



ZEUS

ZEUS

Election Administrator

Manual

December 21st, 2016

Introduction

Zeus is a web-based e-voting platform for conducting verifiable elections in which votes remain confidential and anonymous. All election-related operations, from election setup and configuration by the election organizers to vote submission by voters, are performed remotely over a network connection to the internet.

Voters can access Zeus using a web-browser. The exchange of information is protected by mechanisms similar to those applied to online financial transactions. Voters can submit their votes within the specified time-period and receive a digital vote receipt.

The integrity of the election results is mathematically verifiable through cryptographic methods, without breaching vote confidentiality.

In this document we describe in detail all necessary information for an election administrator (hereafter the admin) to set up, configure and support an online election using “Zeus”. Although primarily addressed to election administrators and the members of the election committee, this manual may also prove useful for voters, as it provides an in-depth understanding of the overall process.



Overview

1. Election Setup and Configuration.

-  [Specifying basic election info](#)
-  [Setting up a ballot](#)
-  [Importing voters](#)
-  [Generating Trustee Keys](#)
-  [Finalizing the election](#)
-  [Sending e-mail invitations to voters](#)

2. Voting Period.

-  [Monitoring the voting process](#)

3. Election End – Results.

-  [Poll closing](#)
-  [Mixing and decrypting ballots](#)
-  [Counting ballots and exporting results](#)



1. Election Setup and Configuration

Specifying basic election info

The admin logs into the Zeus admin web application using the credentials provided by the Zeus platform administrator. Initially, the admin is asked to fill in some basic information regarding the election to be created:

- ✚ **Election type.** In order to create an approval voting election, the user chooses “Single transferable vote election” (Figure 1).

Elections list Create election

To create a new election, enter the necessary information below.

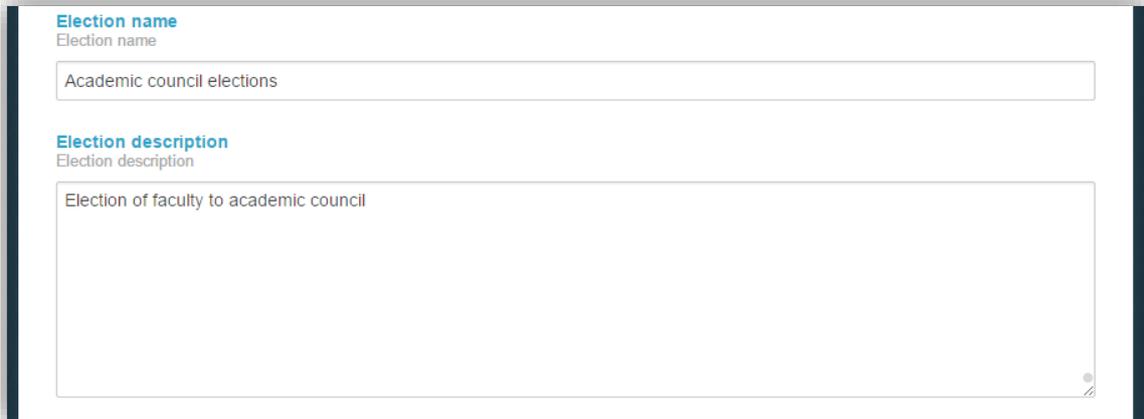
Trial election
This is a trial election

Election type
Choose the type of the election
Single transferable vote election ▼

Figure 1. Election type

Note that the admin may choose to create a trial election in order to get familiar with “Zeus” by selecting the corresponding checkbox (Figure 1).

- ✚ The election’s name and a short description of the election’s topic (Figure 2).

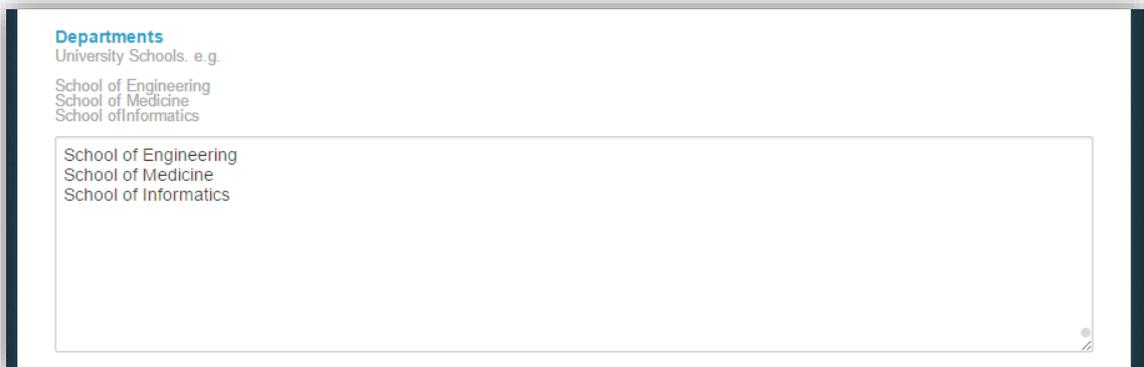


Election name
Election name
Academic council elections

Election description
Election description
Election of faculty to academic council

Figure 2. Election name & description

 The departments of the Institution that conducts the election (Figure 3).



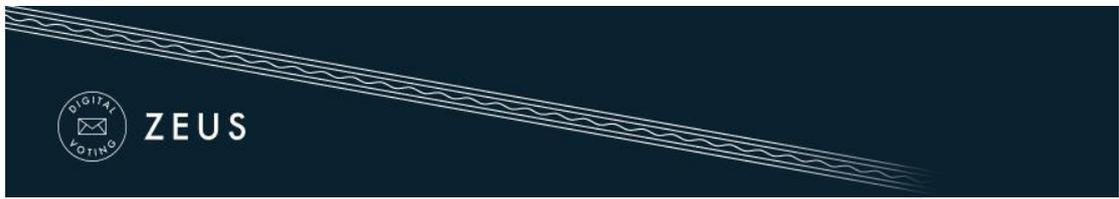
Departments
University Schools. e.g.
School of Engineering
School of Medicine
School of Informatics

School of Engineering
School of Medicine
School of Informatics

Figure 3. Departments of Institution

 The starting and ending date and time of the voting period. The Zeus voting web application will allow votes to be submitted only during the time-period specified by these fields (Figure 4).¹

¹ If necessary, the election organizers may decide to prolong the voting period at a later time.



Voting starts at
When voting starts

2016-11-17 12:00 ▼

Voting ends at
When voting ends

2016-11-18 12:00 ▼

Figure 4. Voting starting & ending date

- Information about the members of the election committee (trustees). The required data are the member’s full name and e-mail address, as shown in (Figure 5). Upon this form (see below), every member of the election committee will receive an e-mail message with instructions on generating their Trustee Key.

