VtUJI
Telematic Voting System

Usage guide for the System Administrator

Id:	VT-D04
Version:	1.0
Date:	June 9 2011
Authors:	Francisco Aragó Monzonís Manuel Mollar Villanueva

Table of Contents

Presentation

You have been chosen to act as the system administrator for this deployment of VtUJI.

Your duty will be to provide the technical support for the deployment and operation of this system, perform the maintenance and monitor the state of the system, to prevent undesired situations or identify needed hardware improvements.

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.

System overview

VtUJI is distributed in the form of a full operative system on a Live CD. This way, its contents can't be altered by malicious agents and the machine where it is deployed doesn't need any further auditing or security checks. Once started on the hosting server, it launches a web application (remotely accessible through any browser on any computer) where organizers and voters will create and manage elections and participate in them respectively.

Before finishing setup, the cyphering key that protects data from attackers will be distributed on the committee's USB memory sticks, which will be formatted as Clauers (Clauer is a project aimed at turning a USB memory stick into a cryptographic object storage device). All data will be protected using this key.

Besides the web voting application, the only access point to the system is an operations menu through the same computer which only can be operated after rebuilding the committee's key as a way to acknowledge their authorization to do so. The web application also has some critical administration routines, but they can only be performed by allowing so from the earlier mentioned operations menu, this way the committee has full control of any critical action to be performed on the system.

Due to its construction and access policies, VtUJI guarantees the integrity and

anonymity of all the electoral processes. As a direct recording voting system, user would usually have to trust on this security not to be breached to keep his anonymity, but as anonymity is usually the main concern for the elector, VtUJI has been built to be compatible with project eSurvey, which allows the elector to easily take control over his own anonymity. This way, even in the worst and most improbable prospects of security breaches and inner corruption, voter anonymity won't be violated.

Logical security measures applied on VtUJI are oriented on minimizing the effects from physical and administrative security failures, but the proper assignment of roles and the execution of some procedures is critical, so that if not applied properly it would greatly harm the confidence chain and undermine voter's trust and the institution's public image. This must be avoided at all costs.

What do I need to deploy VtUJI?

Deploying the server

Prior to the deployment of the server, we need the following elements.

Material

- A PC computer, equipped with an Ubuntu GNU/Linux 10.04 LTS compatible Ethernet card and a CD-ROM drive.
- Between 2 and 4 GB of RAM memory. (*Although not compulsory to run the system, it is necessary to protect it against physical manipulations, since all the CDROM will be copied to the RAM*)
- Some data storage system, among the following:
    1. Local hard drive or Software RAID disk array. Properly partitioned and configured. Use any GNU/Linux installer CD to set it up.
    2. Local hard drive with a valid file system (ext2, ext3, ext4, fat16, fat32). Data will be written on a single file on the root of the file system.
    3. iSCSI accessible remote hard drive.
    4. SMBFS remotely accessible directory.
    5. NFS remotely accessible directory.
- A set of identical copies of the VtUJI Server CD. One for each member of the key custody committee plus one to be the working copy.
- A set of USB drives. One for each member of the key custody committee, plus one to keep the server certificate request and one for you, since you will need it as an identification token (*if you already have a Clauer formatted USB drive, you can bring it*).
- A permanent marker.
- A second computer, with connection to the Internet and the following software, to configure the web application:
    1. Either Windows OS + Internet Explorer or Linux (most common

distributions, such as Debian, Ubuntu, Fedora, CentOS, SuSe)+ Mozilla Firefox 3.6.

2. Clauer Software.

Technical

- A corporate e-mail account for the administrator, to receive notifications from the voting system.
- Another corporate mail account to be the account identifier at eSurveySites. If the organization or the administrator already have an account, they can use it.
- Network configuration for this server (if you need to guess the MAC address of this computer, use a Live CD to start it up):
    1. IP address, net mask, gateway and two DNS servers.
    2. A domain name for the server, configured on your domain name provider to match the previous IP address.
- The server should not be firewalled at all, but if you need to, these are the interactions of the server:
    1. Incoming: HTTP (port 80) and HTTPS (port 443) connections
    2. Outgoing: HTTP/S and SMTP connections. SMTP connections can be relayed through another mail server.
- If using any local hard drive storage configuration, you can optionally use a remote ssh backup system. The encrypted backup file will be written on the home folder of the user and the copy will be overwritten each time, so it is the duty of that system's administrator to keep a copy history if needed. These are the needed parameters:
    1. Server name
    2. User name
    3. Password.
- An SSL certificate authority to whom request the signature of the certificate. It must be accepted in most web browsers/operative systems (specially in Ubuntu GNU/Linux 10.04 LTS).

Facilities

- Server room:
    1. Some partially restricted room, but there's no need for special security measures unless attempts to destroy the whole server are likely.
    2. Must be able to host all the members of the committee at once, plus some technicians, so it is not advisable to house another delicate or expensive equipment on it.

3. A sparsely used meeting room or the election authority office may work.

- Furniture: What you believe sufficient to accommodate the commission and the working technician: A desk and a chair for him and maybe chairs for the other, although not necessary.
- Power supply for the computer should be protected against power surges and be connected to some sort of UPS system. An emergency generator for the worst cases could be a little too much, but it is not discouraged.

Establishing registry posts

For each registry post we want to establish, we will need the following:

Materials

- A computer, with connection to the Internet.
- An adequate supply of voter cards.
- A bar code reader.
- A USB drive (depends, see the following section)

Technical

- The computer must be properly administered (protected against attackers, viruses, Trojan horses and any other hazards that could be used to sniff the voter's passwords).
- The IP of his computer must be preset on the web application, to let him reach the necessary access level. *If the registrar is switching to another post, his IP address must be reset (or set to the new one) on the web application. Otherwise he won't be able to reach the access level he needs to issue voter cards*. Alternatively, if the computer uses Firefox 3.6 over GNU/Linux or Internet Explorer over windows, a Clauer formatted USB drive for each operator can be given instead of fixing the IP.

Facilities

- Some easily accessible counter for all the potential voters, such as secretary or information desks on public service buildings or areas.

Personnel

- One trained and trustworthy administrative.

Establishing polling posts

In case you need to establish a physical polling post to allow voters to go there to cast their ballots, these are your needs:

Materials

- A PC computer, with connection to the Internet.

- Copies of the Voter LiveCD (if available, or compatible with the computer). One for each officer plus one as the working copy.

Technical

- If the Voter LiveCD is not available, the computer must be properly secured, following the guidelines in section '*Voting Booth computer securing*' (page 53).

Facilities

- A station, located in a public access building or room, with enough room to hold all the materials, the officers and the voters.
- A voting booth, adapted to keep the computer in a separate compartment.

Personnel

- The officer board, drafted among a combination of electors, party representatives, or election authority representatives. See the administrative documentation for further reference.
- A technician, serving on call in case of emergency situations (hardware or network failures).

How do I set up the server?

First of all, read the annex '*VtUJI Server Live CD interface usage considerations*' (page 48), to understand some peculiar aspects of the installation interface.

Starting up the computer

The first part of server configuration is related with the configuration and adaptation of the server machine, to be deployed over your network and among the structure of your organization.

First of all, insert the VtUJI Live CD and make sure it is booting from the CD-ROM unit. You will see the splash page for a while. Wait until the installation program is started.

Configuring the server

The installation program will be started as soon as you see a dialog showing the version, the developers and the funders of the project. Hit ok.

Language Selector

Choose the language you want. This will be the interface language for this installation program. It has no effect on the voting application and it is not remembered. Each time you restart the system you can choose again.

Copying the CD to RAM

At this point, the program will try to copy all the content of the CD to RAM. If the system has enough RAM memory it will be copied, if it is clearly insufficient it won't be copied, and if it may be enough, it is left at your choice. This decision is not remembered and can be undone by restarting the server (if you chose to copy it and the system failed or if you upgraded the hardware and want it to be copied from now on).

Copying the CD to RAM is a measure to avoid CD spoofing.

An attacker may access the server physically and replace the CD with an altered one. Any program not currently on execution or not cached on RAM would be loaded from the altered copy, and its behavior would be determined by the attacker. He would gain absolute control of the system.

If your server computer is not prepared to hold all the CD in RAM, we urge you to upgrade it, since it would be a source of mistrust for all the participants on the voting system.

Main selector

The program will prompt you to insert a Clauer to load configuration from to restart the system or to choose to format a new system. Choose **Format.**

If you plug a Clauer, you still can choose to cancel the system restart and go back to this dialog to choose format.

If you plug a plain USB drive (not formatted as a Clauer) or a Clauer with no VtUJI data, you will be prompted to Format the system.

You will be asked three times for confirmation. Please realize that **any USB drive used in this processed will be formatted, losing all the data it may contain**. At any moment, you can go back to the main selector.

License agreement

You will be prompted to read and accept the license. VtUJI is distributed under *UJI commercial license* and *UJI non-commercial license*, which are GNU GPL3 compatible licenses.

Declining to accept the license will cause the system to shut down.

Essential system parameters

The following steps will prompt you to set the essential system parameters, which are those needed to start the basic system functionalities: networking, data storage system access, backup copy access parameters, mailing parameters and key sharing parameters.

All those parameters will be written, cyphered, on the Clauers of the committee, along with the key fragments. Any other parameter will be stored on the cyphered data storage unit.

