

V o t e e r i f i e r

User Manual

Contents

- 1 Introduction
- 2 Overview
- 3 Menu and Options
 - 3.1 File Menu
 - 3.2 View Menu
 - 3.3 Language Menu
 - 3.4 Help Menu
- 4 Beginning a Verification
 - 4.1 Universal Verification
 - 4.2 Individual Verification
 - 4.3 Additional Verification Processes
- 5 Viewing Results
 - 5.1 Tabs
 - 5.2 Organizing Verification Results
 - 5.3 Interpreting Results
 - 5.4 Helper Text
 - 5.5 Candidate Results
 - 5.6 Errors and Exceptions
- 6 Thanks

1 Introduction

Welcome to VoteVerifier, the independent verifier for elections held with the UniVote electronic voting system. This system was designed to boost confidence in the UniVote system by verifying the election results of a given election or election receipt. You should already have general knowledge of the UniVote system, but you can also find more information at www.UniVote.ch.

2 Overview

This manual will guide you through the basic features and operations of the VoteVerifier program. Upon loading you will see the main welcome window and menu bar at the top. You will be guided through use of the program beginning with periphery operations, followed by initiation of a verification, and ending with viewing and interpreting the results that are displayed by the program.

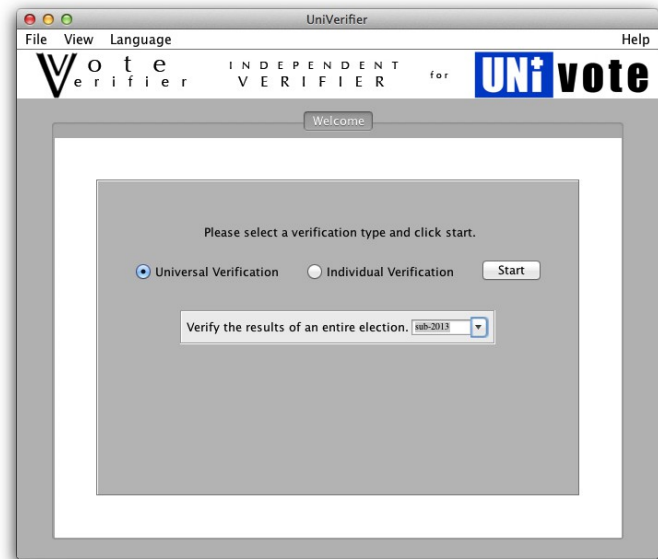


Illustration 1: The program is started up and the welcome panel is shown.

3 Menu and Options

The menu bar provides periphery functionality, which include exiting the program, displaying the text-only output of a verification, changing the language, and viewing information about the development of the program, as well as this manual.



Illustration 2: The menu bar provides periphery functionality.

3.1 File Menu

The *File* menu contains the option to exit and close the program.

3.2 View Menu

The *View* menu contains the option to show or hide the text console. To toggle the visibility, simply click on the check box next to the option *show console*. The console will show up at the bottom of the screen and although the menu has disappeared, the checkbox will now contain a check. To hide the console again return to the *View* menu, and click once more upon the *show console*.

3.3 Language Menu

VoteVerifier supports use in English, German, and French. The language can be changed through the *Language* menu, in which the options for the available languages appear. Upon clicking on one of the options, the program's visual content will be rebuilt with the text in the newly selected language. It is important not to change the language while a verification is in progress, or the progress will be lost and the verification will have to be started again.

3.4 Help Menu

To view information about the development of this software or to link quickly to this user manual options have been made available in the *Help* menu. In this menu you will first see the *About* menu, which will display a pop-up window with information about the development of this program.

To have quick access to this manual, the second option of the *Help* menu comes in quite handy. Click on *Manual*, and the document will automatically be loaded for viewing in your computer's preferred applications for PDF documents.