Trustees
Trustees list. e.g.,

Helen Jones, hjones@email.com
John Smith, jsmith79@gmail.com

David Connor, dconnor@hotmail.com
Helen Jones, hjones@email.com
John Smith, jsmith79@gmail.com

Support email
Voters can contact this email for election support

ac_elections@gmail.com

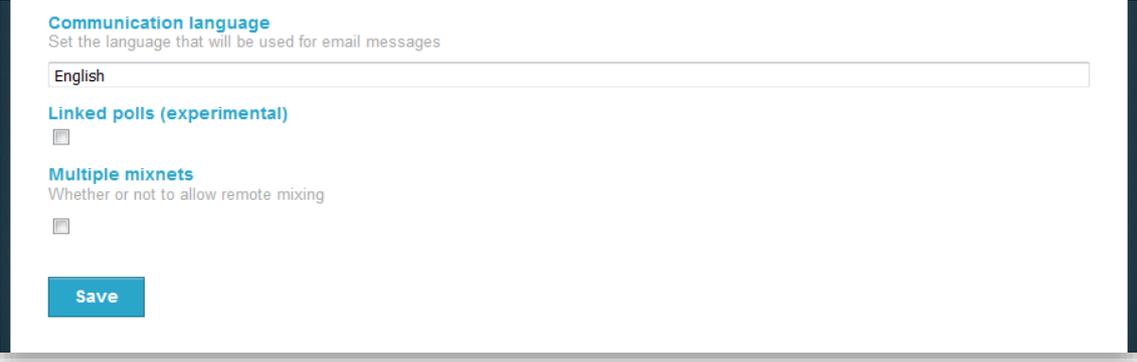
Support phone
Voters can contact this phone for election support

213-123 4567

Figure 5. Trustees & voters’ support data

- An e-mail address and a telephone number where the voters may contact for clarifications and support (Figure 5).
- The communication language that will be used for the voters’ e-mails (Figure 6).

- Optional activation of multiple mixnets. By enabling this option, the host organization will be required to implement external ballot mixing stages that will take place after the polls have closed. The election organizers are exclusively responsible for providing, administering and configuring the hardware and software infrastructure these extra mixing stages will run on. (Figure 6).



Communication language
Set the language that will be used for email messages

English

Linked polls (experimental)

Multiple mixnets
Whether or not to allow remote mixing

Save

Figure 6. Saving election info

Finally, after filling in the fields described above, the user may click the “Save” button, in order to create the election and move on to the next steps of the election setup process (Figure 6). At any time before the election finalization (see below), the admin is able to return here and modify this info by clicking the “Edit election” tab.

Setting up a ballot

After the election is saved, the user will be transferred in “Polls” tab where he/she should add a poll (Figure 7). Optionally the admin may select to add a 2nd step/factor for voter authentication.

Edit election
Election admin actions
Polls
Trustees list

Poll name

2-factor authentication

Optionally select 2-factor voter authentication

Shibboleth login

Oauth2 login

JWT login

Cancel
Save

Figure 7. Adding a new poll

Note that the user can add more polls by clicking on “Add poll” (Figure 8).

Edit election
Election admin actions
Polls
Trustees list

Name	Status	Ballot Size	Voters Registered	Voters Invited	Voters Voted	Select Action
Faculty to Academic council election	No questions set	0	0	0	0	Actions ▼
Totals			0	0	0	

Add poll

Figure 8. Managing Polls

Subsequently, the admin should set up the digital ballot, by clicking on either the icon on the “Ballot Size” column or the “Actions” button and then the “Manage questions” option (Figure 8). The admin should then enter the number of open positions (“Eligibles count”) as well as the possible choices (Candidates) along with their constituencies. The admin may optionally set a limit of open positions per constituency by clicking on the appropriate checkbox and filling the field “Constituency limit” with the maximum number of open positions per constituency (Figure 9).

Edit poll Voters **Ballot**

Candidates List 1

Eligibles count
Number of open positions

Limit elected per constituency
Enable limit of open positions per constituency

Constituency limit
Set the maximum number of open positions per constituency

Candidate 1
Andrew Keller School of Engineer **X**

Candidate 2
Ben Fine School of Medicir **X**

+

Save

Figure 9. Create ballot

To add more options (candidates), the user clicks on the green “+” in the bottom of the page. In order to remove an option (candidate), the admin clicks on the red “x” next to the corresponding answer (Figure 10).

Candidate 1
 School of Engineer ▼ ✕

Candidate 2
 School of Medicir ▼ ✕

Candidate 3
 School of Engineer ▼ ✕

+

Figure 10. Add/remove candidates

After completing the ballot creation, the user can save the changes by clicking the “Save” button and proceed to the next step.

Importing voters

In this step, the admin will have to import the voters. The user should move to the “Voters” tab, click on the “Voter list actions” button and then select the “Import voters” choice (Figure 11).

Edit poll
Voters
Ballot

Total voters count: 0
Votes cast: 0

Filter:

Voter list actions ▼

- + Import voters
- ↓ Export voter list to CSV
- ✕ Delete all voters

Registration ID	Email	Surname	Given name	Middle name	Mobile phone	Has voted	Booth invitation sent at	Last visit	Actions
No voters added									

Figure 11. Import voters

Voters are mass imported into the system (Figure 12) by uploading a CSV file (comma-separated values file) in the appropriate format. The required fields for each voter are the registration number, a personal e-mail address, first name and last name. Optionally, the middle name and a personal mobile phone number may be specified as well.

This file, which is basically a specially formatted plain-text file, should contain all voter-specific data as follows:

- Each line should contain all necessary data regarding a single voter.
- The values on each line correspond to the following fields (in this order):
 - Registration number, e-mail, first name, last name, middle name, phone number
- Values on a single line are separated by a comma (“,”).

The user selects the CSV file, which must have been already created and saved on the user’s hard-drive, and sets the proper encoding. Subsequently, the user clicks the “Upload file” button (Figure 12).

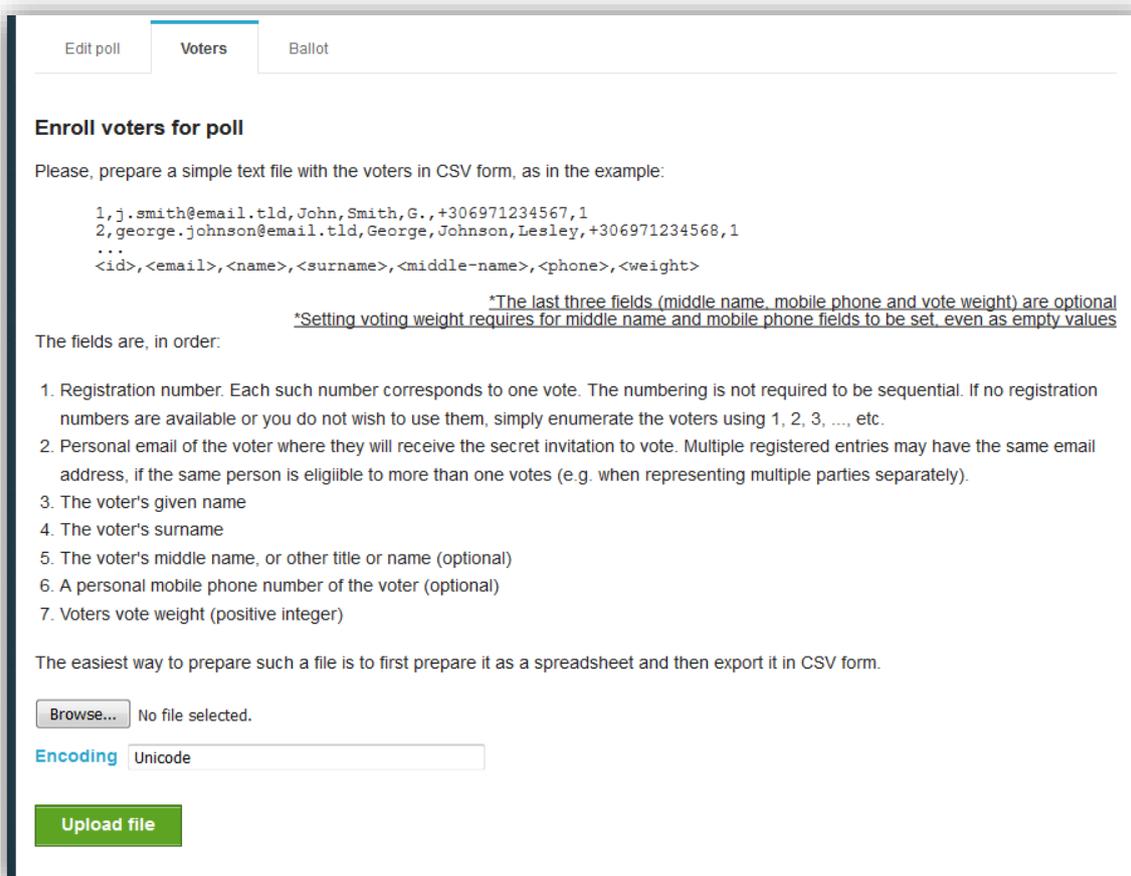
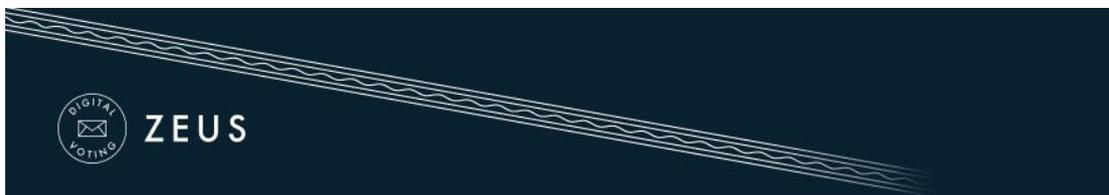