Emergency menu

If some error happens, critical enough to abort the installation process, you will be prompted with a menu, containing this options:

- **Shutdown**: Shutdown the computer.
- **Reboot**: Reboot the computer.
- **Terminal**: Launch a root access terminal, with full access and control. Useful to try to diagnose the failure.

Networking parameters

At first, you will be prompted to choose if you want manual configuration or if you want to search for a DHCP server. This depends on how your network works.

If the program fails to find a DHCP server, he will go back to this selector.

If he can't resolve a Fully Qualified Domain Name (FQDN) for the IP he has been bound to, he will prompt you to tell it. If you are behind a NAT, you still need to provide it.

If you chose user-defined configuration, these are the parameters you will be asked for:

- ***IP address***: In 'A.B.C.D' format, being 0<=A,B,C,D<=255. The address for this server.
- ***Net mask***: Same format as the IP address. A binary mask to tell which portion of the address identifies the network and which part identifies the computer.
- ***Gateway***: Same format as the IP address. It is the router that gives access to computers outside the network the server belongs to.
- ***Primary/secondary DNS***: Same format as the IP address. The computer that will provide translation from Domain name to IP to the server. The secondary is the backup one.
- ***Domain name***: The human readable address for this server (same one as the FQDN mentioned above).

Network access will be configured and checked immediately after getting the parameters. Failing to do so will prevent from going further on the installation process.

Cyphered data location

You are prompted to choose one data access method among all supported methods:

- ***Local drive partition***: You will be prompted to choose among all the partitions of all the hard drives (real ones or virtual ones, like RAID units)

detected on the computer. The chosen one will be fully formatted with an encrypted file system.

- ***Remote directory with NFS***: A fixed size encrypted file system will be written on a file on the chosen directory on the remote server.
  - *Server*: (accepts both an IP address or a domain name). The host exporting the directory.
  - *Port*: (default service port, 2049). The port the NFS service is listening on the host.
  - *Remote path*: The path, inside the host, where the file must be written.
  - *File size*: (in MB). The size of the file containing the encrypted file system. Remember that it cannot be changed, so be farsighted when deciding on this parameter.

NFS configuration considerations.

The administrator of the computer providing NFS access might need to use this parameter when exporting the directory:

no_root_squash

That is because VtUJI works as root always and there's a known bug that prevents clients accessing as root from writing on the exported directory. Using this parameter requires better network configuration, since it is a potential source of security holes, but is the only way to workaround this bug. Please, do some tests before using this configuration on the server to see if it is needed or not.

- ***Remote directory with Samba***: A fixed size encrypted file system will be written on a file on the chosen directory on the remote server.
  - *Server*: (accepts both an IP address or a domain name). The host exporting the directory.
  - *Port*: (default service port, 139). The port the NFS service is listening on the host.
  - *Resource name*: The SMB resource, inside the host, where the file must be written.
  - *User*: The user name on the host through which VtUJI will access.
  - *Password*: The password associated with the user above.
  - *File size*: (in MB). The size of the file containing the encrypted file system. Remember that it cannot be changed, so be farsighted when deciding on this parameter.
- ***Remote drive with iSCSI***: The data will be written on a hard drive accessed remotely through iSCSI protocol. You will be prompted to write an address (IP or DN) and a port for the iSCSI target server that will provide a list of the available targets. If available, the program will scan the target and list all the available targets. Choose one. If the scan didn't work, you will be prompted to write a target identifier.
- ***File on local drive***: You will be prompted to choose among all the

partitions of all the hard drives (real ones or virtual ones, like RAID units) detected on the computer which have a valid file system. Besides each one, it has information about the current file system and its size. The file containing the encrypted file system will be written on the root of the chosen drive. After that, you will be prompted to write the size of this file system (the same as seen above).

Backup copy parameters

At this point, if you selected an storage system implying local storage, you will be prompted to choose if you want to use a remote SSH backup system.

The encrypted backup file will be written on the home directory of the specified user on the specified host.

> **SSH backup copy considerations.**
>
> The SSH backup copy is a single copy. This means that each time it is overwritten. It is the duty of the administrator of the host to keep a backup history if needed.
>
> Notice that the backup process is not a regular one. It's execution is controlled by some logic on the voting application, aimed at keeping it consistent. If you want to keep historic copies of it, do it on low usage moments of the voting application.

- ***Server***: (accepts both an IP address or a domain name). The host where the backup cop will be written.
- ***Port***: (default service port, 22). The port the SSH service is listening on the host.
- ***User***: The user name whose home directory will keep the backup copy. It should be a very lowly privileged user.
- ***Password***: The password associated with the user above.

The access to the backup server will be tested right now. Failing to do so will prevent from going on with the installation system.

Mailer parameters

You will be asked if your network configuration requires mail to be directed through a relay host (because some networks are firewalled for security reasons). If so, you will be prompted to input the address (***domain name only****; IP address is not accepted because it is not a direct access to the server, but a DNS lookup to see who is the mail handler for this domain*) of such mail relay.

Key sharing parameters

Now you will be asked for the key sharing parameters. They must have been decided by the committee before starting this installation process.

- ***Number of members for the Key Custody Committee***: (Minimum value: 2). The total number of members of the committee.

- ***Minimum number of members able to retrieve it***: (Minimum value: 2, maximum value: the above parameter). How many of the above could rebuild the key on their own. This provides certain redundancy, to keep safe from losses or failures.

At this point, the program will give you the opportunity to **review or change all the previous parameters**.
If you go on, the server time will be synchronized with an internet time server and the secure and random cyphering key will be generated and fragmented.

Key sharing

Each member will be prompted to plug a USB device, to be formatted as a Clauer.

Once it is detected, he will be prompted to write a personal password, which has to be at least 8 characters long (it shouldn't be an obvious one, for the sake of security) and repeat it to check for misspellings.

Both system configuration and a share of the key will be written on the Clauer, encrypted with the password.

Once it is written, he will be prompted to unplug it. **Doing so before being asked to may lead to data corruption.** You won't be able to go on until the program detects the Clauer has been unplugged.

In case of error (due to a defective USB drive, for example) the program will prompt for another USB device for this member and won't end until all Clauers are created properly.

System configuration

After writing the Clauers, setup will go on alone for a while.

The cryptographic data storage area is created, formatted, encrypted and a file system is created over it. This process may take some minutes, depending on the size of the drive (and network bandwidth or lag if it is a remote unit).

The mail server is launched, since it will be needed for the next configuration steps.

Web application basic parameters setup

Now, the program will ask for some basic parameters to configure the voting web application; that is, information about the administrator, who will later set up the rest of users and parameters from the web application, through a web browser.

- ***User name***: The unique identifier for the administrator. Use any name you want, but If you plan to use an external authentication method, use your user name on that method.
- ***Password***: The password he will use to log into the web application.
- **Full name**: The real name and surname of the administrator. Use any format, but the most accepted is Surname(s), Name(s).
- ***ID number***: Some number or code that is a unique identifier, available for each potential user and verifiable on a physical document, such as a

driving license, social security card or corporate ID card.

- ***E-mail address***: The e-mail address of the administrator. There, he will receive both voting application messages and system status and emergency notifications.
- ***Timezone***: Select the timezone where the voting system is going to be used (or the nearest to it) among all the proposed ones.
- **Key size**: The program lets you select among three key sizes to be used internally. This decision is currently not critical; but the biggest the key, the safest it will be over time, but also will require more processing time/ power to the voters and the server.

Regarding the user name.

You can create a whole new user name system for this application, since it works independently, but you could replicate the user names on your corporate systems, if you have them. There are some things to have into account.

If you don't have a corporate user name system, the best choice would be to use the ID number as user name, since it sensibly simplifies the establishment and uniqueness control of it.

If your organization does have a corporate user name system, it is recommended to use it but, since user name isn't usually written on the ID card, make sure that the association between the user and his user name comes form a reliable source. That is: load all the user data yourself or provide a lookup system for the voter registrars. Don't trust the voter's word.

At this point, again, the program will give you the opportunity to **review or change all the parameters of this block.**

eSurvey Sites Latency Network parameters and registration.

Now the system will ask you for the parameters to register this server on the eSurvey Sites Latency Network (LCN from now on), to allow voters to get an extra anonymity layer:

- ***E-mail***: The unique ID for your user in eSurvey Sites. It will also be used to receive notifications. If you **already have an account**, you can use it here.

You will receive an e-mail asking to confirm your account if it is a new one. If not confirmed, the account will be deleted.
https://esurvey.nisu.org/sites.php/

- ***Password***: You can choose between setting it or receiving an auto-generated one on the mail address. If you **already have an account**, choose to set it. It **must** be different from the one set above. It would be a severe security flaw.

eSurvey Sites

The LCN is used for multiple purposes besides Telematic Voting. If you are familiar with it, you will know that sites can be unsubscribed and operated in several ways.

Telematic Voting has some special needs: once registered and confirmed, the site will not be operated ever again and won't appear on the sites menu, to avoid giving the administrator power to disenfranchise voters.

- ***Organization***: The real name of your organization or the name of your server. It must be readable, since it will be considered for the acceptance on the LCN and voters will be able to read it.
- ***Name or purpose***: The name or the purpose of the voting system (just a few words long), to discern among various deployments on an organization. It must be descriptive and readable, since it will be considered for the acceptance on the LCN and voters will be able to read it.
- **Country code**: Two letter international country identifier (ie: FR, UK) from the country where your organization is established.

