GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
plan avanza

UNIVERSITAT JAUME·I

FONDO SOCIAL EUROPEO

VtUJI
Telematic Voting System

Usage guide for the
Voter Registry Operator

Id:	VT-D08
Version:	1.0
Date:	June 23 2011
Authors:	Francisco Aragó Monzonís Manuel Mollar Villanueva

Table of Contents

Presentation....3
VtUJI....3
Briefing....3
- Obtaining your credentials....4
- Basic principles....4
- Available equipment....5

Application user guide: voter registry operator....5
- Authentication score....5
- Header....6
- Authentication selection page....6
- Local authentication page....7
- Definitive password settlement....7
- Voting application main page....8
- Voting application main page: Voter registry operator area....8
- Voter registration screen....8
  - Basic view....8
  - Full information view....9
  - Other considerations....10

Credential distribution procedure....10
Exceptional scenarios....12
  - In case of attempted impersonation....12
  - In case of credential theft....12
  - In case of physical threat....13
  - In case of any other suspicious behavior 13

Presentation

You have been chosen to act as voter registry operator for this deployment of VtUJI.

Your duty will be to acknowledge the real identity of the voters and grant them access to the voting system by providing them with access credentials.

Please, read carefully this guide. If you need further information, please refer to the executive, administrative and technical documents.

VtUJI

VtUJI is a powerful and complete tool, developed at the 'Universitat Jaume I', to hold polls, elections and any other kind of referendum through the Internet, where the electorate can participate from any location with its own browser, with no need for additional software nor hardware and providing the highest guarantees of security, integrity and anonymity both to the voter and to the organizer.

This is a tool generally aimed to mid-size private and public corporations, but due to its efficiency, simplicity and personalization capability can be deployed on any situation and on any scale, from small localized communities to great and distributed companies.

Briefing

Before starting on your duties, there's a set of things you have to be briefed about by the organizers. Mainly related to decisions taken about some optional steps of the registration process. Here is a list:

- **Do I have to register new users?** This means if you are allowed to input the personal data of a person requesting credentials whose data is not already on the system. If not, you will only search for him and set his password.
- **How do I know that an applicant has the right to have access credentials for the voting system?** You must be informed on the criteria or the method to do this. It may go from 'everyone is allowed' to, 'only those who are previously loaded', or only those in possession of a corporate ID card, or even a lookup system to discern it.
- **Do I have to set corporate user names?** If not, and as long as the field needs to be filled, put the ID number also there. If you have to, you will be given instructions about how you will get the information: on the ID card, a lookup system, a self-generating algorithm, etc. NEVER trust the applicant; always get it from a reliable source. You will be briefed about the source.
- **Do I have to set a corporate e-mail address or the applicant can suggest one?** That is, it must come from a reliable source as the user name or the applicant can suggest one of his convenience.

- **Which is the canonical from to write the ID number?** Since most ID numbers have multiple parts, there are various ways to write them (with hyphens or spaces between them, etc.). You need a common criteria to avoid duplication users on the system, which would be a severe issue.
- **Do users have to sign a usage/data cession contract?** If your country law or organization directives require so, you will be informed on which and how must it be signed.
- **Where do I get the contract?** You may get a bulk of previously printed contracts or a printer to do it on demand. You will be informed.
- **Do users have to use a security support corporate authentication?** Sometimes, for extra security reasons, users will be required to log in with a corporate authentication system before changing their password. You must inform them about it.
- **Do I need to have a Clauer?** Depending on the mobility of your post, you will be given a Clauer as a support credential to gain enough access level to do your functions. We'll deepen on this later.
- **How do I acknowledge that an ID card is not forged?** You will be trained to identify legitimate ID cards and forged ID cards.
- **Which is the address (URL) od the voting application?** Where you will access to register the voters.
- **How do I log into the voting system?** You will be given credentials.

Obtaining your credentials

As a user of the voting system, you also need credentials to access. They must be given to you when briefed and, as any other user, the **password will be temporary and you need to log in and change it before 48 hours**.

Basic principles

Before starting with your work, be sure to understand and follow this list of basic principles.

Basic principles

- Check carefully the identity of the applicant at all times. Avoid impersonation at all costs.
- Always double check the information that you have input or was there. Duplicated or erroneous data would be disastrous.
- Follow the procedures step by step. Don't skip or obviate the minimum detail. They are there for some reason.
- Use your common sense to face unexpected situations..
- If you are unsure on how to act, contact the election authority before doing nothing.