Figure 12. Mass voters’ import



The CSV file will be parsed by the Zeus server and the list of voters will appear. After verifying the accuracy of the extracted data (Figure 13), the admin confirms the validity of the imported voters.

Figure 13 shows a screenshot of the Zeus interface for confirming voters. It features a navigation bar with 'Edit poll', 'Voters', and 'Ballot' tabs. The 'Voters' tab is active, displaying a 'Bulk upload voters' section. Below this, a message states 'There were 3 entries read from the uploaded file.' A table lists the imported voters with columns for Registration ID, Email, Given name, Surname, Middle or other name, Mobile phone, and Vote weight. At the bottom, there are two buttons: 'Confirm voters' (green) and 'Cancel voter enrollment' (red).

Registration ID	Email	Given name	Surname	Middle or other name	Mobile phone	Vote weight
1	j.smith@email.tld	John	Smith	G.	+306971234567	1
2	george.johnson@email.tld	George	Johnson	Lesley	+306971234568	1
3	billy.t@email.tld	Bill	taylor	L.	+30698765432	1

Figure 13. Confirm voters

The user is redirected then to the “Voters” tab (Figure 14). From this tab the admin can view the detailed voters’ data and perform mass actions (send e-mail to voters, re-import voters, export voters list and delete all voters). The user may also perform actions on specific/individual voters (send e-mail, search for voter, delete voter).

Edit poll
Voters
Ballot

Total voters count: 3
Votes cast: 0

Filter:

✓
✕

Registration ID	Email	Surname	Given name	Middle name	Mobile phone	Has voted	Booth invitation sent at	Visit	
3	billy.t@email.tld	taylor	Bill	L.	+30698765432	NO	None	None	Voter actions
2	george.johnson@email.tld	Johnson	George	Lesley	+306971234568	NO	None	None	Voter actions
1	j.smith@email.tld	Smith	John	G.	+306971234567	NO	None	None	Voter actions

Voter list actions ▾

- + Import voters
- ✉ Send voters email
- ↓ Export voter list to CSV
- ✖ Delete all voters

Figure 14. List of voters and related operations

Generating Trustee Keys

The last step before the finalization of the election is the generation of the Trustee Keys by the members of the election committee. These keys will be used for the encryption of ballots and the decryption of their anonymized content in order to determine the final result.²

² Losing any of the Trustee Keys after finalizing the election makes it impossible to decrypt the ballots and determine the result of the election. Each member of the election committee is responsible for safe-keeping his/her Trustee Key.

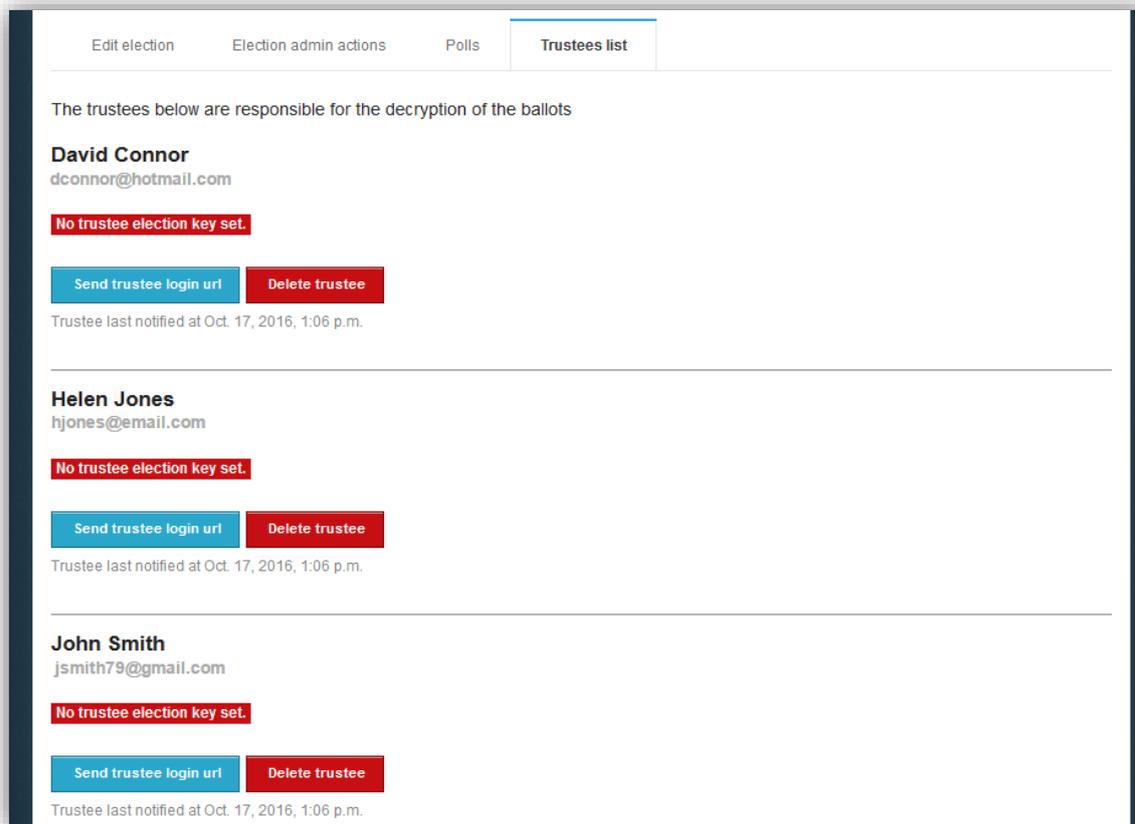


Figure 15. The “Trustees list” tab

Through the “Trustees list” tab the admin can monitor the progress of the key generation process for each trustee (Figure 15). From there, the user may resend to a trustee the e-mail message with the login url or even remove a member from the election committee in case of an error.³

When an election is created, every member of the election committee automatically receives an e-mail message with instructions on how to generate their Trustee Key (Figure 16). This message contains a personal, unique link for each trustee (Figure 16). The trustee should click on this link in order to create his/her Trustee Key.

³ Members of the election committee cannot be removed after the finalization of the election.