At this point, again, the program will give you the opportunity to **review or change all the parameters of this block.**
Once the parameters have been accepted, it will connect to eSurvey Sites and request the registrations. If any error happens, it will go back to the parameter definition to solve the problem. The program won't go on until the registration is done.

You will receive an e-mail asking to confirm your request before 48 hours or it will be discarded. Do it as soon as possible.
https://esurvey.nisu.org/sites.php/

The database server is launched and the database is created.

Web server setup

Now, the program will ask you if you want to set up a secure (HTTPS, secured communications, using an SSL certificate) web server or a plain one (HTTP, not ciphered connection). For tests purposes, it can be left plain; but if this deployment is going to be used to hold serious elections, **it is essential to set up a secure web server,** because even though the voting process would be protected and authenticated by the eSurvey system, local authentication and the rest of operations (reviewing participation, records or results) would be vulnerable to sniffing, man in the middle and other dangerous attacks.

If you choose to set up a plain web server, you can activate SSL later, on the maintenance menu, but yu'll need to gather the committee again.

If you choose to setup a plain server (after confirmation), it will be self-configured and this step of the installation will finish.

If you choose to set up the SSL server (after confirmation), you will be prompted to tell the **domain name** associated to this server (through which the users will access the voting system). The suggested value is the domain name specified/automatically deducted during network configuration.

Verify or edit the domain name and hit OK (then confirm).

You will be prompted to insert a USB drive (it won't be formatted nor destroyed) to keep the certificate request.

Once the request is written (along with some instructions for the solicitor of the certificate), you will be prompted to remove it.

Handle this USB to the one responsible of processing the certificate request to the certification authority (if it is not you).

> **If for any reason you need to read this request again, you can do it without authorization from the maintenance menu.**

The program will generate a temporary self-signed certificate to work with while you get the certificate signed. Most browsers will issue some warning because the server is presenting a self-signed certificate. Ignore it.

> If using SSL, all plain connections (http) will be redirected to the secure server (https), to avoid voters exposing themselves. This won't work the opposite way if using a plain server.

When the certificate is ready, in the future, you can install it from the maintenance menu without authorization.

Creating a Clauer for you

This step is optional, but you should do it if you don't have a personal Clauer device, since you will need it to gain the necessary access level on your first connection to the voting application to configure it.

If you have your own working Clauer, skip it.

Else, you will be prompted to insert a USB drive.

Once the program has detected its insertion, it will prompt you to input and repeat the password.

The drive will be formatted as a Clauer, but nothing will be written on it.

Once it is formatted, you will be prompted to remove it. You won't be able to go on until you do so.

Server is configured

You will be informed that the system is properly started.

Also, you will be informed that the administrator (you) have been awarded with privileged access to the voting application.

These privileges will be withdrawn as soon as the computer is rebooted or any action in the maintenance menu is selected (so abstain from hitting any entry on the menu for now).

If you accidentally revoked your privileges, there's a maintenance menu option to recover them temporary, but it requires authorization.

You will be presented with the maintenance menu. Some actions require authorization from the committee and some don't. These operations will be explained on section '*Server maintenance application usage guide*' (page 24).

Now it's moment to access the voting application through a web browser and finish the configuration.

Configuring the voting application

The final step is to configure some aspects of the web application. You should do this in front of the committee, but you will need the other computer mentioned on the requirements section. This could be done any other moment before setting up an election, but it has to be reviewed by the committee.

We will enumerate those aspects that need to be configured, but refer to the section '*Voting application usage guide: system administrator operations*' (page 33) to fully understand how each section of the interface works.

First administrator login

For this step you need another computer, with network connection with either Windows OS and Internet Explorer or GNU/Linux (any common distribution will work, as long as it is compatible with the Clauer software) and Mozilla Firefox 3.6.; any of them with the Clauer Software installed.

Open your browser and connect to the domain you set for the the voting application. If you set up the SSL server, you may be warned that the domain is providing an untrusted certificate. Ignore it.

At this point, you should insert your own Clauer (the one you have just created if you didn't bring one of your own)

On the main page, you will see some moving numbers. This is the logo of the internal authentication method. Click on it.

You will be prompted about this page wanting to read from the Clauer. Accept it. From now on, having this Clauer inserted when logging in will add one point to your authentication score.

Input your user name and password.

Then fill the CAPTCHA test (write the three numbers you can see in the image on the corresponding field).

Hit the enter button to log in.

From now on, if you connect to this application from the IP address associated with this computer, you will have one more point to your authentication score.

If there was some error, you will be notified with a red warning below the button.

If you entered the right credentials, you will be granted access to the application with at least one point in your score (plus IP and Clauer if that's the

case).

By now, you should have an score of three.

Voting application main page

On the main page you will see your name on the upper left corner and some colored areas. The uppermost area, in yellow, labeled '*operations as site administrator*' holds the operations that only your role can perform.

If you don't see this area, you did not gain the necessary score. Repeat the previous step and be careful.

Adding population

Your first step should be to add all the privileged users of the voting system: election managers, voter registry operators and, if needed, other system administrators (for emergency cases). Add them and then assign their roles. See section '*Voting application usage guide: system administrator operations*' (page 33) to understand how to operate this view of the application.

Also, this would be a good moment to add the whole population of the voting system (all the potential electors), if it is available. Otherwise, election administrators will have to do it.

If you need to edit your information, you can do it. Especially if you are using an external authentication method and your user name doesn't match your user name on the external method.

Configuring authentication

This is another critical point of the configuration.

If you only plan to use local authentication, it is over. Just be sure that your administrators keep their Clauers properly, since it will be the only way to gain enough score to access the administrator operations.

Some special authentication methods are provided natively with VtUJI.

Don't activate the IP authentication, since it works only to authenticate devices on a closed network.

STORK is an European project aimed at providing authentication across borders. You'll find more information on the usage guide below.

You can connect to up to ten external authentication providers. To do so, you'll need to develop a login gateway (follow the stub presented on the technical documentation). Just input here the URL where the gateway is hosted and use type '1' (the only currently supported gateway method. See the annexes for further information).

The issue of external authentication

Using external authentication methods is quite useful for maintenance and management duties, but having this external dependence when an election is ongoing is highly discouraged, since its administrator could disenfranchise voters with impunity.

To this end, VtUJI lets you establish different authentication profiles for each election, allowing or restricting some of the available methods or requiring some of them at the same time, all this at your consideration and adaptable for the needs of each election.

Note that for each available method through which a voter successfully authenticates, he will gain one score point, until reaching his maximum access level (which depends on the role). This means that he will be awarded the same score for each method, it doesn't matter how strong it is. Be careful and evaluate all authentication combinations and verify that they are strong enough for your standards.

Also, be aware that configuring the same external method twice will let a user gain two points by authenticating once with each entry. Be careful with this.

Minor parameters

- ***Help URL***: The destination URL for the help link on the header of the page (it must be an absolute address and accepts external links). It should be some corporate site where you give personalized information about the voting system or your electoral regime, specially those aspects that fall outside this application. There's a default help page you can use. Type:

  http://YOUR__DOMAIN/ayuda.html

- ***Error image***: Configure the image shown when the required image is not found. You can upload a personalized image.
- ***Default domain***: When you input user data, you can skip writing the domain of the email. It will be assumed that he belongs to the default domain. Here you set this domain.

The value of the default domain

There's not a default value for the default domain. You will be given a suggested value on the form field but, it is not stored until you hit the update button. If you don't store it, your e-mail addresses will have no domain and messages won't be sent.

- ***CSS***: This will let you change the appearance of the voting application to follow your corporate standards. This could take some time and need some expert manipulation.

eSurvey

This configuration area doesn't need privileges to be operated, and this step still can't be done.

Once your eSurveySites Certificate is signed, access this area and a 'Cert updated' message will appear (and the red error message will have disappeared). Make sure **it is done before holding any. Election**

If error messages keep appearing, please contact the administrator at eSurvey Sites.

Decrease management level

Once the configuration is finished, hit this button to withdraw your privileges.

The server went down. What do I do?

If the server was powered off, this is the procedure you must follow to restart it.

Before turning on the server

You must extract the CD-ROM and let the committee examine it.

Put it back and start the server. You will see the splash page for a while. Wait until the installation program is started.

Start-up program

The installation program will be started as soon as you see a dialog showing the version, the developers and the funders of the project. Hit OK.

Language Selector

Choose the language you want. This will be the interface language for this installation program. It has no effect on the voting application and it is not remembered. Each time you restart the system you can choose again.

Copying the CD to RAM

The same process as explained on the installation.

Main selector

The program will prompt you to insert a Clauer to load configuration from, to restart the system or to choose to format a new system.

Insert one of the commissioner's Clauers.

Choose **Continue**.

You won't be able to go on until you insert a Clauer.

Type in the correct password for this Clauer, for the configuration to be read.

If the program can't find any configuration data, or it is not a Clauer, or you decline to provide a password, he will send you back to the main selector.

Start-up menu

If configuration was correct, you will be prompted to select an action to be done.