Available equipment

This is a list of all the equipment you may have available on your desk. Check it beforehand to avoid interrupting your activity. Be sure to regularly check the levels of consumables and order them ahead, to avoid running out of stock.

- **A computer with internet access**. It will be administered and will have the most common security measures to avoid third party surveillance or tampering. Please refrain from doing dangerous actions that may end with the computer hijacked by an attacker. He could impersonate you on registering fake users or obtaining passwords and you could be blamed on that.
- **A bar code reader**. The password on the voter cards will be coded in bars. This way, you are less likely to make misspellings.
- **A Clauer formatted USB drive** (*Optional*). As stated earlier, you will need it to access your functions if you switch frequently from desk to desk.
- **A box of voter cards** (*Consumable*). The cards that you will give away to the applicants.
- **A printer** (*Optional*). If you are instructed to print contracts on demand.
- **White paper** (Optional, *Consumable*). To print the contracts.
- **Printer ink** (Optional, *Consumable*). To print the contracts.
- **Ball pens** (*Consumable*). To facilitate the users take notes or anything.

Application user guide: voter registry operator

Now, we will describe all the interface elements of the application that you will use.

Authentication score

Each user is assigned a role, classified by the sensibility of its functions.

The execution of each role's functions requires reaching a certain authentication score. In your case you need score 2.

The score can be raised by one point by successfully authenticating using any of the available methods, or up to three points if using local authentication.

Local authentication will award you one point for providing th correct user name and password, and will additionally give one point for logging in from the usual IP address and another one for the physical possession of a certain Clauer (by connecting the Clauer to the computer during the authentication, you will need Clauer software to achieve this[1]).

These additional information can be preset by the system administrator on the population edition or it will be set after the first successful login (the IP address and the identifier of the Clauer connected to the computer you are logging

[1] See http://clauer.nisu.org/ for more details.

from will be recorded).

This is why, if your desk is permanent, you will gain an extra point only by the preset IP of this computer, or if you switch desk frequently, you will be given a Clauer (also, if there's a corporate authentication system, you can use it instead of the Clauer).

Header

Every page of the application shares a common header area, which contains the following elements (some of them will appear once authenticated):

Always

- ***Title***: A title, 'Telematic voting' and a logo (optional) are located in the center of the header area.
- ***Language Selector***: On the uppermost right corner, a set of flags let you change the language of the interface. You will be directed to the main page (or authentication selection page if not logged in) after each switch.
- ***About***: Besides the language selector, this link will pop up a window showing information about the funders and developers of this project.
- ***Help page*****:** Once configured, it will show help information about the use of VtUJI.

When authenticated

- ***Start***: On the upper left corner of the header area, it will get you back to the main page.
- ***Your full name***: Next to the 'Start' button. The full name of the user whose credentials you used to log in. You can always click on it to be directed to the authentication selection page, where you can authenticate with other method if you are required to. If you have a special role and you didn't reach your maximum access level, a red message will invite you to keep raising your score.
- ***Exit***: Next to the 'Start' button. Will immediately void your session and your score and direct you to the authentication selection page.

Authentication selection page

Every time you access the system and you are not authenticated, you will be shown the authentication selection page, which has the following layout:

- ***Authentication method list***: Below the title area, centered and in a single column, all the available authentication methods will appear. Either as logos or as text links. Click on any of them to use it to authenticate. The first one will be the default method.
- ***Report a problem***: At the bottom of the authentication method list, this link will send you to a form to contact a polling station officer to ask him for help or to report irregularities. It will sequentially ask you for the following data (in order of appearance, hit proceed after each selection):
  - ***User ID***: Your user ID. Not you user name or full name, to identify yourself.

- ***Election***: The election you need help or want to complain about.
- ***Officer***: (or All) The name of the officer to whom you want to address your complaint/request.
- ***Message***: The message you want to send.
- ***Image numbers***: An automated Turing test, to avoid sending massive amounts of messages in order to collapse the server or the accounts of the officers. Write the numbers on the image.

Sometimes you will be **redirected to some other external page** (check the address bar on your browser) instead of this one. It will be an external authentication method and this is because the redirection to the default authentication method is activated. To **force showing the authentication selection page**, access again and you won't be redirected.

When you are set a temporary password, if you try to log in with any other method, you will be directed to the local authentication page to set your definitive password. You won't be able to continue until you do so.

Local authentication page

It is the basic and the only independent and autonomous authentication method. These are the fields shown.