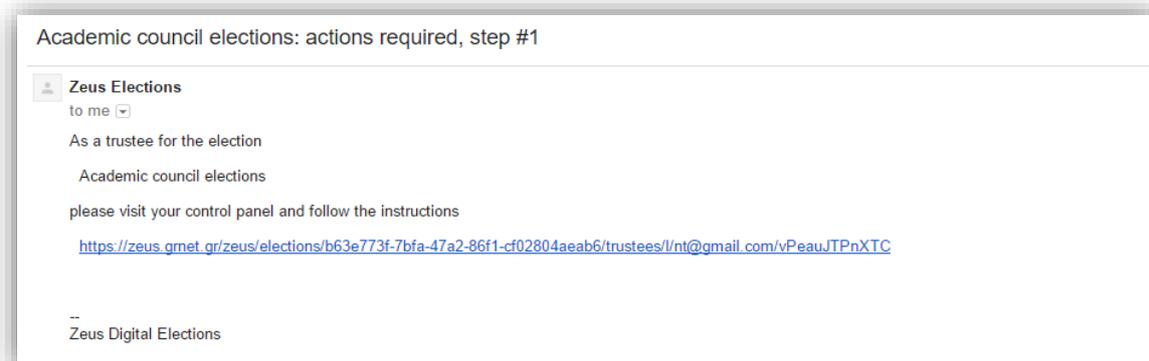
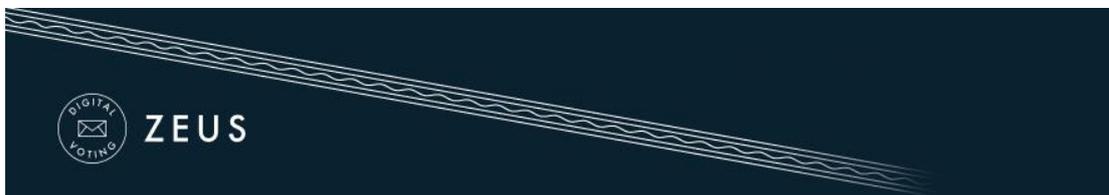


Figure 16. E-mail sent to Trustee

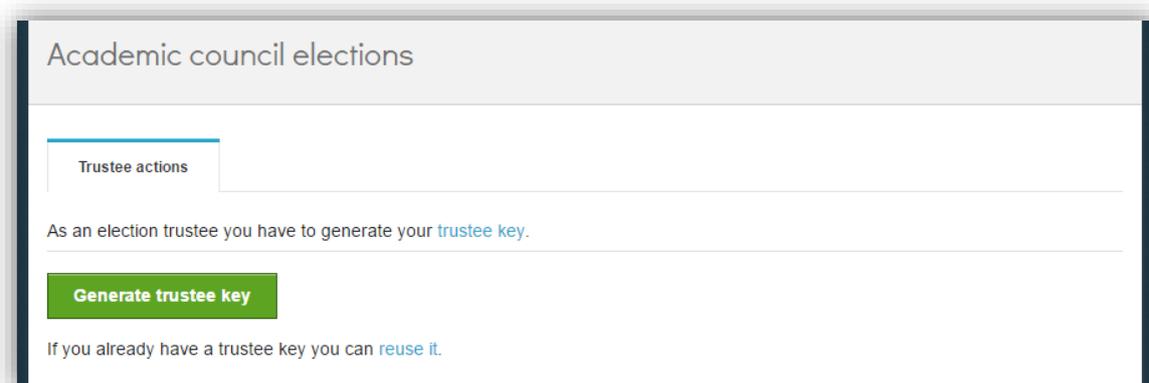


Figure 17. Trustee Key generation

By clicking the button “Generate trustee key”, a Trustee Key is generated in the user’s web browser automatically (without any involvement of the Zeus server). The user is asked to save the Trustee Key locally (e.g. on his/her personal computer’s hard-drive, on a portable storage device, etc.) by clicking the “Save your trustee key” button (Figure 18). This file must be kept safe and confidential until the election’s closing, since it is required for the decryption of the anonymized ballots and the review of any ballot challenges.

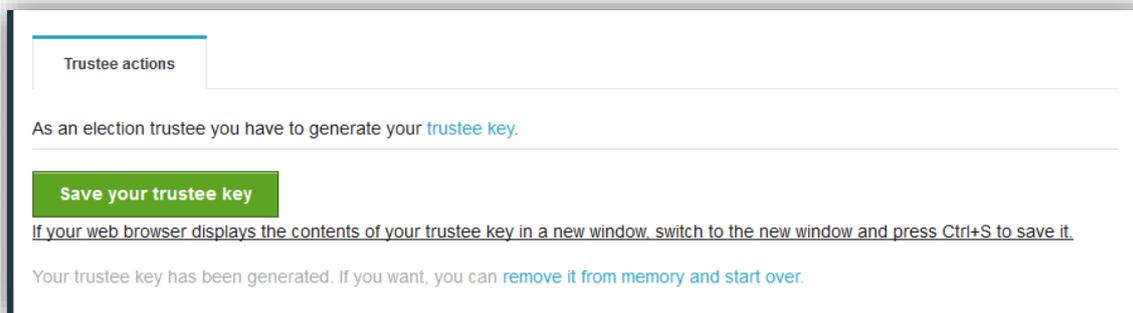
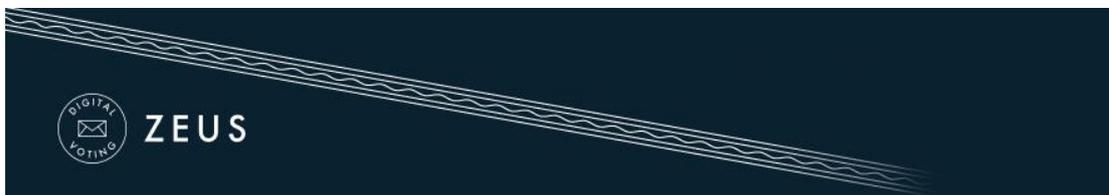


Figure 18. Trustee Key storage

After ensuring the Trustee Key is safely stored, the user may proceed to activate it by clicking the “Activate trustee key” button (Figure 19). At this point, the public part of the Trustee Key is sent to Zeus in order to be used in the encryption of ballots. The private part of the Trustee Key, which is contained **only** in the local file saved by the user, will be required later on, at the ballot decryption stage.

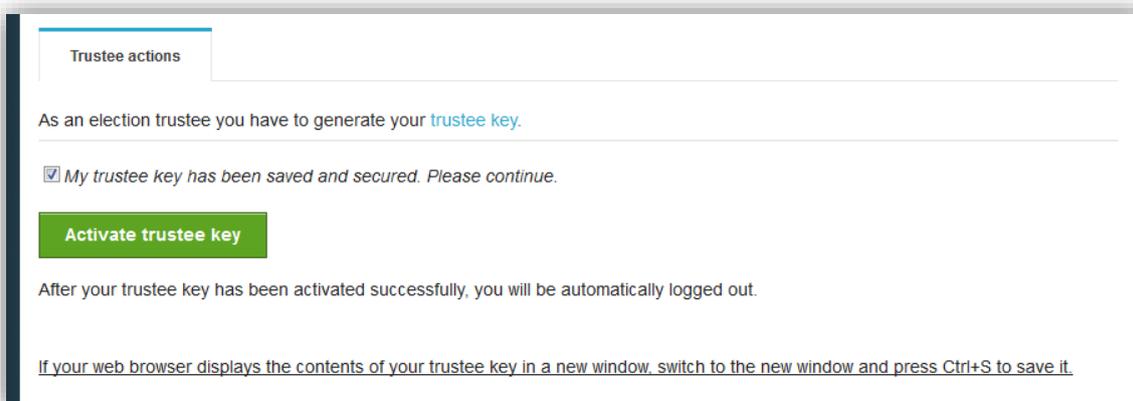


Figure 19. Trustee Key activation

The final step, which is also a prerequisite for the finalization of the election, is the verification of the generated Trustee Keys. The purpose of this step is to ensure that all members of the election committee have successfully saved their Trustee Keys and will be able to recover them when needed.

