

Guide

**Cast as intended -
Challenging the vote**

Introduction

Devices and systems can be compromised. A malicious actor can potentially embed code in the election system or on the voter's device that changes the vote without the user being aware. In other words, we cannot necessarily trust our devices.

Assembly Voting's election systems allow the voter to check the content of the encrypted vote on a secondary device. If there is a mismatch, it could be a sign that the election system is compromised.

Our voting system allows voters to challenge their vote as often, with as many devices as they feel necessary, to ensure that no part of the voting process has compromised their vote.

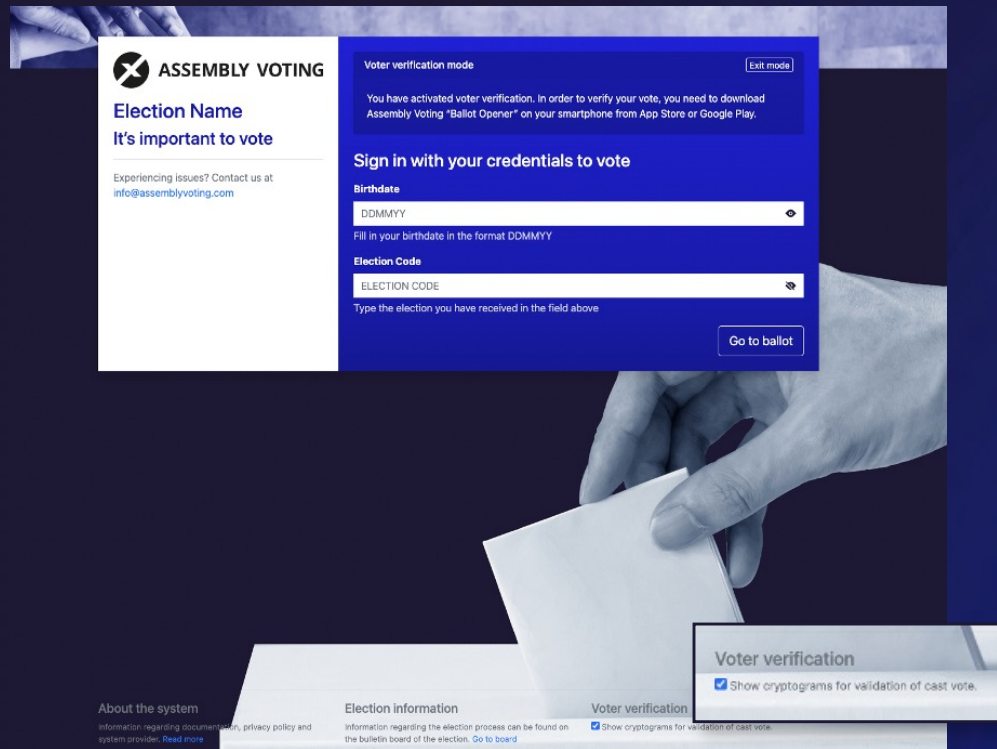
This means that the voter is able to open their envelope and view the vote before submitting it to the digital ballot box, as many times as they want, to give enough evidence that the vote inside the envelope matches, what the voter expected it to be.

Table of content

- 04** Enable Voter Verification mode
- 05** Encrypt your vote
- 06** Submit or challenge your vote
- 07** Challenge your vote
- 08** Resubmit your vote
- 09** Your receipt