- ***User ID or user name***: Your user ID or your user name.
- ***Password***: The password you have been given (either the temporary or the definitive one, depending on the state of your credential distribution process).
- ***Image numbers*****:** An automated Turing test to, in case of massive credential theft, avoid massive impersonation and ballot injection. Write the numbers on the image.
- ***Enter***: Submits the authentication request.
- ***Generate new password***: If you check this box, once you are successfully authenticated, a new definitive password will be generated. It will override your current one and you will be directed to the '**definitive password settlement**', the same as after logging in with the temporary password.
- ***Back***: Sends you back to the authentication selection page.

If you fail, you will be notified why in red below the submit button.

If a Clauer is detected, you will be prompted if you want to let the program read its ID. If you accept, you can add one more point to your score.

Definitive password settlement

- You will be shown an screen with your new password (case sensitive) clearly identified. Write it down before hitting **Continue**, or else you won't be able to log in again. This is the same screen your applicants will see.

Voting application main page

The main page is divided in sections, delimited by horizontal colored areas. Each area clusters all the functions of a role, ordered from the highest to the lowermost role. The number of shown areas depends on the role associated with your user and the score you have currently earned. These are the ones you will see:

- Voter registry operator operations (default: cyan)
- Polling station officer or chairman operations (default: pale green)

The voter role has three different assigned areas: One regarding ongoing elections that are active and he hasn't voted yet, another regarding ongoing elections where he has voted or still are not active, and another regarding past elections.

- Pending election area (default: light purple)
- Current elections area (default: pale yellow)
- Previous elections area (default: pale yellow)

Voting application main page: Voter registry operator area

The only control you will find there is a *Start* button that will lead you to the voter registration screen.

Voter registration screen

Basic view

The initial interface of the screen contains the following elements:

- ***User ID***: To input the unique ID number associated to the user (remember to use always a canonical from).
- ***Password***: To input the new password for the user. It is not an obfuscated field, since you need to check that it is correct and there is little harm if anyone reads it.
- ***Update button***: Click it to submit the data.

At this point, you can perform two operations:

- ***User data querying***: As you are informed below, input the ID number only and hit *Update* to be shown all the available user data on the full information view.
- ***User password settlement/user insertion***: Write an ID number and a new password (the one in the voter card).
  - *If the user existed*, a message line will show the ID number, the full name of the user and will confirm that the password has been updated. From this moment, the 48 hour counter has been reset.
  - *If the user didn't exist*, you will be prompted to inform you and the full information view will be loaded, with only the User ID and password fields

filled with the information you have provided.

Full information view

In this view, all the user information fields are shown. These are the following:

- ***User ID***: Same as above.
- ***Password***: Same as above.
- ***User***: The user name associated to the user. It is a unique identifier, and **once inserted, it can't be modified**.
- ***Surname, Name***: The real name and surname of the user. It is not a unique field.
- ***E-mail***: The e-mail where the user will receive notifications from the applications. It is not a unique field.
- ***Update button***: Click it to submit the data.
- ***Last modified***: It will show the date of the insertion or last data/password update for this user and the name of the registry operator who did it. It is information to track down impersonators. It will be overridden after each update, so be sure not to update the data before checking if there is any suspicion of impersonation. It won't be shown if the user was inserted by the system administrator or the election administrator, at least until a registry operator updates the information.

In this view, you can perform the following operations:

- ***User data querying***: As explained above, write an ID number (and not the password, or it will be updated) to load the information for its user.
- ***User data update***: Change the value of the data fields. You need to set a value for the password or else it will be considered a query and won't be updated. Outcomes may be:
  - **Updated**: When properly updated, a message line will show the ID number, the full name of the user and will confirm that the password has been updated.
  - **Partially updated**: No error happened, but some fields are locked (the full name) because the user was an officer or candidate on any of the elections. The unlocked fields will be updated, but the rest won't. A 'partially updated message line will appear'.
  - **Update error**: When an error happens (usually, you tried to edit the user name or the ID number), you will be prompted. The fields on the page will show the information you had changed, but it had not been updated (if you query again, you will get the old information).

> Even if you didn't change the full name on a user who has it locked, you will get the partially updated error. It is an implementation issue but won't affect you. Ignore it.

- ***User insertion***: Exactly the same behavior as on the data update. Fill in the information fields and hit update. If the values on the unique fields (ID number and user name) are not duplicated, an '*added*' message line will show up. Else, you will be prompted with an error and user won't be inserted.

Other considerations

- You can only query the user data using his ID number: not by full name, e-mail or user name.
- if you have overridden user data and you want to bring back the original value, just blank the password field and hit update. This way it will be queried instead of updated.
- If you made a mistake and need to delete a user, contact the system administrator. You are not able to delete users.