A new e-mail message with further instructions is sent to each member, prompting them to visit Zeus once more and verify their generated Trustee Key. The user must follow the link included in the message and click on “Confirm key possession” (Figure 20).

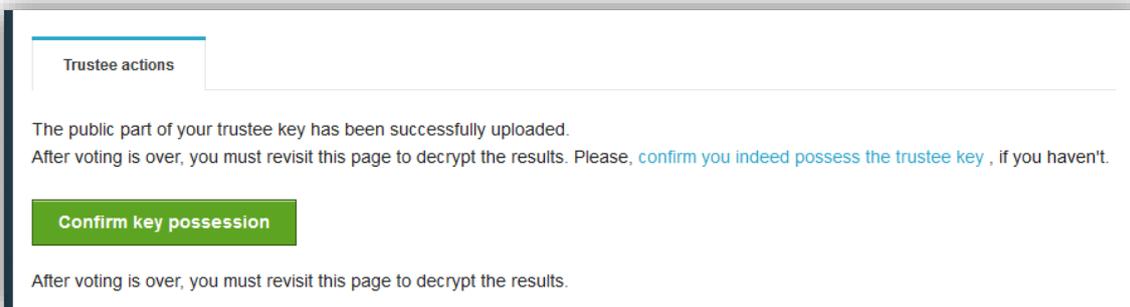
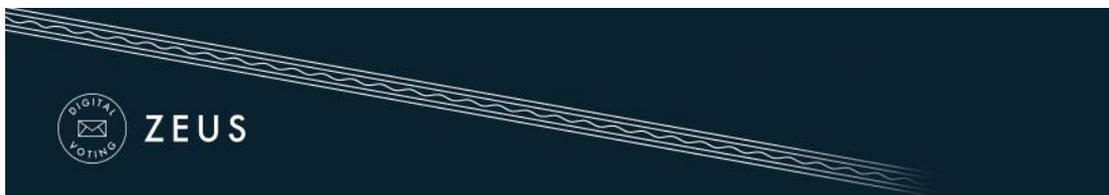


Figure 20. Trustee Key verification (1/2)

The user is asked to browse his/her file-system and select the file containing his/her Trustee Key. Then, the user clicks the “Verify” button in order to trigger the verification process (Figure 21). Once the application successfully verifies the Trustee Key, the user is automatically logged out.

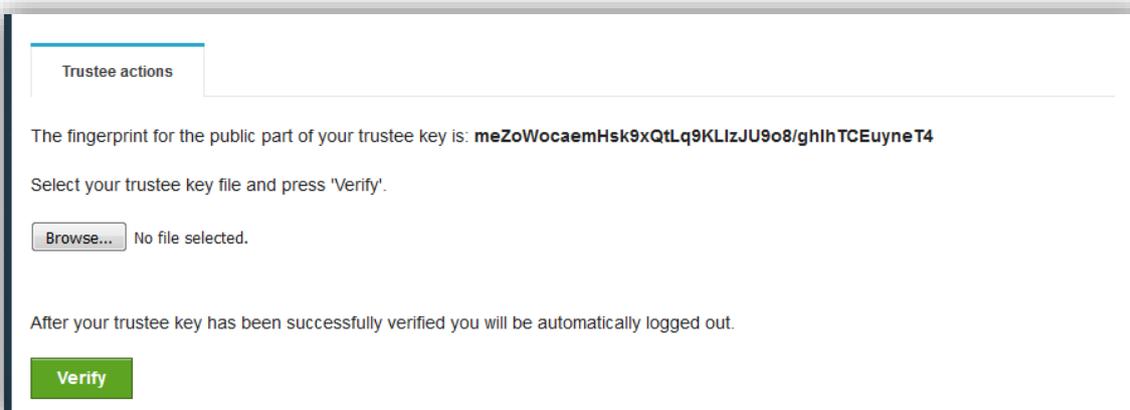
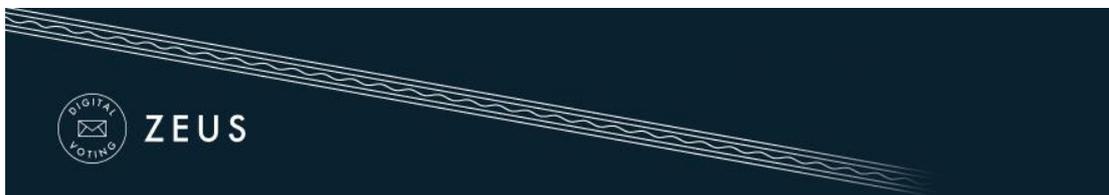


Figure 21. Trustee Key verification (2/2)

Finalizing the election

After all steps mentioned above are completed, the admin may move on to the finalization of the election by clicking the “Freeze election” button in the “Election admin actions” tab (Figure 22). Once an election is finalized, its basic data is not allowed to be modified (e.g. the starting date, the members of the election committee, the list of candidates,



etc.). However, some data such as the ending date (which may be postponed) or the voters' list remain modifiable.

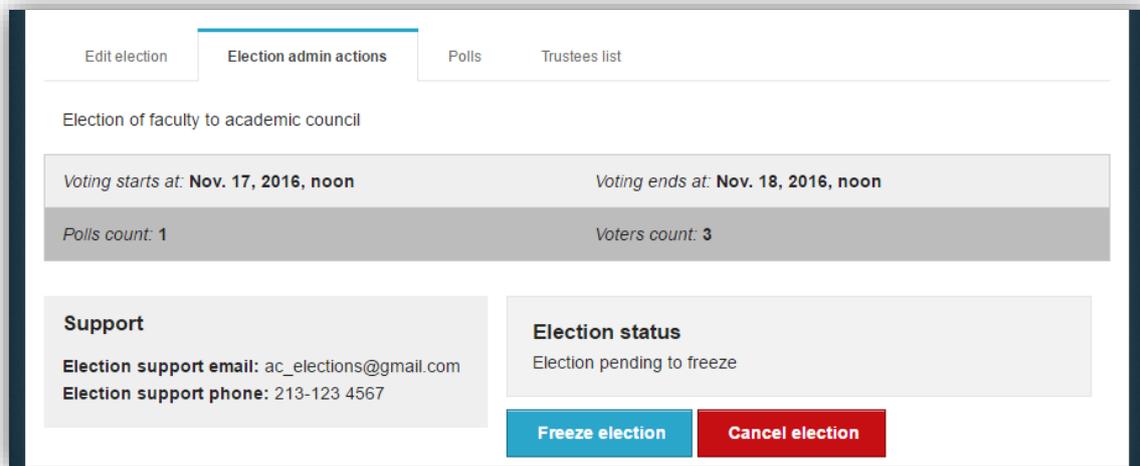


Figure 22. Election finalization

Sending e-mail invitations to voters

Following the finalization of the election, the admin should visit the “Polls” tab, where he can configure and send mass e-mail invitations to the voters. Each invitation contains a personal and confidential link to the Zeus voting web application. Using this link, the voter will be able to visit the election page at any time and find more info about the election, including the composition of the election committee, the list of candidates, the starting and ending dates, contact details for election support, etc. Furthermore, the voter will be able to cast his/her vote during the time-period specified by the admin.

