ +45 26 16 96 38

✉ sales@aion.dk

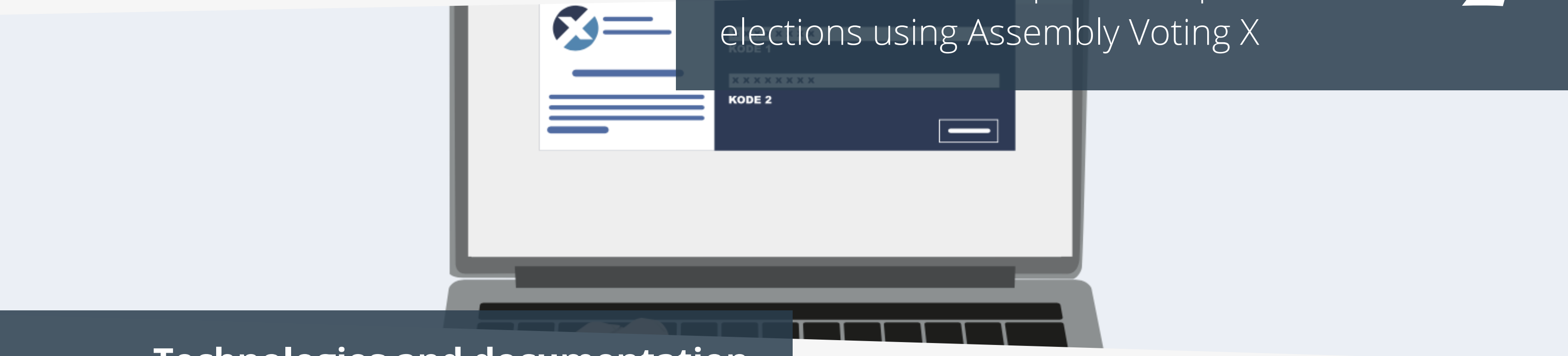
ASSEMBLY VOTING X

OVERVIEW

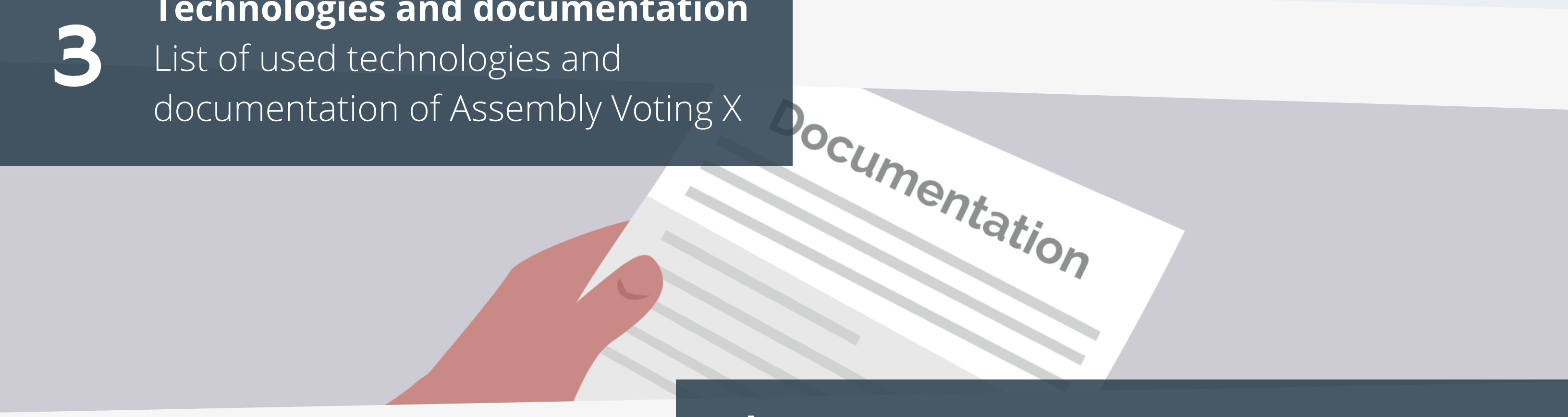
1 **The digital polling station**
Introduction to the concept of the digital polling station