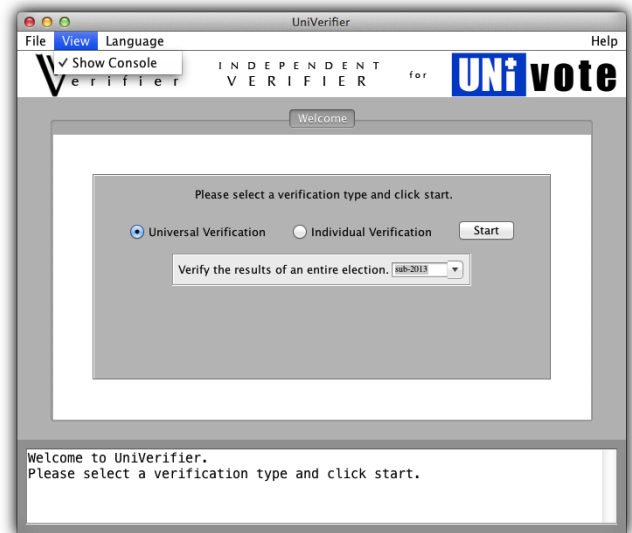


Illustration 3: A handy text output console can be show and hidden. When the program begins it is hidden.

4 Beginning a Verification

There are two possible verification types that can be carried out. The differences between the two are primarily thoroughness. The Universal Verification option will evaluate every applicable parameter of the election system of a given election ID, whereas the individual verification verifies comparably much less.

4.1 Universal Verification

The length of a typical verification process using the Universal Verification is approximately 2 to 10 minutes depending on the processing power of the computer. In this verification all certificates, signatures, mathematical proofs, are verified and displayed for the user.

When the program begins you are all set to begin the universal verification, which is already selected by default. If an active internet connection was detected and a connection was successfully established with the election board, a list of possible election IDs will be displayed in the text box in the middle of the screen. This list constitutes the only possible election IDs that may be used to start a verification. If, however, no connection was possible, you are still able to manually enter an election ID and try to click start. If a connection was possible, the appropriate verification process will begin upon clicking start.

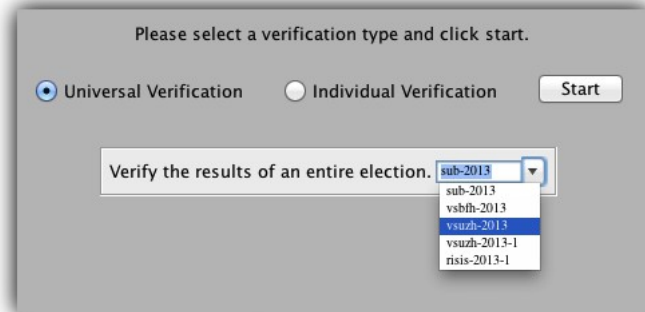


Illustration 4: The election IDs can be selected out of a provided list or inputted manually.

To choose one of the possible election IDs provided click on the downward-facing arrow in the text box in the middle of the screen. A list of the possible election IDs will pop-up and you will be able to select a new election ID from this list. After clicking on one of the possibilities, your selection will now be displayed in the text box, and you are now ready to begin the verification process by clicking on the blue *Start* button.

Clicking start causes a new tab to appear and its content will be immediately displayed. The verification results begin to appear and the status of the verification process is displayed. More about this verification tab can be found in the section entitled **Viewing Results**.

4.2 Individual Verification

The individual verification process is comparably much faster than universal verification. In this verification the certificates, signatures, mathematical proof, and if the ballot was included in the election results. The entire process lasts less than a few seconds.