The admin clicks on the “Batch polls actions” button and then on “Send voters email” (Figure 23).

Edit election		Election admin actions		Polls		Trustees list	
							Batch polls actions ▼ <input type="checkbox"/> Send voters email
Name	Status	Ballot Size	Voters Registered	Voters Invited	Voters Voted	Select Action	
Faculty to Academic council election	Frozen	1	3	0	0	<input type="button" value="Actions"/> ▼	
Totals		1	3	0	0		

Figure 23. Batch polls actions

The admin may view a template of the e-mail that will be sent to the voters (Figure 24). The user may specify the subject of the automatically generated e-mail message and/or add extra information to the message’s body, such as further details, instructions, etc. (Figure 25). Finally, by clicking the “Send” button, the application starts to gradually send out the invitations. The duration of this procedure varies based on the number of voters. (In the usual case, it completes within a period of a few minutes to a couple of hours.)



ZEUS

Send email to election 'Academic council elections' voters (all voters selected)

Templates: [Time to Vote](#) [Additional Info](#)

```
Subject: Zeus Elections -- <SUBJECT>

Legitimate recipient: <VOTER_SURNAME> <VOTER_NAME>
Dear voter,
<BODY>
You are invited to vote in the poll:
    Academic council elections

starting Nov. 17, 2016, noon,
and ending Nov. 18, 2016, noon
Your registration ID is: <VOTER_LOGIN_ID>.

To submit your vote, follow the link below
<VOTER_LOGIN_URL>

Information:
* You can vote more than once. Only your last vote will be counted.
* For information about the voting you can contact the trustees by phone,
    213-123 4567
or by email,
    ac_elections@gmail.com
* If you want to initiate an audit vote,
the valid audit codes are
pass1 pass2 ...
Otherwise ignore those codes above.

The voting takes place in the web browser in your computer,
where your choices are recorded and encrypted before being submitted.
We recommend the following browsers:
- Mozilla Firefox (version 10 or newer)
- Google Chrome (version 8.0 or newer)

Important:

The present message is strictly personal and confidential.
Do not forward or show it to others. Do not reply to this.
Instead, you can write to ac_elections@gmail.com.
If you are not the legitimate recipient, please delete this message
and contact helpdesk@zeus.grnet.gr

--
Zeus Elections
```

Figure 24. Template voter e-mail



ZEUS

Email subject:

In place of BODY:

Send To:

Figure 25. Editing/Sending e-mail

2. Voting Period

Monitoring the voting process

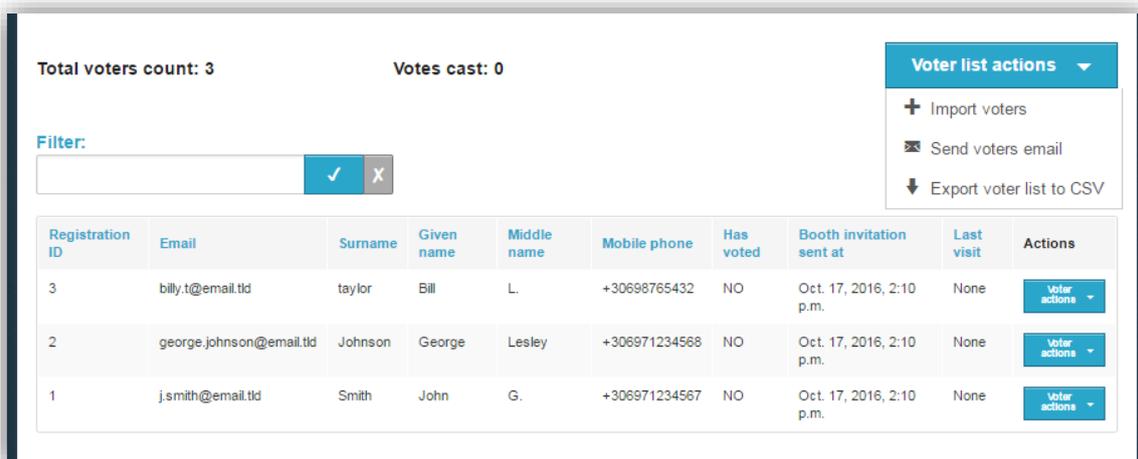
During the voting period, the admin has access to real time data enabling him/her to monitor the progress of the voting process.

The following information can be found in the “Polls” tab (Figure 26):

- Total number of voters
- Total number of votes cast
- Detailed record of the electors that have voted
- Sent date of the last e-mail invitation per voter
- Date of the last visit to the voting application per voter⁴

Additionally, the admin is able to perform various actions (Figure 26), such as:

- Resend e-mail invitation to a voter
- Remove an voter⁵
- Add/Edit an voter (by importing a new CSV file)
- Send custom e-mails to a specific group or all voters
- Export voter list in CSV format



The screenshot displays a web interface for monitoring voters. At the top, it shows 'Total voters count: 3' and 'Votes cast: 0'. A 'Filter:' input field is present. On the right, a 'Voter list actions' dropdown menu is open, showing options: '+ Import voters', '✉ Send voters email', and '↓ Export voter list to CSV'. Below this is a table with the following data:

Registration ID	Email	Surname	Given name	Middle name	Mobile phone	Has voted	Booth invitation sent at	Last visit	Actions
3	billy.t@email.tld	taylor	Bill	L.	+30698765432	NO	Oct. 17, 2016, 2:10 p.m.	None	Voter actions
2	george.johnson@email.tld	Johnson	George	Lesley	+306971234568	NO	Oct. 17, 2016, 2:10 p.m.	None	Voter actions
1	j.smith@email.tld	Smith	John	G.	+306971234567	NO	Oct. 17, 2016, 2:10 p.m.	None	Voter actions

Figure 26. Monitoring the voting process

⁴Note that visiting the voting application does not necessarily imply vote casting.

⁵Removing a voter is possible only as long as he/she has not cast a vote.

3. Election End – Results

Poll closing

At the specified ending date and time, vote submission is automatically disabled. However, the admin may postpone the ending date (even at this point) if the election organizers decide there are justifiable reasons. After visiting the “Edit election” tab, the admin can extend the voting period, by specifying a later date in the “Voting extended until” field (Figure 27) and clicking the “Save” button.

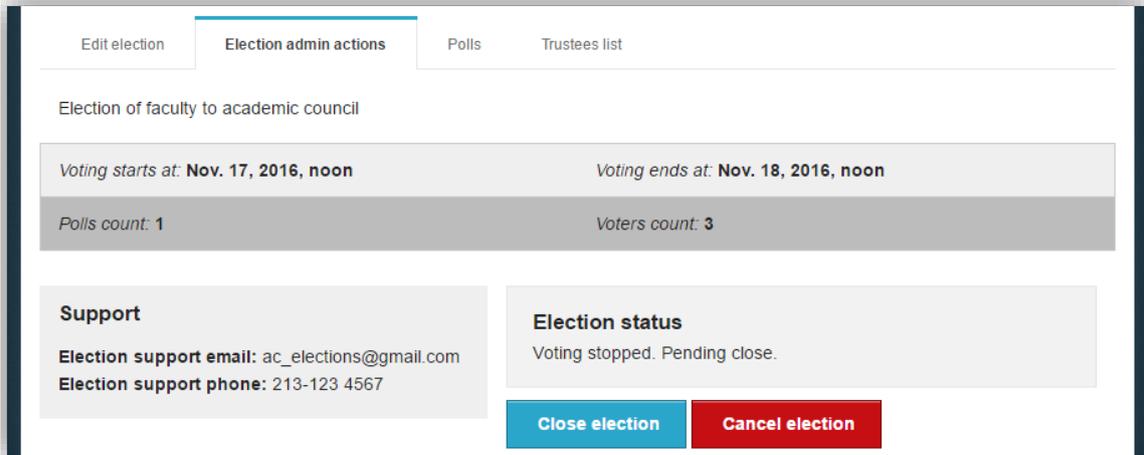


The screenshot shows a form with three sections for configuring voting times:

- Voting starts at** (When voting starts): Date field contains 2016-11-17, Time dropdown contains 12:00.
- Voting ends at** (When voting ends): Date field contains 2016-11-18, Time dropdown contains 12:00.
- Voting extended until** (Voting extension date): Date field contains 2016-11-18, Time dropdown contains 17:00.