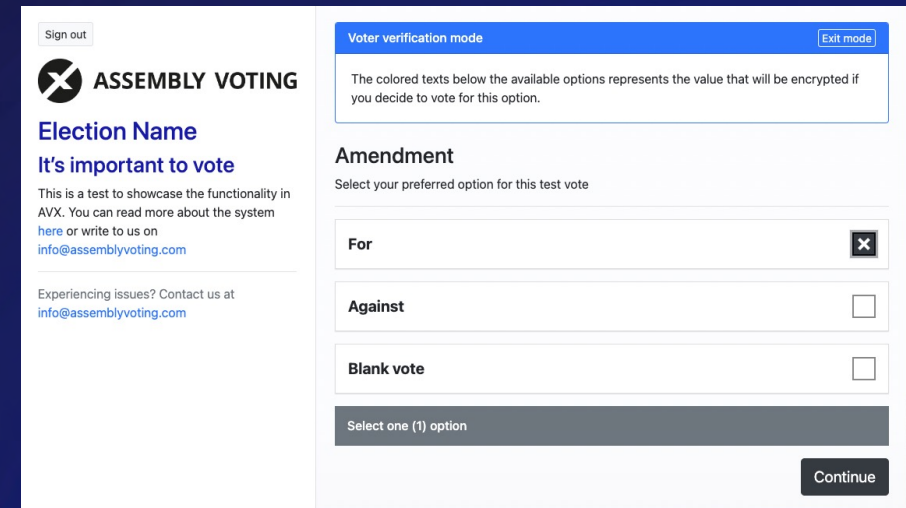
Enable Voter Verification mode

1. Turn on the voter verification mode on the election site. This functionality is shown at the bottom of the election site.



The voter verification allows you to check the content of the encrypted vote on another device through an application that can read and decrypt the vote you are about to submit.

2. Sign in to the election with your voter credentials.
3. Vote on the ballot(s) and click "Continue"



Encrypt your vote

The vote must be encrypted to ensure that it is cast anonymously and privately. This ensures that no one else can challenge and see the content of the vote.

1. Write down or memorize the colored text below the selected option (in this case, “yes”).
2. Continue to the next step by clicking “Encrypt vote”.

Sign out

ASSEMBLY VOTING

Election Name

It's important to vote

This is a test to showcase the functionality in AVX. You can read more about the system [here](#) or write to us on info@assemblyvoting.com

Experiencing issues? Contact us at info@assemblyvoting.com

Voter verification mode Exit mode

The colored text below the selected option represents the value that will be encrypted. It is also the value that you should see, if you decide to open your ballot for verification of its content.

Please confirm your vote

Amendment

For
yes

Back Encrypt vote

What do you mean by “encrypt vote”?

You can interchange encrypting your vote with the physical action of you putting the filled in ballot inside an envelope, so that the ballot and what you voted for is no longer visible to anyone.

Submit or challenge your vote

You can now either “Submit envelopes” if you are satisfied with your choice and trust the system to cast as intended or “Open envelopes” if you wish to challenge the vote to see whether the election system has registered and encrypted your vote correctly.

Voter verification mode Exit mode

This is your encrypted ballots.

If you want to verify the content that was encrypted by the system, you can click on “Open envelopes”. This verification ensures that the system is encrypting the casted votes as intended by the voter. After opening an envelope for verification of its content, you will need to recast your vote.

Submit or open your envelopes

Amendment

Envelope (Cryptogram)
0266b67260d39a41be1c48508e841459ef2d1ca80020bae554b6f45938757295ee
03dc8e9e1e3d37ab91cd649424e1e0c65b66fe9b8d20a243f5f013ce72a973b8e5