To begin an individual verification change the selected verification type to individual verification by clicking on the button. The setup choices under your selection will change to display instructions for selecting a

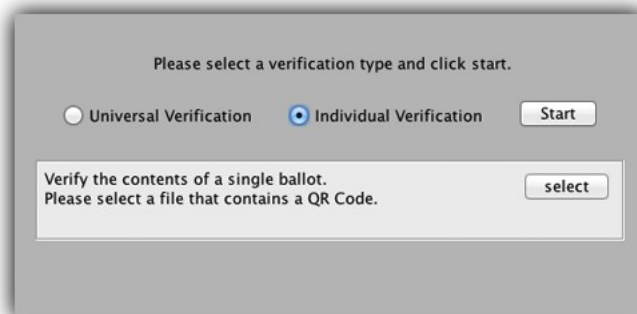


Illustration 5: Execute an individual verification by selection an file which contains an election receipt in the form of a QR code.

file which contains an election receipt in the form of a Quick Response Code (QR Code). To choose the election receipt you wish to verify click on the *Select* button and a file chooser window will be displayed. Navigate to the file which contains the election receipt and click *Select*. The program shows you the name of the file your have selected. If you are content with your choice, you may continue by clicking on *Start*.

The contents of the file you provided will be checked for validity. If the file contains a valid QR Code a new tab will appear containing the verification results. More about this verification tab can be found in the section entitled **Viewing Results**. If the file provided did not contain a QR Code, you will be notified of this, and instructed to choose a different file.

4.3 Additional Verification Processes

It is possible to begin multiple verification processes that run parallel to each other. To begin another verification process while another is running, return at any time to the *Welcome* tab by clicking on it. Here you will be able to follow the steps described in the sections *Universal Verification* and *Individual Verification* to begin another verification.

5 Viewing Results

5.1 Tabs

The verification results are displayed in a table in separate tabs for each election verification process. The text at the top of each tab identifies the process to the user. A tab with results for a universal election displays the election ID of the results it contains. If the results are for an individual election the tab shows the prefix *Ind:* followed by the election ID. Clicking on a tab will show the results for that election verification process. Clicking on the *Welcome* tab will allow you to begin a new election verification process.



Illustration 6: The different verification processes are organized into tabs with the corresponding name of the election ID.

Each tab is organized into three parts. At the top there is a view panel which shows choices to view the results organized in a different way or to view the results of the election, which shows how many votes the parties and candidates received. After the button panel comes a text area in which *Errors and*

Exceptions will be displayed. And finally there is the main results panel in which the verification results are displayed. Each component of the tab is discussed in detail in the rest of this section.

5.2 Organizing Verification Results

When the verification tab appears that default organization for the results is set to specification. This means that the results are ordered according to how they are listed in the system specification of the UniVote electronic voting system.

System Specification Organization Sections

- System Setup
- Election Setup
- Election Preparation
- Election Period
- Mixing and Tallying

By clicking on the other buttons next to *Specification* it is possible to change the organization. Clicking on *Entity* will order the verification results according to the entity in the UniVote system responsible for generating the content that was verified.



Illustration 7: Control how the verification results are organized with three different views.

Entity Organization Sections

- Parameters
- CA
- EM
- EA
- Tallier
- Mixer
- Voters

Finally, it is possible to view the results sorted according to the type of verification that was carried out.

For example if a certificate was verified, than the results of this verification will appear with all the other results for certificate verifications.

Type Organization Sections

Parameters
Certificate
RSA
NIZKP : proofs

5.3 Interpreting results

There are 4 possible outcomes for the verification results. A result may pass, fail, not be implemented, or have caused an error. In the case that the result passed the verification a green checkmark will appear at the end of the line where the verification is described. If the verification was unsuccessful, then in place of a green checkmark, a red “x” will appear.



Illustration 8: Icons representing the four possible verification results.

The two remaining results of a verification are special cases in which either the content for the verification has not yet been implemented by the UniVote team, or an error occurred during the processing of the verification. If a verification has yet to be implemented an orange question mark will be shown. If an error was produced then a yellow warn symbol is shown. In any case except a successful result, additional information about why the test failed and what this means can be obtained through the *Helper Text*. More information about this feature is available in the section *Helper Text*.