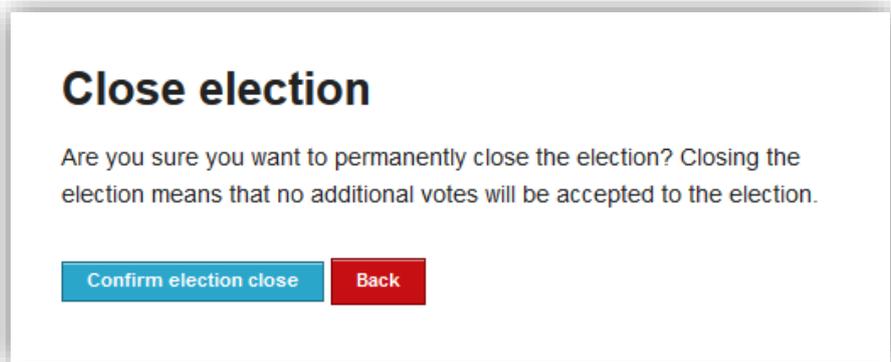
Figure 27. Extending the voting period

In order to conclusively end the voting process, the admin has to visit the “Election admin actions tab” and click the “Close election” button (Figure 28). After confirming the action by clicking the “End” button in the confirmation dialog that appears (Figure 29) the voting process is completed. After closing the election, no modification of its data is allowed.



The screenshot shows the 'Election admin actions' tab for an election titled 'Election of faculty to academic council'. It displays voting start and end times (Nov. 17, 2016, noon to Nov. 18, 2016, noon), poll and voter counts (1 poll, 3 voters), and support contact information (ac_elections@gmail.com, 213-123 4567). The 'Election status' is 'Voting stopped. Pending close.' At the bottom, there are two buttons: 'Close election' (blue) and 'Cancel election' (red).

Figure 28. Closing election



The dialog box has a title 'Close election' and a message: 'Are you sure you want to permanently close the election? Closing the election means that no additional votes will be accepted to the election.' At the bottom, there are two buttons: 'Confirm election close' (blue) and 'Back' (red).

Figure 29. Confirming election closing

Mixing and decrypting ballots

Once the election has been closed by the admin, the mixing of ballots starts automatically. This mixing stage (along with any external mixing stages performed by the election organizers) in conjunction with the previous encryption of ballots anonymizes the ballots, ensuring vote confidentiality. From the “Election status” the admin can monitor the mixing progress (Figure 30).

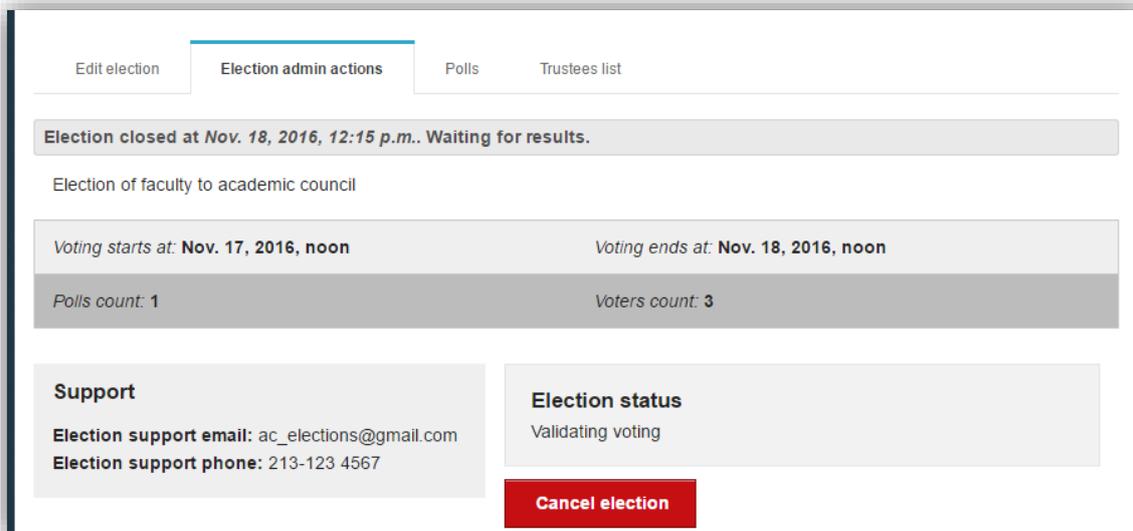


Figure 30. Starting ballot mixing

As soon as the mixing stage has been completed and before being able to determine the outcome of the election it is necessary to decrypt the anonymized ballots using all Trustee Keys (Figure 31). A new e-mail message is sent to each member of the election committee, instructing them to visit Zeus and complete the partial decryption of the election data using their Trustee Key.

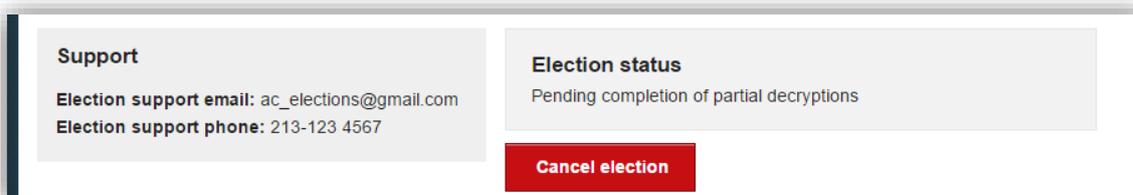


Figure 31. Finishing ballot mixing

Every member of the election committee has to visit Zeus (by following their personal link) and browse their file-system in order to select the file containing their Trustee Key (Figure 32). Then, they should click the “Perform partial decryption” button, in order to start the partial decryption process (Figure 33).