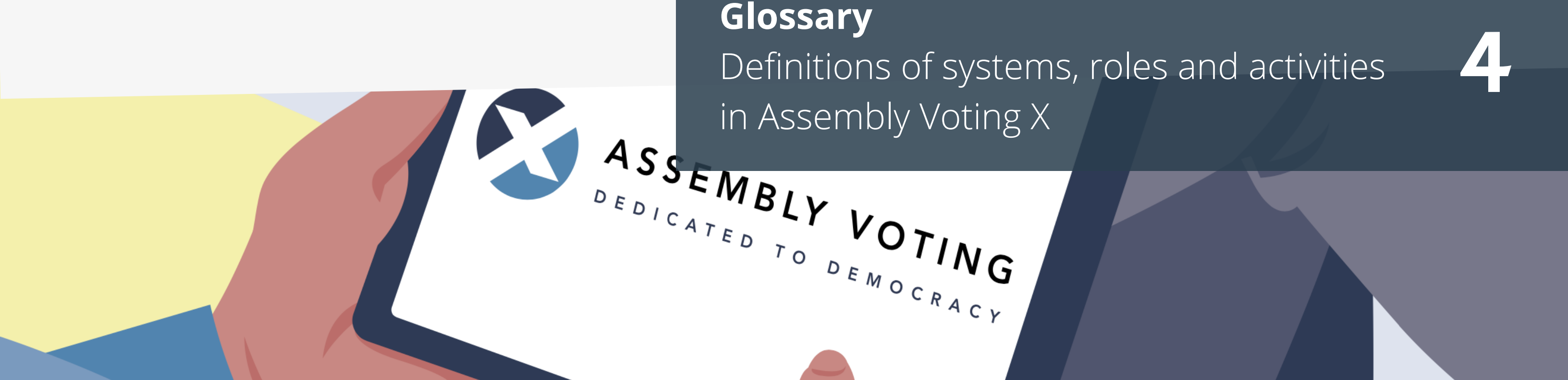
The election process **2**
Introduction to the practical operation of elections using Assembly Voting X



3 **Technologies and documentation**
List of used technologies and documentation of Assembly Voting X



Glossary **4**
Definitions of systems, roles and activities in Assembly Voting X



I. THE DIGITAL POLLING STATION

Assembly Voting X is built to comply with the same fundamental democratic principles as implemented in the physical polling stations for e.g. General Elections. This means that all parts of the electoral process, from start to finish, can be monitored and verified by election officials and independent external parties.

In the digital polling station, the polling booth, paper ballots and ballot box are replaced by advanced, mathematically proven encryption technologies. Assembly Voting X hereby ensures the voting secrecy and anonymity of the voters, and the system also provides evidence that only valid votes are included in the election result.

As in the physical polling station, trust in the Assembly Voting X electoral process is ensured through system design, shared responsibility and verification opportunities throughout the election process; not through uncontrollable trust in a system provider and individuals.

The success criterion is an election result beyond any doubt - no more and no less!

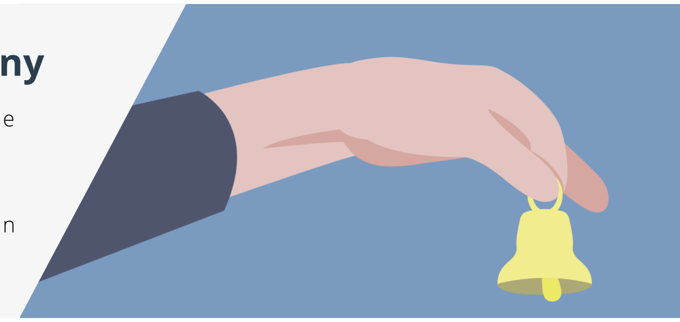
The digital polling station - Assembly Voting X

Pre-election activities: Setting up and preparing the election

This is a fully transparent process, which is documented for both setup of the solution and data management processes. The system does not contain any voting codes or other sensitive personal data that could be used for illicit voting. The setup within the system is documented and 'locked' after approval in the election opening ceremony.

Election opening: Election opening ceremony

Digital election officials check that the election setup complies with the statutory rules. An Election Control App is used by the key election officials to ensure that the 'digital ballot box' is sealed, so that results cannot be accessed during the election process. Only after the election opening ceremony is complete, the voting process can begin.



Right to vote: Personal voting cards

The voter is granted access to the online ballot via codes issued by two independent channels. There is the option, if required, of using a digital signature: e.g. a 3rd party authentication credential. An encryption algorithm allows codes to be sent to each individual voter with only a signature saved in the voting system. This means that the codes are never revealed to the voting system or the system provider.

Voting secrecy: Voting behind the curtain

The individual's vote is encrypted on his/her own local device in the browser. When cast, a cryptogram with voter ID and vote is submitted to the voting system. If the voter is in doubt, as to whether the vote cast has been properly encrypted, they can use a Ballot Opener App that can be downloaded from App Store or Google Play. The voting system makes it possible to overwrite your vote if you are subjected to voting pressure.