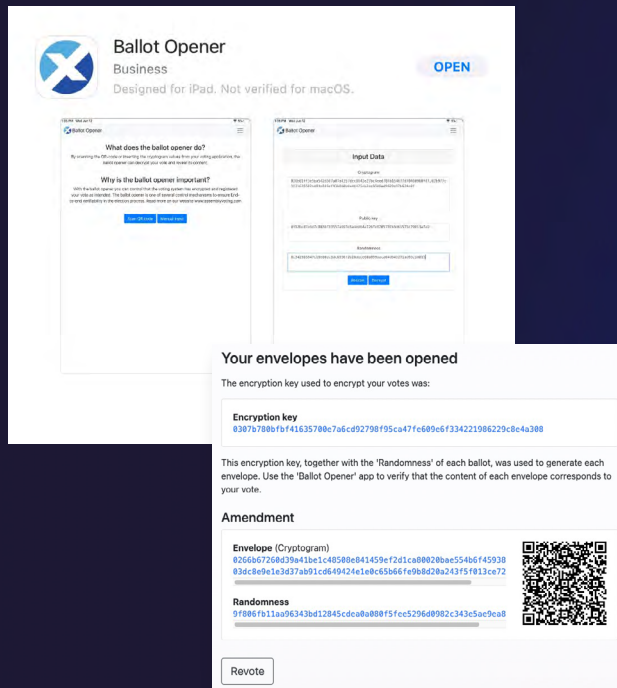
Open envelopes Submit envelopes

Challenge your vote

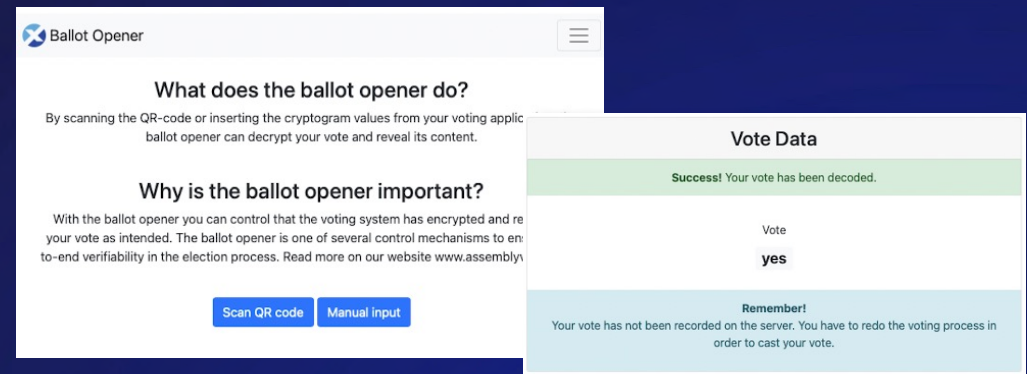
Challenging the vote will require you to vote again because once the vote has been decrypted and spoiled, it becomes invalid.

1. Download the Ballot Opener app. Download it from either the Google store or the App store to another device.

2. Click on "Open envelopes," which will display an encryption key and a QR code. The "encryption key" is a public piece of information used by all voters to encrypt the vote together with the "private randomness." This together generates the envelope, which is the value submitted as the vote.



3. Either scan the QR code or input the value manually in the ballot opener app. Then verify that the value contained in the vote is, in fact, the value you voted for (in this example, "yes").



Envelope (Cryptogram) - This value is the encrypted vote. The ballot has now been put inside the envelope and the cryptogram is the envelope hiding your vote.

Encryption key - This is a unique value that is used to identify the election system. This is a public piece of information that can be found on the election board.

Randomness - This value is the voter's unique way of putting the ballot inside the envelope. This is a secret

information that is only revealed to the voter, to ensure they can challenge the vote before submitting it. Once the voter chooses to submit the vote this information will be deleted.

QR code - The Encryption key, Envelope cryptogram, and Randomness cryptogram have been generated into a QR code, that can be scanned by a device with access to open the Ballot Opener application, which the voter will need to install to continue the process of decrypting the vote.

Resubmit your vote

After challenging your vote, you must resubmit an unchallenged vote because the process of challenging the vote spoils the original vote. A new, unchallenged vote ensures the privacy and anonymity of your vote.

1. Click on "Revote" to resubmit your vote.

Voter verification mode Exit mode

Use the Ballot Opener app to scan the QR-code of each envelope. You can also insert the cryptographic values in the application to reveal the content of your ballot.

If the content of the envelope is identical with the vote you casted for, it means the system correctly encrypted your vote. Otherwise, it is an evidence that the system has been corrupted. In such case, please contact support.

Please note: These votes will NOT be included in the result. You have to vote again!

Your envelopes have been opened

The encryption key used to encrypt your votes was:


Encryption key
0307b780bf41635700e7a6cd92798f95ca47fe609e6f334221986229c8e4a308

This encryption key, together with the 'Randomness' of each ballot, was used to generate each envelope. Use the 'Ballot Opener' app to verify that the content of each envelope corresponds to your vote.

Amendment

Envelope (Cryptogram)
0266b67260d39a41be1c48508e841459ef2d1ca80020bae554b6f4593803dc8e9e1e3d37ab91cd649424e1e0c65b66fe9b8d20a243f5f013ce72

Randomness
9f806fb11aa96343bd12845cdea0a080f5fee5296d0982c343e5ae9ea8



Revote

2. Vote on the ballot once more and click "Continue" and "Encrypt vote."

Voter verification mode Exit mode

The colored texts below the available options represents the value that will be encrypted if you decide to vote for this option.