- ***Start voting system***:Start the voting system normally.
- ***Recover a former installation***: If the data support broke down, this entry lets you build a brand new system and to restore the newest data backup copy from an SSH server (further information on page 44)
- ***Launch root access terminal***: An action for emergency situations. Lets you launch a full access terminal at this point. Data area is not mounted, network is not configured and services are still down, but lets you get into the system to try to diagnose it.
- ***Shutdown system***: Shuts down the system, if you don't want to go on.

Choose **Start voting system**.

The key fragment will be read now. And you will be prompted to remove the Clauer (the program won't go on until you do so).

Key reconstruction

At this point, you will be prompted to input another Clauer (the program won't go on until he detects that you did so).

Type in the correct password for this Clauer, both the key and the configuration will be read.

The read configuration will be compared to the previous one. If they differ, it means that either it is corrupted or it was deliberately manipulated by the owner of that Clauer. You will be shown both configuration files and you'll have to compare them and select which one to use.

> Once the system is started, perform a key renewal (further information on section '*Server maintenance application usage guide*', page 24) to assure that the proper configuration is stored on each Clauer.

After that, you will be prompted to remove the Clauer (the program won't go on until you do so).

This Clauer solicitation loop is infinite, since the program doesn't know how many commissioners are present. After each loop, you will be asked if there are still Clauers to be inserted.

If there are problems with some Clauer, try repeating with the same one.

If you run out of Clauers and accidentally got into the loop again, just repeat the process with one of the Clauers that has yet been read. The program may warn you that some fragments are corrupt, but don't pay attention.

Once you stop inserting Clauers, the program will try to rebuild the key. Upon failure, it will try to recover by rebuilding the key testing each possible combination of the fragments he has. This process may take some time.

Anyway, the program will later test that all the inserted fragments are valid,

and warn you to reset the key as soon as possible if it finds some irregularity.

Service startup

If the key rebuilding was successful, the system will be started autonomously.

First, network configuration will be set up.

Then, the data area will be accessed and mounted.

The key fragment verification algorithm described earlier is passed now. You may be warned to renew the key.

And finally, mail server, database server and web server are started.

If you chose to, the backup service is activated now.

The program will inform you that it was successfully started and will be on standby at the maintenance menu. Some actions require authorization from the committee and some don't. These operations will be explained on section '*Server maintenance application usage guide*' (page 24).

After restarting, the administrator is **not awarded privileges** on the voting application. If you need them, you'll have to use the maintenance menu entry.

Which are my duties during operation?

Once the system is set up, there are some regular duties you must assume to guarantee the continued and trouble free operation of the server.

- **Finish the registration process on eSurveySites**: Regularly access the eSurvey screen on the web application until you are notified that the certificate is installed. If you have any trouble, contact eSurvey Sites administrator (see page 15 for further detail).
- **Monitor the server**: Verify that all the parameters are normal (temperatures, drive and memory usage, etc.) use the maintenance interface on the same server (see page 30) or the remote statistics page (see page 50). If there's any trouble, gather the committee for a maintenance session (see maintenance guide at page 24).
- **Maintain the SSL certificate**: The SSL certificate has a expiration date. Be aware and make sure that you have it renewed as soon as it expires or gather the committee to act with foresight in case you see that the expiration might fall on an election period. See page 27 for details.
- **Verify the key fragments periodically**: Gather the committee to verify that all the fragments are correct and nobody has forgotten his password. Choose a frequency to avoid bothering the commissioners, especially if their number is big, for it would make it difficult to gather them at the same time and the process would be long and tedious. See page 25.
- **Arrange the execution of maintenance sessions**: It is your duty to coordinate or to communicate with a coordinator to gather the committee

to get authorization for any maintenance operations you would detect that are needed. Be sure to study what needs to be done and the severity of the situation, and communicate it ahead of the reunion to the committee so they can object or arrange to bring a technician with them to control the actions.

- **Maintain old elections**: The voting application has an interface to clean heavy and useless data from old elections, to improve the application efficiency. It is your duty to seek the authorization of the committee and the election authority to perform this task on the elections that they allow to.
- **Be on call during elections**: You or some delegate administrator must be on call on electoral periods, to quickly react to any unexpected situation that may affect to the results of the election, thus mitigating its extent.
- **Maintain physical polling posts**: You or some delegate administrator must be assigned on call to do maintenance on location for any deployed physical polling post that may experience network or hardware failures, or any other technical issues.
- **Maintain registration posts**: You or some delegate administrator must be assigned on call to do maintenance on location for any deployed registration post. This is not as critical as the above, since their function extends over a long period of time and it is not so critical.

Server maintenance application usage guide.

In this section we explain all the maintenance actions available on the system menu. Some of them (harmless) can be performed without authorization, but most of them will require the reconstruction of the key in order to acknowledge that you are under surveillance of the committee when performing this action.

Each action will require the reconstruction of the key, since it is the only way to assure that any action is performed under surveillance of a sufficient amount of officers. An scheme where you would rebuild the key once to start a maintenance session and would close it at the end would be way more convenient but dangerous if the committee forgot to close the session, since anyone could do harmful actions with impunity.

All the actions marked with (U), do not require authorization to be performed.

Give temporary privileges to the administrator

Will give access to the privileged operations on the voting web application until they are revoked.

First, it will demand the Clauers and rebuild the key the usual way. If you fail or abort this process, you will be sent back to the menu.

You will be prompted with a message telling that the administrator now has privileges, and they will be revoked when you hit OK (and select withdraw on the confirmation prompt).

You will be sent back to the maintenance menu.

Reset administrator credentials

Will let you change your password and reset your associated Clauer and IP address.

First, it will demand the Clauers and rebuild the key the usual way. If you fail or abort this process, you will be sent back to the menu.

A prompt will show the user name of the administrator (in case he is absent and you don't know it).

You can change your voting application password now.

Additionally, you are given privileges on the voting application, which will be withdrawn as soon as you perform any other maintenance operation, much like at the end of the installation.

You will be sent back to the maintenance menu.

Create new administrator

Will let you create a new administrator user, or give this status to an existing one.

First, it will demand the Clauers and rebuild the key the usual way. If you fail or abort this process, you will be sent back to the menu.

A prompt will let you input your user name. If it already exists, the program will update the data for it.

You will be prompted to set your voting application password.

Now, it will ask for your full name.

And your ID number.

And finally your e-mail address.

From now on, all the system notifications and warnings will be sent to this address instead of the former administrator's.

Additionally, you are given privileges on the voting application, which will be withdrawn as soon as you perform any other maintenance operation, much like at the end of the installation.

You will be sent back to the maintenance menu.

Verify key shares integrity

Will let you verify that all the key fragments are correct.

First, it will demand the Clauers and rebuild the key the usual way. If you fail or abort this process, you will be sent back to the menu.

The integrity of the fragments will be verified.

If there's some error, **Renew data ciphering key** procedure will be triggered.

Else, you will be informed that they are alright and you will be sent back to the maintenance menu.

Renew data ciphering key

Will let you change the key that is shared among the Clauers, and change the sharing parameters.

> **Data area encryption scheme**
>
> The file system in the data area is cyphered using LUKS, which follows a double key scheme. Data is cyphered using an **inner key**, which is stored in an special header area and cyphered with one or more **outer keys**. This way, adding or deleting outer keys is an easy and simple task, and the real cyphering key is never exposed.
>
> Changing the inner key is a dangerous and not supported operation, so it usually requires transferring the data to another encrypted data area.

This operation will change the outer key.

The procedure is failsafe. If something may happen (like a power failure), the system can be restarted using the old key until the moment the sharing of the new key is done. That's why you must use a new set of USB drives to write the new key.

First, it will demand the old Clauers and rebuild the key the usual way. If you fail or abort this process, you will be sent back to the menu.

After that, you must input the sharing parameters. Old values will be suggested.

The new key is generated.

The new Clauers are demanded to be written. Same process as during the installation.

Once the key is shared, old key will be deleted and the old Clauers can be stored for other uses.

You will be sent back to the maintenance menu.

Move data to new location and set new key

Will let you change the inner cyphering key for security reasons and also relocate data to a new location, to prevent hardware failures or due to administration/efficiency reasons.

This operation requires you to prepare a different data storage location, the way described at the beginning of this guide. You will be warned only if you are trying to use the same partition/drive on local drive mode or the same target on iSCSI mode, because you need both file systems at the same time to make the transfer. Since the other modes write the encrypted file system inside a file, a new file will be created on the same location.

The backup server parameters can be the same as on the old location.

The procedure is failsafe. If something may happen (like a power failure), the system can be restarted using the old key until the moment the sharing of the new key is done. That's why you must use a new set of USB drives to write the

new key.

You will be prompted to input the following set of parameters (see installation section for details):

- Data Storage parameters.
- Remote backup parameters (depending on your data storage selection).
- Key sharing parameters.

The new key is generated.

The new Clauers are demanded to be written. Same process as during the installation.

Once the key is shared, the new data storage area will be created.

All the data will be transferred there. This may take long.

The new copy of the data will be checked for copy errors. If something may happen, the old data area won't be destroyed, so you can access it using the old Clauer set.

If everything went as expected, the old data will be securely deleted. This process is quite slow and may take a long time.

If SSH backup is still in use, an immediate backup will be performed.

You will be informed that you can now dismiss the old Clauers.

You will be sent back to the maintenance menu.

Operations over SSL web server certificate

This variable entry contains all the operations related with the setup of the secure web server (using SSL and a certificate).