Credential distribution procedure

Now we will detail the formal procedure you must follow to provide an applicant with his credentials.

1. The applicant will go to your desk.

Identification check

2. Ask him to hand over his ID card.
3. Check that the ID card is valid, not forged and has not been altered.
4. Check the identity of the applicant with the photograph on the ID card.
5. Check the consistency and validity of the data on the ID card by asking to the applicant questions about the relevant data you find there (name, address, e-mail address, ID number, etc.). Compare the answers.
6. If you are not satisfied with the result of any of the checks,
   - Deny the credentials to the applicant.
   - Inform him to direct any reclamation to the election authority.
7. Now, check if the applicant has the right to be part of the voting system. Use the criteria or lookup service you have been trained about.

Data insertion/verification

8. At this point, search the applicant's ID number on the system, to retrieve his information. Remember to use the canonical form you have been instructed about or else you may create a duplicate of the user.
9. Look for the information about the last modification (if any). Also ask the applicant the reason of his application (password loss, hijack, etc).

- Check with the applicant that it matches the last time he was on a registration desk.
- If not, there may be an impersonation. Inquire further on the applicant and report this information along with the last modification date and operator to the election authority, to open an investigation.
- See section '*Exceptional scenarios*' in page 12 for more information.

10. If the applicant's data is not registered on the system and you ARE NOT authorized to insert users,
    - Deny the credentials to the applicant
    - Tell him to report to the election authority if he believes it is a mistake.
11. If the applicant's data is not registered on the system and you ARE authorized to insert users,
    - Type in the information from the ID card.
    - If the information for any field is not on the ID card, use the methods or lookup services you have been provided with to infer or retrieve them.
    - Don't trust the word of the applicant on any of that information, specially the user-name.
    - If you have been allowed to, ask the applicant about the e-mail address they want to use on the voting system (inform them that it will be used to send them notifications).
    - Double check every field for misspellings, inserting wrong data would have serious consequences; specially on the user name and the ID number field.
12. If the applicant's data is registered on the system,
    - Double check the values with the ones on the ID card.
    - Correct any mistakes you may find (if the application lets you).
    - If you have been allowed to, ask the applicant about the e-mail address they want to use on the voting system (inform them that it will be used to send them notifications).
13. Hand back the ID card to the applicant.

Password settlement and contract signing

14. Offer the box of mixed voter cards to the applicant, so he can choose one randomly.
15. Ask the applicant for the card.
16. If you are instructed to, give the applicant the contract to be signed (print it if you need to).
17. If the applicant refuses to sign the contract, end the process now.
18. Once you get back the signed contract, register the password on the voter

card with the bar code reader.

19. Submit the new/updated data.

20. Give back the card to the applicant.

Voter briefing

21. Inform the applicant about his user name on the voting system. Write it on the card or let him do it.

22. Inform the applicant about the URL of the voting application.

23. Inform him about the following points:

    - That the password is temporary, and that he must log in before 48 hours or it will be voided.
    - To use a safe and trusted computer to take this step. He must not trust a public computer or a shared account.
    - That he will be given a definitive password, and advise him to write it down on the voter card.
    - If you were instructed about, that he will need to log into the corporate login system before logging on the voting application, as an extra security measure.
    - To store the card safely until he needs it.
    - That while he has the definitive password, he can change it as many times as wanted using the voting application.
    - That if the temporary password is voided or he loses the definitive password, he must go back to the registration desk to reset it.
    - That if he suspects his credentials were stolen or misused by a third party, he must go back to the desk to renew them and report the incident.

Exceptional scenarios

You may face several situations that differ from the normal distribution of credentials.

In case of attempted impersonation

Remember that you control the process; abort the credential distribution if you can't be completely sure that the applicant is legitimately doing it, and report immediately to the election authority.

In case of credential theft

If some user suspects that his credentials have been revealed or stolen, check the last update data and verify that he was on that desk at that time.

If so, renew the password immediately.

Else, if the user still has his password and is still valid, instruct him to change it using the application (this way, the registrar information will be kept).

If he lost it, try to keep the registrar information if possible (if the user needs to use the password immediately, renew it).

Anyway, report the incident with the higher level of detail to the election authority.

In case of physical threat

If you are under any kind of physical threat or coercion, cooperate as much as possible. Report the incident and its extent as soon as it ends.

In case of any other suspicious behavior

Abort the credential distribution and report to the election authority.