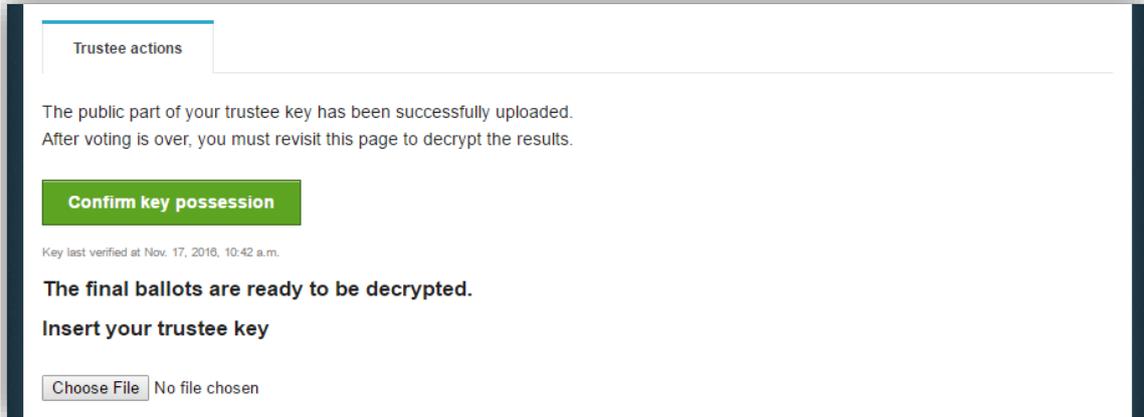
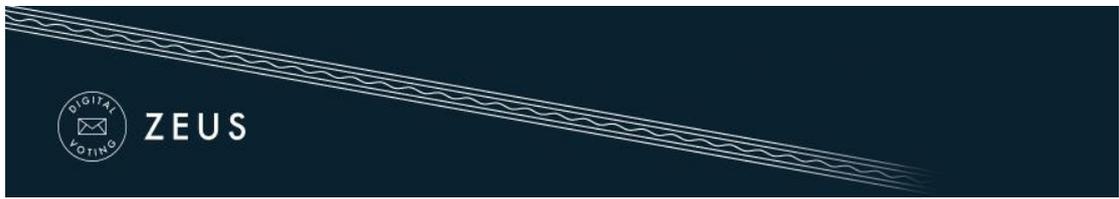


Figure 32. Inserting Trustee Key

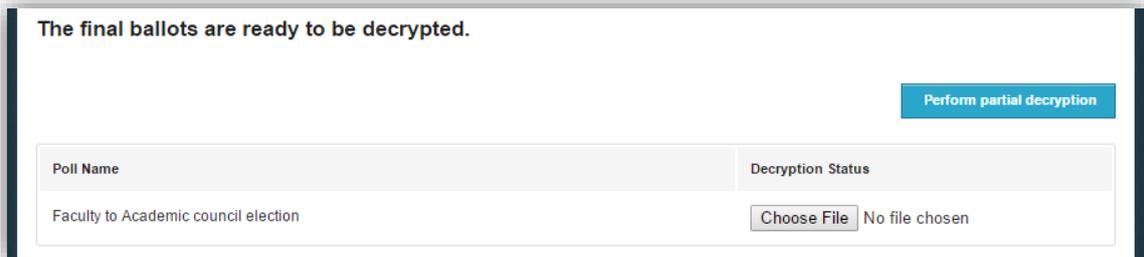
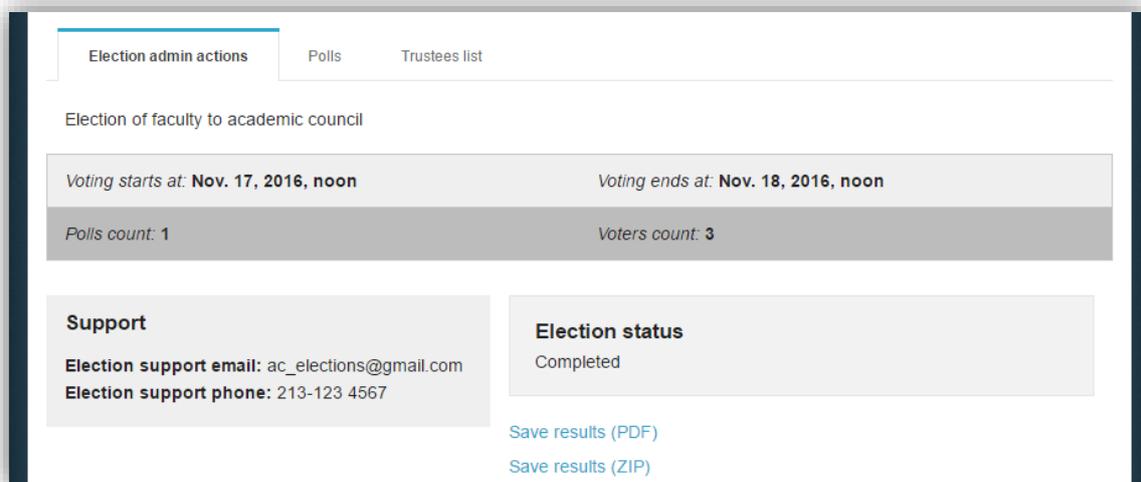


Figure 33. Performing ballot partial decryption

The duration of the partial decryption process varies based on the type of the election and the total number of votes. When the process finishes the message "Decryption uploaded." appears in the decryption status.

Counting ballots and exporting results

Having collected the output from all partial decryptions, “Zeus” will automatically process the data, determine the election results and display them to the admin. The admin can monitor the election status until its completion from the “Election admin actions” tab (Figure 34). From the same tab the admin has the option to download the results report for offline access in PDF or ZIP format, whereas from the “Polls” tab he/she may view and export the results of each poll separately (Figure 35).



Election admin actions | Polls | Trustees list

Election of faculty to academic council

Voting starts at: **Nov. 17, 2016, noon** | Voting ends at: **Nov. 18, 2016, noon**

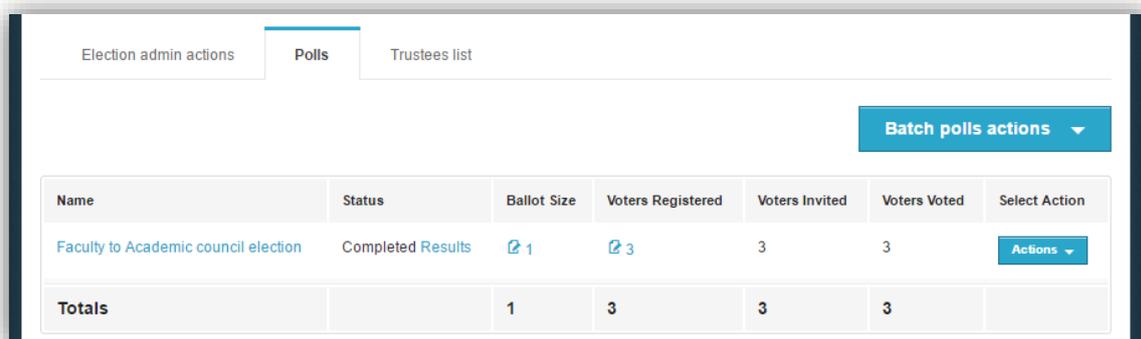
Polls count: **1** | Voters count: **3**

Support
 Election support email: ac_elections@gmail.com
 Election support phone: 213-123 4567

Election status
 Completed

[Save results \(PDF\)](#)
[Save results \(ZIP\)](#)

Figure 34. Viewing and exporting election results



Election admin actions | **Polls** | Trustees list

[Batch polls actions](#) ▼

Name	Status	Ballot Size	Voters Registered	Voters Invited	Voters Voted	Select Action
Faculty to Academic council election	Completed Results	1	3	3	3	Actions ▼
Totals		1	3	3	3	

Figure 35. Viewing and exporting poll results



Prerequisites

A personal computer with an active internet connection is all that is needed for a user (administrator, member of the election committee, elector) to access Zeus. One of the supported web browsers should be installed on the user's personal computer. If not already installed, the supported web browsers can be downloaded by following the links below:

-  For **Google Chrome**: <https://www.google.com/chrome/>
-  For **Mozilla Firefox**: <https://www.mozilla.org/firefox/>

In order to secure your personal computer and data, it is recommended to follow these guidelines:

- ✓ Keep the computer's operating system up-to-date and make sure to always install the latest security patches.
- ✓ Use firewalls and antivirus software.
- ✓ Ensure any browser plug-ins/add-ons are kept up-to-date.
- ✓ Do not install or use third-party toolbars in your web browser.