Since it is a continuous process, it passes through several states.

Switch to web server with SSL certificate mode

If you configured the web server as plain, the only entry will be to activate the secure mode.

The process is exactly the same as in the installation. Refer to that section to solve any doubts.

The server will be started using a temporary self-signed certificate.

You will be sent back to the maintenance menu.

Read certificate request again (U)

If for any reason (you lost it, it was corrupted, etc.) you need to read again the certificate request, you can do it from here, without authorization.

You will be asked for a USB drive.

After it is written, you will be sent back to the maintenance menu.

> **Obtaining the certificate request remotely**
>
> Besides the menu entry, the certificate request can be read at any moment (even after the certificate is installed, since it is necessary to renew it without changing the private key) from the following URL:
>
> http://YOUR__DOMAIN/server.csr

Install certificate (U?)

Once you have your certificate signed, you need to install it.

This option applies for the installation of the first certificate, the renewed certificate without changing the private key or the new certificate changing the key.

This option **can be executed both with or without authorization**, depending on the situation. If you try to do it when there is a valid certificate, you will need authorization. Otherwise, when the certificate is self-signed or it has expired, you will be able to do it without authorization.

The program will ask you to insert the USB drive containing the certificate.

Once it is detected, he will let you choose the certificate file with a file selector.

The program will ask you to insert the USB drive containing the certification chain (all the authorities from the one that sign the certificate to the root one).

Once it is detected, he will let you choose the chain file with a file selector.

Both the certificate and its chain will be checked. They must be in PEM format, the certificate must match the private key and the whole chain must be trusted (the root authority must be among the ones trusted by the system). Or else, the installation will fail and you will be sent back to the menu.

Renew certificate and private key (U?)

If your certification authority doesn't allow changing your key to renew the certificate after its expiration, provide them with the request you got at the installation (you can read it again from your web server, at http://YOUR__DOMAIN/server.csr), and then install the certificate they give you.

If your certification authority requires to generate a new key, follow this process.

This option **can be executed both with or without authorization**, depending on the situation. If you try to do it when the certificate is still valid, you will need authorization. Otherwise, if you do it when the certificate has expired, you will be able to do it without authorization.

You will be asked the same as on the installation, and the new request will be written on a USB drive.

The main difference is that the server will keep working with the old certificate (either it is valid or expired) until you get to install the new one.

Change mail server parameters

This option lets you change the mail server configuration. Even though this data is written on the Clauers, you won't need to rewrite them.

First, it will demand the Clauers and rebuild the key the usual way. If you fail or abort this process, you will be sent back to the menu.

You will be prompted to set the new value for the parameters.

They will be written on the data storage area.

The mail server will be reconfigured.

You will be sent back to the maintenance menu.

Change network configuration parameters

This option lets you change the network access configuration. Since it is basic configuration data, it needs all the Clauers to be rebuilt (also, the shared key will be voided and a new one will be written on the Clauers. Any commissioners not present will find their Clauers invalidated).

First, it will demand the Clauers and rebuild the key the usual way. If you fail or abort this process, you will be sent back to the menu.

You will be prompted to set the new value for the parameters.

The network access will be reconfigured and tested.

You won't be able to go on until the server verifies that it has network access.

You will be redirected to the parameter form after each attempt.

If the configuration is valid, the program will switch to the **key renewal** procedure.

You will be sent back to the maintenance menu after the Clauers are written.

Change remote backup copy parameters

This option will not appear if you chose not to use a remote backup service. It will let you change the location and access parameters for the SSH backup server while the system is running.

Since it is basic configuration data, it needs all the Clauers to be rebuilt (also, the shared key will be voided and a new one will be written on the Clauers. Any commissioners not present will find their Clauers invalidated).

First, it will demand the old Clauers and rebuild the key the usual way. If you fail or abort this process, you will be sent back to the menu.

You will be warned about the need for a new set of Clauers. If you decide to abort the operation, you will be sent to the menu.

Fill the new values for the SSH backup service.

As usual, you won't be able to go after the accessibility of the server is verified.

If the configuration is valid, the program will switch to the **key renewal** procedure.

You will be sent back to the maintenance menu after the Clauers are written.

Reset system stats gathering

This option lets you restart the gathering of system statistical data. It is intended for the event that the hardware of the server changes, so you will need to update the sensor list. Don't do this for fear of using up all the storage space. The space used by the stats database is bounded.

First, it will demand the old Clauers and rebuild the key the usual way. If you fail or abort this process, you will be sent back to the menu.

You will be prompted to confirm that you really want to restart the statistics.

Once they are restarted and the new array of sensors is detected and configured, you will be informed.

You will be sent back to the maintenance menu.

You can access this statistical information using this public URL.
http://YOUR__DOMAIN/statgraphs/hourly.html

System status monitor (U)

This options offers real time statistics of the system. They are slightly more detailed than those shown on the graphs at the URL.

You won't need authorization to see this data.

Each time you need to refresh the data you'll have to press REFRESH.

To go back to the menu, press BACK.

The information shown is the following:

- **Date**: Date and time of the last refresh.
- **Uptime**: The amount of time elapsed since the last system reboot.
- **Idle**: Percentage of the uptime that the system has spent doing nothing. An indicator of the system load.
- **Load 1m, 5m, 15m**: An average measure of the system load for the last minute, five minutes and fifteen minutes respectively. This value is bound by the number of processors/cores/threads available on the system. It will be the sum of a value between 0 and 1 for each processor available.
- **CPU**: The percentage of the CPU capacity on use at the refresh moment.
- **Memory**: The percentage of the system memory (RAM) on use at the refresh moment.
- **Interfaces**: Shows a list of all the network ethernet interface cards of

this computer and tells for each one if it is transmitting and/or receiving data at the refresh moment.

- **System temperature sensors (if available)**: Shows a list of all the temperature sensing devices connected to the computer (all of them are named) and, for each one, it shows all his sensors and the temperature they are registering at the refresh moment (in Celsius degrees). *This is useful to diagnose cooling problems that may lead to hardware failures.*
- **Fan speeds (if available)**: Shows a list of all the fan control devices connected to the computer (all of them are named) and, for each one, it shows all his fan controllers and the speed they are registering at the refresh moment (in revolutions per minute). *This is useful to diagnose cooling problems that may lead to hardware failures.*
- **Hard drives**: Will show a list of all the hard drive units connected to the system (with its manufacturer and model between parentheses if available). Each one will provide the following information:
  - **Reads**: How many blocks per second are being read from this drive at the refresh moment.
  - **Writes**: How many blocks per second are being written from this drive at the refresh moment.
  - **Temperature (if available)**: The temperature at the hard drive sensor, in Celsius degrees. *This is useful to diagnose cooling problems that may lead to hardware failures.*
  - **Partition usage (if any)**: Will list all the partitions on the drive and show their current usage and the total amount, in human readable units (MB, GB, etc.) and on percentage.
- **Special partition usage**: VtUJI has two special partitions that need special consideration. Shows their current usage and the total amount, in human readable units (MB, GB, etc.) and on percentage:
  - **Encrypted data area**: The real data area where the information of VtUJI is stored. It can be located in many places (iSCSI drive, local drive, loop back file system on a file on an NFS directory, SMB directory or local partition directory). This is the real indicator of how many space is left for VtUJI to store data. If this file system is full, VtUJI won't be able to store election information and ballots, so get sure that you have enough storage space.
  - **RAM file system**: Since VtUJI is distributed in a CD-ROM, it needs some space where to store the information that needs to change during the operation of the system. To this end, it creates a file system over the RAM system memory, that uses half of it and will disappear when you reset the computer. If the CD was copied at the beginning, you will see an increase in this usage. If this file system is full, VtUJI won't work properly, so get sure that your server has enough

RAM.

Suspend computer (U)

The best way to protect the system against attackers, extend the life of the hardware and save energy when it is not being used at all is to power it off. To avoid having to gather the committee every time we want to restart it, we can simply suspend the computer.

You don't need authorization to suspend it.

Confirm that you want to suspend. Else, you will be sent back to the menu.

The server will go down.

When you want to power it up, just hit the power key on the computer and you will be sent back to the maintenance menu.

Launch root access terminal

This is the last resort when trying to solve server problems and the other menu options don't work. Be careful with what you do over sensitive information and the persistent data area. Any changes over temporary partitions can be undone by rebooting the computer.

First, it will demand the Clauers and rebuild the key the usual way for authorization. If you fail or abort this process, you will be sent back to the menu.

You will be prompted to warn you about how critical is this operation.

You will be shown a text area. There you must write the e-mail address for every person interested in receiving a copy of the list of all the commands that you will input during the terminal session, for auditory purpose (one address per line).

You won't be able to go on if any address is badly formatted.

The terminal will appear. It has no job control, so you **won't be able to use signals** (like Ctrl+C to end a program), so be careful with launching programs with infinite loops (like ping) or you will have to do a hard reboot on the system.

Once you have finished your work, write '*exit*' to get back to the maintenance menu. The e-mail with the session log will be sent now.

Shutdown system (U)

You don't need authorization to shut it down (any attacker has more expeditious ways to shut it down).

Confirm that you want to shut down the computer. Else, you will be sent back to the menu.

The system will execute the shutdown sequence.

You will be requested to extract the CD-ROM and hit ENTER.