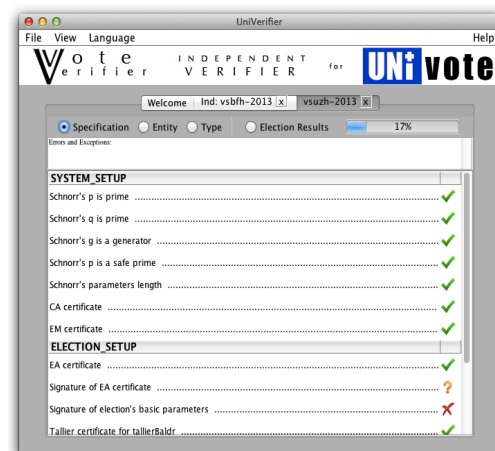


Illustration 9: The verification output is displayed in a corresponding tab.

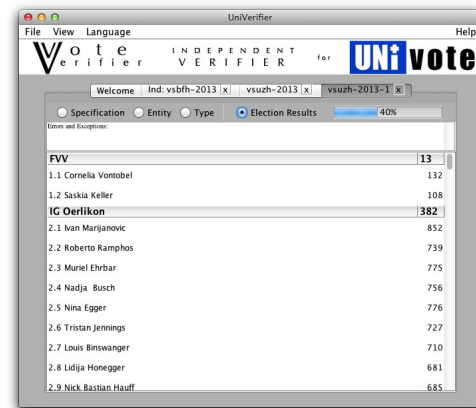
5.4 Helper Text

If a verification was not successful additional information about what went wrong may be obtained by clicking on or placing the mouse over the verification for which you would like to retrieve more information. A small blue helper text will appear and provide a brief explanation of why the verification was not a success.

5.5 Candidate Results

This view shows the results of the elections. It provides the information of how many votes were received by which candidates and parties. The choice *Election Results*, which is located after the choices for organizing the verification results, will take you to this view. The results are also organized in table form according to political party. In this section on one view is possible.

The table header shows the name of the party and how many votes it received. The content of each table lists the candidate for that party, as well as how many votes each candidate received.



The screenshot shows the 'Election Results' view in the UniVote application. The window title is 'UniVerifier'. The menu bar includes 'File', 'View', 'Language', and 'Help'. The main area displays a table of election results for the 'vsuzh-2013-1' election. The table has two columns: 'Candidate' and 'Votes'. The candidates are grouped by party: 'FVV' and 'IG Oerlikon'. The 'FVV' group includes Cornelia Vontobel (132), Saskia Keller (108), and Ivan Marjanovic (852). The 'IG Oerlikon' group includes Roberto Ramphos (739), Muriel Ehrbar (775), Nadja Busch (756), Nina Egger (776), Tristan Jennings (727), Louis Binswanger (710), Lidija Honegger (681), and Nick Bastian Hauff (685).

Candidate	Votes
FVV	13
1.1 Cornelia Vontobel	132
1.2 Saskia Keller	108
IG Oerlikon	382
2.1 Ivan Marjanovic	852
2.2 Roberto Ramphos	739
2.3 Muriel Ehrbar	775
2.4 Nadja Busch	756
2.5 Nina Egger	776
2.6 Tristan Jennings	727
2.7 Louis Binswanger	710
2.8 Lidija Honegger	681
2.9 Nick Bastian Hauff	685

Illustration 10: Election Results displays the voting results of the elections.

5.6 Errors and Exceptions

If there were any serious problems during the verification process such as a system crash, or broken contact with the election board, you will be notified of them in the *Errors and Exceptions* text area at the top of the results panel. In the odd case that there were so many errors that the screen became filled, this text area will contain all this information and allow you to scroll through the information.



6 Thanks

Thank you for using the VoteVerifier independent verification software for UniVote electronic elections. We hope that you feel more assured in the discretion, veracity, and exactitude of the UniVote system, and that you will continue to use this software in the future. For questions and comments, please visit the UniVote website at www.UniVote.ch and contact one of the members of the UniVote team.