Ease of use: Manageable and easily accessible digital ballots

The electronic ballot paper makes it easy to assess the various electable candidates and options, and the vote itself is designed not to leave any doubt as to whom or what you have voted for. Unlike the paper ballot paper, the digital ballot paper is easily accessible to visually impaired and dyslexic voters.

Anonymity - Digital envelope with encrypted voice inside

The cast vote is submitted, received and stored in encrypted form. The principle is the same as with a physical postal vote, which contains an 'outer envelope' with voter ID and an 'inner envelope' with the vote cast. Encryption technology ensures that only validated vote encryption programs are included in the counting of results.

Vote integrity - Checking the ballot box

In the physical polling station, everyone can keep an eye on the ballot box throughout the election process. Similarly, in the digital polling station scenario, you can keep an eye on the digital ballot box. A publicly-available digital bulletin board, based on blockchain-inspired technology, serves as the ballot box. Here, the voters, the election officials, and other auditing parties can monitor the vote encryption programs received and other activities in the online voting system.

Election closing ceremony - Anonymisation of votes and generation of election result

When an authorised number of digital election officials have logged on to the Election Control Application, voter ID and vote are separated irreversibly from each other by a digital Mixer process. This process is conducted on the basis of several independent processes with proof that no votes have been removed, attributed or modified during the process. Only after anonymisation is complete, can the decryption of the votes be conducted.

Documentation - Full transparency before, during and after the election

There must be full documentation in an election. It must be possible to verify whether any activities have occurred, that may cast doubt on the outcome of the election. All technical parts in Assembly Voting X and system activities are fully documented. Moreover, the system technologies are based on open-source technology and verification protocols are made available for e.g. election officials, voters and external auditors to scrutinize the technology and election activities.

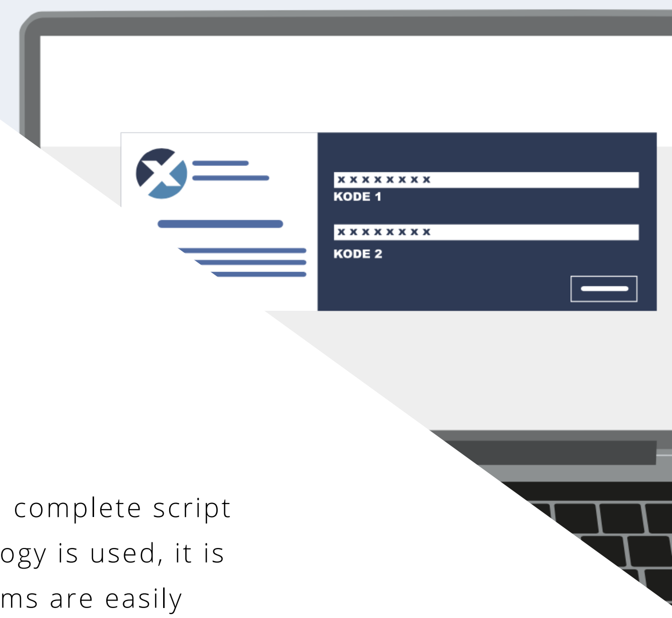
What is an End-to-End verifiable voting system?

A digital election solution, in which all parts of the electoral process can be checked and verified by election officials and independent parties. An End-to-End verifiable election system must provide 'trust by design' based on fully-documented and mathematically-proven system construction in order to ensure full voter anonymity and election integrity.

What is a black box voting system?

A voting solution, in which it is impossible for election officials or neutral parties to check all parts of the electoral process. It is based on 'uncontrollable trust' that system providers and election managers will not make mistakes or manipulate the electoral process.

2. THE ELECTION PROCESS



Assembly Voting X comes as a full-service solution with a complete script for all stages of the election. Although advanced technology is used, it is essential for the legitimacy of the election that the systems are easily accessible and user-friendly for the various stakeholders involved in the election (system administrators, election administrators, election officials, voters, and, if necessary, external auditors).

Based on experience from 4,000 legislative and statutory elections, the solution has been designed in a way, that all stakeholders can operate the different functions of the solution easily and securely. This reduces the risk of error and increase the efficiency in preparing and conducting elections.

Unlike printed ballot papers, time is not spent designing, printing and mailing ballot papers to voters. Instead, our standardised processes and systems are optimised, to be able to prepare and implement documented secure online elections even at short notice.