Voting application usage guide: system administrator operations

We will present here the different operations that can be performed by the system administrator over the voting web application, and a description of the interface elements of each screen. Notice that the layout may change if you edit the CSS, but all the elements will be present.

You will notice that the system administrator can perform all the actions of any other role, but we'll explain them on their corresponding role guides.

Privilege level

The administrator role is a quite critical one. He needs to be able to perform some maintenance actions that could affect the integrity of the elections and be used by accident or maliciously. Thus the committee, as the sole depository of confidence needs to assure that they can't be performed without their authorization.

To this end, the administrator operations are divided into two groups: privileged and unprivileged ones.

- **Unprivileged operations:** Help URL, Error image, eSurvey (some actions)**.**
- **Privileged operations**: population management, polling post committees management, default domain, CSS editing, authentication configuration, eSurvey (some other actions).

There is a **second level of privilege**, but it cannot be gained by common means. It is intended for extremely rare situations, and it needs to be gained through a full access terminal (see page 32). The operations at this level include: voting web application remote update, ballot box key regeneration, and eSurvey Sites certificate renewal.

Also, when the system administrator is in privileged mode and performing election manager functions, **most of its integrity restrictions may be overridden**, even on closed elections. So you will be able to change all the parameters without restriction, so be very careful when working on privileged mode.

Authentication score

At the beginning, each user is assigned a role, classified by the sensibility of its functions (see population section below).

By default, all of them are awarded role 0, and depending on their functions, they can be promoted.

The execution of each role's functions requires reaching a certain authentication score:

- 1: Voter
- 1: Polling station officer or chairman ([1])
- 2: Voter registry operator
- 2: Election manager
- 3: System administrator

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[2]).

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 from will be recorded).

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.

---

1 In some special cases, like opening a troubled ballot box, the polling station chairman may be required an score of 2. He will be informed adequately.

2 See http://clauer.nisu.org/ for more details.

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.

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:

- System administrator operations (default: yellow)
- Election manager operations (default: pale red)
- 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)

The number of shown areas depends on the role associated with your user and the score you have currently earned.

Population

On this screen you will be able to add, check and edit the information of every system user. Two views are available depending on what you are doing: the user addition view and the user listing view, being the first one the default one.

- ***Letter map***: The upper part of this screen is constant, and shows a map of buttons, one for each letter, arranged like a Qwerty keyboard, plus an All button. Besides the letter, there's a number on each button. It is the number of users whose *Surname,Name* starts with that letter.

User addition view

- ***Text Area***: Below, there is a text area where you can add users (one per line), using the format explained next to it. We'll deepen on this later.
- ***Load from file check box***: If checked, push 'Add' and you will be shown a file upload form. Use it to load a file from your computer containing users; one per line and using the same format that you would use on the text area. Select the file and push 'Add' again. A progress meter will appear to show the upload progress, and then another one will appear to show the data processing progress.
- ***Add button***: Pushing this button will automatically add all the users declared BOTH on the text area and the file to upload.
- ***Download button***: Will download a comma separated file containing the data for all the users currently on the system.
- ***Delete button***: As it tells, it will delete all the users that are not listed on any election voter rolls. Use it only if you need to clean the user list.

User input data format

These are the fields that you can set on input, the rest can be edited later. Each line represents one user, and has the following format:

username!idNumber!Surname, Name

or

username!idNumber!Surname, Name!emailAddress

Obviously, none of the fields may contain the character ! As part of its content.

- **username**: the user name that identifies each user in any computer system. They can be created expressly for this system, but if the members of your organization already have usernames, it is highly recommended to use them, since they will remember it easily and you'll be able to use external authentication systems, as we'll explain later.
- **IdNumber**: a unique identifier for every user. Many countries or corporations assign an id number to the citizen/employee (id Card, Social Security number, etc.). This is what is expected in this field. Again, it can be created expressly for this system, but it is highly discouraged. It must be present in some physical, difficult to forge, card issued by the organization along with visual information (a photograph) to *let a registrar personally verify the link between the person and his ID*.
- **Surname, Name**: The full name of the user.
- **EmailAddress**: Optional, but recommended. The personal email address of the user, where he will receive notifications. It can be a corporate account. You can specify it three ways:
  - *Full email address*: username@domain, the classical way.

- *User name*: if only the user name is given, VtUJI will assume that the domain is the default one. See page 40 for more information.
- @: If you only write an @ character, VtUJI will assume that the *username* is that specified earlier as the user name for vtUJI, and the domain is the default domain.

User listing view

- ***Letter buttons***: Pushing any letter button will change to the user list view, showing a list of users whose *Surname,Name* field starts with that letter ('All' will list all the users).
- ***Pagination***: If the number of users is large, it will show a pagination interface on top of the list. Where you can **sort the user list** using the main fields and jump to another page. The amount and size of the pages depends on the number of selected users and are shown on a **page selector** at the beginning of the list. Push 'Update and jump' to go to the selected page or sort the list.
- ***Discard button***: Pushing this button will discard any changes you have made on the user data and will get you back to the user addition view.
- ***User list grid***: Will show the selected users on an editable grid, one per line and with all its information fields.

User grid fields

- ***Id***: An inner unique identifier. Not editable.
- ***User***: Explained earlier.
- ***UserId***: Explained earlier.
- ***Surname, Name***: Explained earlier.
- ***eMail***: Explained earlier.
- ***Role***: A number, indicating the role of the user on the application. This is which functions are available for him. Each level can perform the functions of all levels below it.
  - 0: Voter / polling station officer or chairman
  - 1: Voter registry operator
  - 2: Election manager
  - 3: System administrator
- ***Password***: The field is blank. It is used to set the inner authentication temporary password.
- ***IP***: The IP address where this user first logged in (presumed to be his usual address). -1 indicates that it is not yet registered. The value shown is represented as a signed integer, not in standard IP notation (255.255.255.255), but in can be set using both notations.
- ***ClId***: The unique identifier of a Clauer physically belonging to the user. -1 indicates that it is not yet registered.

Some **fields may be** disabled, namely, their full name. They contain sensitive

information from people who has been linked with an election (either as polling post officer or as candidate). Since their names are registered in the records and ballots, changing them would leave the system inconsistent, so their values may not be changed until they stop being related with any election on the system. This restriction can't be overridden on higher privilege levels.

Editing and deleting a user

To commit any changes to this view, hit any letter button (or 'All'). Any other action will end losing all the changes.

Hit discard to dismiss any changes on the view.

Any field not disabled can be changed, but User, UserId and eMail are unique fields. If there's any problem submitting the changes, you will be prompted.

- *To delete a user*: Set all fields blank and then commit.
- *To set/change the password*: Type it in plaintext on the corresponding field. It will be temporary (48 hours), after which, it will be voided if not changed for the definitive one.
- *To reset the Clauer Identifier or IP address*: Set the value -1. The next time the user logs in their values will be read again.
- *To set the usual IP* address: Write it in standard notation on the corresponding field. It will be stored and shown in signed integer notation.

Polling post committees

This screen is a management interface for all the closed polling posts (containing one or more elections; see the election administrator guide for further information). Shows information about them and lets you delete the voter rolls and ballots if you need to for legal reasons or storage space needs.

Each line represents a closed election, and has the following elements:

- ***Edit button***: Will load the election edition interface for this closed polling post, where you can review and change data.
- ***Record button***: Will show the results record for all the elections of this closed polling post. Even though you edited any data, the record won't be altered.
- ***Empty rolls and ballot box button***: Deletes the voter rolls and all the ballots stored on the database for each election on the polling post. This way you can fulfill legal requirements and clean the system for a better future performance. Be careful, since it will delete them **without asking for confirmation**.
- Name of the polling post.
- Name and e-mail of the election manager who created this polling post.

Help URL

This screen lets you set the URL associated with the help link located on the header.

Initially, it won't have any value, and the link will direct nowhere.

Write it on the text box and hit 'Update'.

The URL must be complete, including domain and protocol. Otherwise it won't be updated:

http://DOMAIN/path/

It should be some page where you show the information you want to give to your users, but you can provisionally use a help page included with the application:

http://YOUR_DOMAIN/ayuda.html

Error Image

This interface lets you choose the image that will be shown anytime that an image is required and is not available. Also, it can be used to upload images for other purposes (change the header logo, candidate photographs, etc.)

Images can be public or not and hidden or not. Public images can be requested without being authenticated, and hidden images won't be shown in this interface unless you force to do so.

For each image, you have the following fields:

- ***Select***: The currently selected image to be used, which will be effective when you hit back
- ***Name***: The name of the image. Erase it and hit Update to delete them from the system.
- ***Image***: Click on it to select.
- ***Public***: Whether It is public or not (can be accessed without being autehnticated).
- ***Hidden***: Whether It will be shown on the list or not.

At the bottom, we find the upload form and the action buttons:

- ***Upload image***: If you check it and hit 'Update', you will be shown a file upload dialog. To upload a file from your computer, select it in the dialog and hit 'Update'.
- ***Load from web***: Write here an image's URL to download it from the Internet.
- ***Update button***: Submits all the changes (deletions, uploads, etc.)
- ***Back***: Gets back to the calling screen, returning the selected image as the chosen one.
- ***Show hidden images***: If you check it and hit 'Update', hidden images will be shown on the image list. Uncheck it to hide them again.

Default domain

This interface lets you configure the default e-mail domain (see the *Population* section to know its use).