Amendment

Select your preferred option for this test vote

For

Against

Blank vote

Select one (1) option

Continue

Voter verification mode Exit mode

The colored text below the selected option represents the value that will be encrypted. It is also the value that you should see, if you decide to open your ballot for verification of its content.

Please confirm your vote

Amendment

For
yes

Back Encrypt vote

3. You can now choose to rechallenge your vote (follow the previous steps) or submit your final vote.

Voter verification mode Exit mode

This is your encrypted ballots.

If you want to verify the content that was encrypted by the system, you can click on "Open envelopes". This verification ensures that the system is encrypting the casted votes as intended by the voter. After opening an envelope for verification of its content, you will need to recast your vote.

Submit or open your envelopes

Amendment

Envelope (Cryptogram)
0266b67260d39a41be1c48508e841459ef2d1ca80020bae554b6f45938757295ee03dc8e9e1e3d37ab91cd649424e1e0c65b66fe9b8d20a243f5f013ce72a973b8e5

Open envelopes Submit envelopes

Your receipt

Once you submit the envelopes, your vote is registered, and you can download the receipt file.

1. Download the receipt and save it somewhere safe for later. It includes cryptographic information about your submission and will allow you to follow up on the status of your submission later on.

Receipt

Your vote has been registered. Thank you for your participation.

[Download receipt file](#)

Your envelopes

Amendment

Envelope (Cryptogram)
039e1c6f698d8e7f61f8eea7051a5649e0c20c26935830b7bce2662ee3d62d0082
02a9a0d31fb5df87d15fc8da4390ecc61bbd99387a483073532a600a81d38c5d3

These were signed with your public signing key and sent to the server:

Voter's public signing key 033c7f8e5c1df6449edda85d863394e61e81f49fb47798dc04adace58a721	Acknowledgement and registration The server acknowledged your submission, registered it and sent back a server signature as a proof of registration.
Voter signature 1639c7da4a82a3d83e81ee7591abc9474bac8de89ad1526268696d128b01f8986a6fc97415f84663256181d589e6d950e87c287bbc496d61d3e85f6f1	Board hash at acknowledgment time - 2022-10-13T09:31:01.183+02:00 2ddffc03603ecfeb3f6a7680fd731cb68a853a4bd40754431f2390dd7eeba1
	Board hash at registration time - 2022-10-13T07:31:01.236+00:00 2ddffc03603ecfeb3f6a7680fd731cb68a853a4bd40754431f2390dd7eeba1
	Board hash after submission registered 3c778a069364d7aeb581fc304f0768387ec73ba3eb709133e1234a570f72b2ed
	Election's public signing key 027673214d7b308d0e3ff6bdeab763ef4b6b0e54421d0148031791f0fd800b836b
	Server signature 2a3976019d40a9bd0afce33abb837fdc4c06922569aa16dd7f131b8f7824fac4e0fe99cc10dec557ad95323fea180dc1187cd3c1d310b71606f30ff170e948e2

[Back to sign in](#) [Finish](#)

2. Click on "Finish" to terminate the login session.

What does it mean?

Envelope (Cryptogram) - This value is the encrypted envelope holding the vote.

Voter's Public signing key - This is a public piece of information that allows anyone to verify that it was actually this eligible voter who submitted the vote.

Voter signature - This is the signature the eligible voter sent in with the vote.

Board Hash at acknowledgment time - Information about the digital ballot box at the moment the vote was acknowledged.

Board hash at registration time - Information about the digital ballot box at the moment the vote was registered.

Board hash after submission registered - Information about the digital ballot box after the vote submission was registered.

Election's public signing key - This is a public piece of information that allows anyone to verify that the receipt was signed by the election system.

Server signature - The election board's signature that it has received the vote.



Assembly Voting was the first provider of statutory digital elections in Denmark (2001). Today we are the most widely used supplier of digital election solutions in Scandinavia. 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.