A complete election solution
- Assembly Voting X

Assembly Voting X performs the activities required for each election in a structured manner for the entire election process. The following pages provide an overview of the activities that usually feature in an Assembly Voting X operated election.

All systems and data management processes are fully documented and audited in accordance with the ISAE3000 standard.

Pre-election activities

Main activity	Sub-activities	Verification
Specification of requirements	Requirements for the election setup are specified on the basis of applicable laws and electoral rules. This includes use of Codes, digital signatures, digital election officials, etc.	• Specification of requirements is documented and verified by the election client
System setup	The voting system and any supplementary systems are set up in accordance with the specification of requirements.	• System admin validation • Log of all system activities
Election materials	Preparation of voting cards and supplementary electoral information for voters and election officials. Incl. required information.	• Verification of content by the election administrators • Verification of content by system operator
Data	A Data Protection Agreement (DPA) is prepared prior to uploading voter data and data on the election officials via a secure upload function (Assembly Files)	• Mutual approval of DPA • Log of activities in the on the bulletin board
Test	Election setup, data, election materials etc. are tested	• Verification by client and/or external audit
Voting code generation	Generation of one or more voting codes by one or more independent channels using a script function. An associated public signature is returned to the system administrator.	• Verification of signatures uploaded into the system
Upload of registered voters	Upload of registered voters to backend with associated public key.	• Verification of the number of registered voters by client and/or external audit
Election opening ceremony	Checking the election setup, distribution of encryption keys to election officials and inspection of the 'empty digital ballot box'. System lock of the approved setup.	• Verification via the Election Control App and the Bulletin board by the digital election officials

continues on the next page

Activities during the election

Main activity	Sub-activities	Verification
Distribution of polling cards	Independent channels provide voting codes to the voters in voting cards.	• Bounce report and opening rate report
Right to vote (eligibility)	Voters are validated by entering the code combination sent to them and/or by a 3. part authentication.	• Verification by signature authentication from codes distributed to voters
Checking digital vote in browser	Voters can verify that their vote is properly encrypted in the browser	• Verification via Ballot Opener App by voters
Checking registered vote	Voters can verify that their vote is properly registered in the 'digital ballot box' by uploading a vote receipt on the bulletin board	• Verification via upload of vote receipt by voters on the bulletin board

Post-election activities

Main activity	Sub-activities	Verification
Election closing ceremony	The election officials log on to the Election Control App. The mixing process (anonymisation of votes), decryption and generation of result is initiated when a sufficient number (a threshold) of digital election officials are conducting the election closing ceremony.	• Verification via proofs of valid ballots in the Election Control App by the election officials
Election result	The election officials approve the election result prior to announcement.	• Verification via Election Control App by the election officials
Documentation of the election	Full documentation of all activities on a publicly-available bulletin board. Control protocols available for (external) audit of election.	• Verification via control protocols by digital bulletin board
System documentation	Full documentation of the online voting system is available: technical design, mathematical evidence, open-source technologies and server setup.	• Verification via reviews and audits by independent auditing companies, academic institutions, NGOs and others

3. TECHNOLOGIES & DOCUMENTATION

Assembly Voting X is based on mathematically-proven algorithms and technologies. The technologies used are available for audit via open-source software. This ensures that all elements of the online voting system are fully documented and accessible to researchers, independent auditors, and other stakeholders.

Key technological components of Assembly Voting X

All technologies used are fully described and documented scientifically to ensure full documentation and transparency in the online voting system.These include:

- Discrete logarithm zero-knowledge proof
- Furukawa mixing proof
- SHA256 hash function
- Elliptic curve cryptography – secp256k1 curve
- Threshold cryptography based on ElGamal cryptosystem
- Schnorr digital signatures

Integrity

Integrity and control options in all elements of the electoral process constitute the cornerstone of a democratic election. Assembly Voting X ensures full integrity through individual and universal verification options: for example, for registered voters, election officials, independent auditors, observers etc.

Vote cast in the online voting system as desired

Individual verification: The system contains a mechanism (ballot opener app) that can prove that the digital vote has been properly registered in the cryptogram containing the vote.

Vote registered in online voting system as cast

Individual verification: A bulletin board, based on blockchain-inspired technology, logs all election activities in the system without exception. By uploading a ballot receipt in the bulletin board, the registered voter can verify that the vote has been properly registered and has not been edited or removed during the course of the election process.

Vote counted as registered

Universal verification: The voting counting process generates evidence documenting the correctness of the calculated election results. This means that the results of the election correspond to the content of all the encrypted votes received during the electoral process on the bulletin board.