Initially, it won't have any value, so if you declare addresses without domain, mailer program won't know where to send the messages.

The first time you access it, YOUR_DOMAIN will appear as a suggested value, but it is **NOT SET**. Unless you hit update, this suggested value will not be stored and internally it will remain empty.

eSurvey

This is the interface to manage all the aspects related to the compatibility with eSurvey Sites[3].

Sometimes, using eSurvey may generate log entries, irrelevant most of times, but sometimes they reflect real user incidences that may be tracked using these logs.

On the upper side of this screen, error messages about the validity of the eSurveySites certificate will appear. If the certificate has been signed, it will be downloaded and you will be notified by a log entry.

Hit 'Refresh' to reload the log list.

The clean logs button will delete all the logs (privileged mode) or old logs (unprivileged mode).

If there are too many logs, it will show just some and allow you to load the rest.

For each log entry, you have this information (some of them are buttons):

- ***Reference code***: A code to track the package in the origin node. Contact an eSurveySites specialist to know how to use it.
- ***Origin IP address***: Which node came the package that has generated the log entry from.
- **Survey ID**: The identifier of the election the package was addressed to. If it couldn't be guessed (the package couldn't be deciphered) it will be '-'
- Log message.

Hitting any of these buttons will filter the logs and only show those that have the same value on that field (same IP, same reference code, etc.).

Unprivileged mode

You are only allowed to see the logs and delete old logs (various days old).

3http://esurvey.nisu.org/sites

Privileged mode

You are only allowed to see the logs and delete all logs.

Special privilege mode

The following options will appear. The are for emergency situations. Use them only if the keys have been violated. Make sure that there are not ongoing elections:

- ***Regenerate ballot box key***: If checked, it will destroy the current ballot box key and generate a new one.
- ***Regenerate signing key and certificate***: If checked it will the current eSurveySites certificate and request a new one. Follow same the procedure as in the installation. The server will be operative (although its signature will be untrusted)
- ***Proceed***: Will execute the checked options among the previous.

Software update

This option will appear **only if you are in the second privilege level** (which needs to be activated from the inside of the server)

It will check if the application is already up to date or if there is a new version available. If there's a new version it will let you download it (the software is signed. Don't worry about eavesdroppers).

This is an emergency measure in case of big security flaw on the application. Installing new software is not encouraged because it would break the confidence chain established when installing the server.

Be aware that when you **reboot the server**, the software will **fall back to the previous version**.

CSS

This screen shows you the CSS code used as the layout for the page. You can change it to match your corporate appearance. Use a CSS expert to edit it.

Manage authentication

This page will let you configure the different available and some new authentication methods. These will be the available methods to access the application, and any subset of them can be defined to be used for each election.

The four kinds of authentication methods are:

- ***Internal***: The basic internal authentication we have previously commented at length.
- ***IP***: Authenticates you by the IP address you are connecting from. Don't use it on common installations where users must authenticate themselves. It is intended only for deployments over protected networks where you need to identify the requesting device/computer, not the person who is using it.
- ***STORK***: An European project to provide a network of servers capable of

communicating with identity providers across Europe and provide authentication capabilities while encapsulating the source.

- ***External***: Any external authentication provider that you might want to use. Since VtUJI can't understand all of them and is not allowed to include external software, we provide a stub implementation of a gateway that you must personalize and host on one of your servers to bridge with the external authentication service. In this gateway model, VtUJI will redirect the solicitor to the specified gateway and when the solicitor comes back, VtUJI will ask the gateway if the he was successfully authenticated and will expect to receive his user name. If it matches a user name on the system, he will be granted access.

The interface elements are the following:

- ***Update***: Hit it to submit any changes
- ***Methods***:
  - ***Method***: The internal name of the method.
  - ***Name to be shown***: The name that will be shown in the authentication method selector.
  - ***Image***: An image representing the authentication method that will substitute the previous name.
  - ***Available***: Check it if you want to make this method available or disable it temporarily (configuration won't be lost when disabled).
  - ***By default***: Choose which will be the default authentication method (initially will be the Internal authentication)
  - ***Type***: *Only for external authentication methods*. It tells the kind of gateway you are implementing. Currently, there is only type 1, so use it.
  - ***URL***: *Only for external authentication methods*. The address where you are hosting the authentication gateway.
- ***Jump to default***: If checked, when you are accessing the application and you are not authenticated, you will be directly sent to the default method page, skipping the method selector page.

The default authentication

Deciding on which method must be the default one is an important question. If you activate the 'jump to default' option, this method's screen will be the first screen they will always see when accessing the application.

Furthermore, once you are assigned a temporary password, before logging in with the local authentication and getting the permanent password you will be required to log in with the default authentication method, as an extra security feature for the credential distribution process (evidently, if the local is the default authentication method you won't be required nothing).

STORK Configuration

- ***Use the test PEPS***: Since STORK is still under development, mechanisms for public access and registration over the network are not decided yet. If you want to try it, check this option and you will access to the test PEPS server. Be aware that quality of service is not assured on the test server.
- ***Countries of the world***: A list containing all the countries in the world. STORK infrastructure requires every participating country to have a central PEPS server. Select which countries you know that already have a PEPS and you want to rely on.
- ***Your provider name***: If not using the test PEPS server, write here the descriptive name of the service you are providing which will be seen by the users (also tell that it has to do with telematic voting).
- ***Your provider ID***: this is a unique structured identifier string awarded by a central broker organization which is still not available.
- ***Your country (as provider)***: The international two letter country code where your voting server is located. Use uppercase.
- ***PEPS URL***:The address where the PEPS server you will be requesting is hosted. It is your entry point to the STORK network. Contact your country PEPS server administrator.
- ***PEPS certificate***: The certificate of this PEPS server, to reliably verify signed responses. Contact your country PEPS server administrator.
- ***Update***: Click it to submit the changes.
- ***Certificate to be sent to PEPS***: The certificate that your server will use to sign the requests to your PEPS. He may need it to authorize and verify your requests. Contact your country PEPS server administrator.

Decrease management

Hitting this button will immediately revoke the privileges for the administrator, if you need to do it without physically accessing the server machine.

System backup pending message

Sometimes, you might find a message on the system administrator area telling that there is a pending system backup. It may appear if you are using SSH backup and will be there until the next backup check finds it and performs the backup. Then it will disappear.

If not performed, a server failure might lead to a data loss

There's not a determined time for it to disappear. It depends on the size of the backup file and the bandwidth to access the backup server.

If you find that it is there for too long (some hours may be too long), contact the backup server administrator to check the situation and the link between both machines, and arrange a maintenance session to access the server and diagnose the cause.

For emergency situations

In this section, we will provide information that may be useful when things go wrong. Most of them are tips about how VtUJI works, but there are other

Recovering a backup of the server

When a former copy of the voting system is needed (because we need to restore that previous state or a hardware failure caused the destruction of the current data), you must do the following.

Start up the system

Begin the same way you would on a normal startup (see page 21) until you reach the start-up menu. There, select '**Recover a former installation**'.

New Installation

To restore a backup, the program will first need to perform a new installation on the current grounds (if due to a hardware failure, you would be recovering it on a different machine, possibly on a different location). We'll show only the differences with the initial installation.

Warning

After accepting the license, we will be warned. The **Clauers used in this installation** must be **different from the used in the former** one, since we will need them at the end of the installation to obtain the parameters and keys to decipher the backup copy.

Configuration Parameters

We will only be asked for the basic parameters: *networking* parameters, *data location* parameters, *SSH backup* parameters (if applicable, and referring to the new installation, not the old one), *mailer* parameters and *key sharing* parameters.

The rest of parameters will be taken from the backup copy.

See the corresponding sections for further detail.

Reconstruction of the former key and backup parameters procurement

After creating the new data storage area, you will be prompted to insert the former Clauer set, in order to get its configuration data and key shares.

The procedure is the same as on a regular system start-up, so refer to that section for any doubt.

Backup copy retrieval

Once the key is rebuilt, the program will access the former SSH server and retrieve the cyphered backup file.

The file will be deciphered and each file will be relocated on the data area.

Any problem happening until this point will restart the process from the moment you are requested the former set of Clauers.

The services will be restarted and the database will be restored.

If the database restoration fails, you will be prompted with the emergency menu, so you can try diagnosing the issue with full access.

RAID unit manipulation

If you deployed your VtUJI server over a Linux Sofware RAID drive, here are some examples and considerations you should take into account:

Create a Linux software RAID

Being hda1 and hdc1 two drives/partitions of the same size and md0 the identifier of the RAID drive we want to create:

mdadm --create /dev/md0 --level=raid1 --raid-devices=2 /dev/hda1 /dev/hdc1

This will create a RAID 1, which mirrors all the data on both drives, providing data redundancy.

A super block containing the RAID information will be written on each drive.

Create a partition table

This command sequence will create a single partition over the RAID drive

- fdisk /dev/md0
- c (dos compatibility off)
- u (units to sectors)
- o (new table)
- n (new partition)
- w (write partition table)

Check the state of the RAID

To check the state of the RAID unit:

mdadm --detail /dev/md0

To check the state of one of the drives:

mdadm --examine /dev/sda

If you execute this command:

cat /proc/mdstat

You will see this string:

[UU]

containing one 'U' for each unit attached to the RAID. If there was any degraded drive, the 'U' would be switched for an '_':

[U_]

Check the state of the operations over the RAID

Using *cat /proc/mdstat*, you can check the progress of long operations over the RAID, like a reconstruction or adding a new unit.