System security

The online voting system is constructed to ensure anonymity and voting secrecy 'by design'. End-to-End encryption in the electoral process and mixing processes in the result statement, guarantee voters complete anonymity and voting secrecy throughout the electoral process.

Digital signature

A built-in, digital-signature-based 'login procedure' features a verification mechanism, which ensures that all votes cast originate from registered voters. In addition, the digital signature helps to ensure that votes cast cannot be tampered with during the election process.

End-to-End encryption

An encryption protocol ensures that, under no circumstances, is it possible to read parts of the result until the election process is complete and the election officials initiate the result ceremony with decryption of the votes.

Mix-net

The Mixing Protocol breaks any connection between the voter's identity and the vote cast, thereby ensuring full anonymity. The mixing process is organised by several independent parties and must be properly completed, before it is possible to initiate the decryption process of the registered votes.

Documentation

The components of the online voting system are based on mathematically-proven algorithms and technologies, that are available for impartial review. The documentation and use of open-source software form a key part of the universal verification of the online voting system.

Mathematical evidence

All the technologies and the system structure have been mathematically proven and reviewed by academic researchers.

Technical design

Detailed documentation showing the technical design of the Assembly Voting X solution.

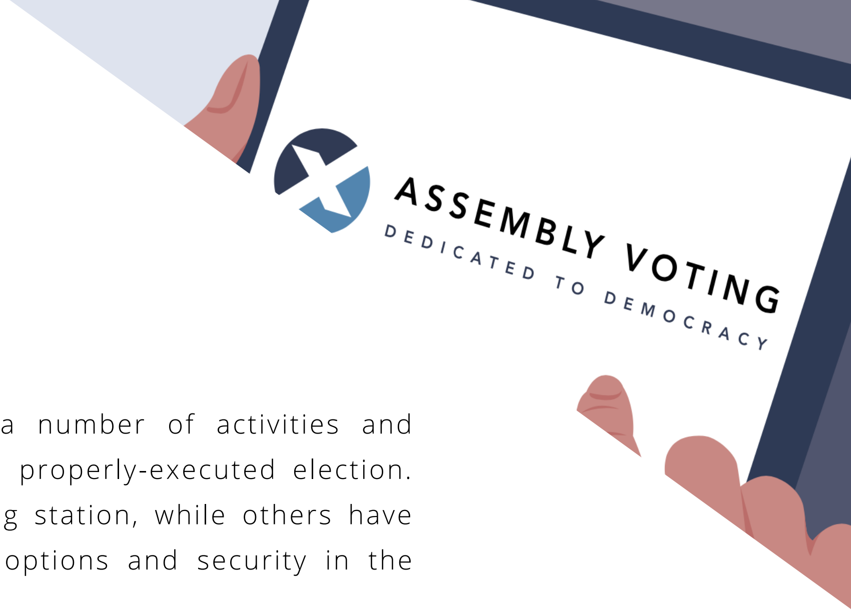
Open-source software

The open-source software used in Assembly Voting X is available for review on GitHub.

ISAE3000

ISAE3000 is used to review all systems and data management processes in Assembly Voting.

4. GLOSSARY



In the digital polling station there are a number of activities and features, each of which helps to ensure a properly-executed election. Some are familiar from the physical polling station, while others have been added to ensure the same control options and security in the digital polling station.

Ballot opener App

An app that can be downloaded from App Store or Google Play for voters to check the content of the vote encrypted in the online voting system

Bulletin board

All activities during the election are registered on the bulletin Board. The bulletin board is used for both the individual and universal verification of a properly conducted election.

Digital election administrator

A named administrator responsible for setting up the online voting system in accordance with election rules.

Digital election official

Authorises the election setup and seal the digital ballot box prior to the opening of the election.

Election Control App

The digital election officials use the Election Control application to conduct the opening and closing ceremonies of the election.

Election opening ceremony

Before the election opens, the digital election officials must conduct the election opening ceremony, in which they authorise the election setup and share decryption keys with each other so that no one has access to votes along the way.

Election result ceremony

Before the election result is calculated, the digital election officials must log on to the Election Control application. The mixing process, decryption of the votes and result generation then starts.

Individual verification

Functions of the online voting system that enable each voter to verify that the online voting system handles the cast vote correctly.

Mixing process

Technology for separating voter ID and vote prior to calculation of the election result.

Universal verification

Features and documentation that can be used for general supervision of the online voting system and the election: e.g. checking registrations on the bulletin board.

Vote receipt

A receipt received after registration of a vote. The receipt can be uploaded on the bulletin board to check that the vote has been properly registered.