Reconstructing a degraded RAID

Suppose that the drive/partition hdc1 from the md0 RAID is broken. Follow this steps:

This will mark the drive as failed:

mdadm --fail /dev/md0 /dev/hdc1

This will remove the failed drive from the Array:

mdadm --remove /dev/md0 /dev/hdc1

Shut down your computer and substitute the broken drive

Be careful when substituting drives

Careless handling of the dive substitution process may end in a total loss of your data, so follow carefully this guidelines:

- **Clean any reused drive before attaching it**. Especially if that unit belonged to another RAID, because conflicting RAID information will end up in a bad synchronization and data loss.
- **Each drive must be attached to the same port that it was before**. Since Software RAID identifies its units by the port they are attached to, connecting a working drive to the port where the failed drive was would end up confusing the working unit with the failed one and probably dismissing all the data. If a degraded unit with old data was connected to the port where the working unit was, **they would synchronize with the old data, not the new one**.

We erase all possible leftover RAID information on the new drive, in case it came from another array:

mdadm --zero-superblock /dev/hdc1

Finally, we add the new drive to the RAID:

mdadm --add /dev/md0 /dev/hdc1

At this point, the synchronization process will start. You can check its progress the way stated above.

System RAID notifications

If a RAID is detected, VtUJI server activates a RAID monitor to continuously check the state of the array. In case there was any problem, an e-mail would be sent to your address.

After booting the system, you will be sent a test message showing the state of the RAID. If you don't receive the message and you know that there is a working RAID, you will never receive any RAID notifications, risking a future data loss. Start tracking the cause for this malfunction (from the mail server to the internals of VtUJI, with a Root access terminal. Use the maintenance options you need).

System RAID malfunction message

This is how a malfunction message looks like. It will be sent to your e-mail in the event of a failure.

```
This is an automatically generated mail message from mdadm
running on DOMAIN

A DegradedArray event had been detected on md device /dev/md/0.

Faithfully yours, etc.

P.S. The /proc/mdstat file currently contains the following:

Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5] [raid4] [raid10]
md0 : active raid1 sdb[1]
      488386452 blocks super 1.1 [2/1] [_U]

unused devices: <none>
```

It will tell the domain name of the computer operating the RAID, an error message (degraded array in this case) and a dump of the command *cat /proc/mdstat*.

Miscellaneous tips

Mail is not being received

Did you set user e-mail addresses without domain? Are you sure that you hit the update button on the default domain configuration screen?

Problems during boot process

If you access the system with a root terminal, you will find that the contents of /var/log directory never show the boot process messages. That is because logs are stored in the encrypted data area and at some point, they are linked to the standard log directory.

All the logs generated prior to this moment, are stored at /var/currbootlogs directory, just in case you need them to diagnose any problem.

They are reset after each reboot.

Annexes

VtUJI Server Live CD interface usage considerations

The graphic user interface of the installer and maintenance applications of the Server Live CD is implemented with *Dialog,* a Toolkit whose widgets have some peculiar behavior that needs to be explained to be used properly:

Dialogs

All dialogs will have at least one **action button**. If there's more than one, they can be **navigated** with the **TAB** key. The selected one will be highlighted with a different color.

To **execute** the selected button, press **ENTER**.

Check boxes

When facing a list of check boxes, you can **navigate** it using the **ARROW keys (up and down)**.

To **select** or deselect a check box, press **SPACE**.

Forms

To **navigate** the fields in a form, use the **ARROW keys (up and down)**. The selected field will be highlighted with a different color and the cursor will be inside the field.

The **action buttons** will be accessed by pressing the **TAB** key. The form will be part of the navigation of the action buttons (so, if the form has two buttons, to get back to the form we will have to press TAB three times).

File dialogs

There are three areas:

- *Directory Tree* (upper left): Shows the directories inside the working directory (the currently selected one), plus the meta directories: '.' (current directory) and '..' (parent directory).
- *Directory content* (upper right): Shows the files inside the working directory.
- *Path* (bottom): Shows the current absolute path. It can be edited.

To **navigate** between the areas (and the action buttons), press **TAB.** The selected item will be highlighted by color or cursor position changes, but it can sometimes be subtle. If you **can't guess** on which area you are, press TAB button until you detect an area and then count. The areas will be navigated in this order:

path, all the buttons, directory tree and finally directory content.

Once selected, the directory tree and directory content areas can be navigated with the **ARROW keys (up and down)**. The selected item will be highlighted, but notice that its content won't be showed on the directory content area and it won't be added to the path.

To select a directory as a part of the path, select it and press **SPACE**. It will be added to the path but it's content is still not shown.

To open a directory, select it and press **SPACE** twice. It will be added to the path and it's content will be shown on the corresponding area.

To select a file, select it and press **SPACE**. It will be added to the path.

Editing the path will immediately cause the update of the content shown at the directory tree and directory content areas.

Using **alphanumerical keys** will always switch focus to the path area and the path will be edited.

To **execute** the selected button, press **ENTER**. The path written on the path area is the one to be used at the moment the button is executed.

System statistics page

This page can be accessed remotely through the web server. Since it doesn't offer any sensitive information it has public access.

It can be accessed on the following address:

http://YOUR_DOMAIN/statgraphs/hourly.html

The last update date of the page is shown on top. All the graphs are presented in four detail periods:

hourly, daily weekly and monthly.

Click on the link to see the information available for this period.

Each graph will present data in one of this ways:

- **Absolute value**: It will present the exact value read by the sensor at that point. To represent bounded data or when the useful information is in the value itself.
- **Differential value**: It will present the difference between the last and the current values read by the sensor. This way, a horizontal line represents a value that grows at a constant rate. Useful for data that is always growing, to avoid overflowing the counters, and when the growing/decreasing rate is more important than the value itself.

Now, we'll enumerate all the graphs and the information represented on them:

System Memory usage graph

(*Absolute*). The percentage of system memory (RAM) currently in use

System load graph

(*Absolute*). The load average of the system. This is an abstract metrics about the workload of the system. It is bounded between 0 and N, being N the number of processors/cores/threads on your computer.

Core sensors temperature graph

(*Absolute*). The temperature value, in Celsius degrees, for each available temperature sensor on the chipset, motherboard or any other sensing device.

Hard drive temperatures graph

(*Absolute*). The temperature value, in Celsius degrees, for the temperature sensor on any SMART compatible hard drive.

Hard drive read blocks graph

(*Differential*). It will show the variation rate for the number of read blocks for each available hard drive. A steep curve means a sudden increment on read disk accesses.

Hard drive written blocks graph

(*Differential*). It will show the variation rate for the number of written blocks for each available hard drive. A steep curve means a sudden increment on write disk accesses.

Network interfaces, received bytes graph

(*Differential*). It will show the variation rate for the number of received bytes, through each ethernet interface on the system.

Network interfaces, transmitted bytes graph

(*Differential*). It will show the variation rate for the number of transmitted bytes, through each ethernet interface on the system.

Petitions served by the web server graph

(*Absolute*). It shows two data sources: The number of petitions served by the Apache web server and the number of server kilobytes.

Web server CPU and memory usage graph

(*Absolute*). It shows two data sources: The percentage of system memory (RAM) and the percentage of the CPU capacity currently used by the web server processes.

File systems usage graph

(*Absolute*). It will show the current percentage of space used on any available disk partition on the system. Additionally, it will show the usage for the special partitions:

- **EncryptedFS**: The effective amount of space used inside the encrypted data area, regardless of the method used to allocate this data area.

- **RamFS**: The amount of space used on the volatile file system over which the system is working. If the CD was copied to RAM, it will be reflected here.

eSurvey

eSurvey is a project aimed at providing real and total anonymity to all its users. It is highly fault tolerant, anonymous by cryptographic means and its origin is absolutely untraceable, physically and temporally.

The key elements of this project are the eSurvey client (and its variant the eSurvey toolbar) and eSurvey Latency Network (LCN). It is a network of servers, hosted by independent and trusted organizations that receive and relay the packages containing the ballots/surveys without any knowledge about the content and the path it is following on the network. Additionally, each node will retain the package for a random period of time, established by the client.

The client, written in Javascript and totally multi—platform and installation-free, wraps the package with a set of encrypted layers using the public key of each node (and the destination server) he wants the package to travel through , being the inner layer cyphered with the destination server key and the outer with the first node in the path. Each layer has information about the next node and how much time must be the package retained. The client chooses randomly the path and the retain time at each server.

Two dates are defined, the closing date and the end date. The packages are wandering the network for some time until no more packages are admitted on the election (**the closing time**). After this time, and before the **end time**, all the packages will be sent to the server. This way, even if there are only two votes, you can't discern who sent which ballot.

This way, the destination server is not able to relate an authenticated user (it knows the authentication time and origin IP address) with the origin IP and arrival time of the package, thus making it impossible to establish a correlation between a voter and his vote. The only way to do it is that all the organizations owning the nodes which the package went through would collude and reveal the information to the destination server, but this is absolutely impossible.

The client needs to trust the key of the server to avoid impersonators (that would make the voter believe that they are sending their vote to the legitimate destination server), so your server key must be signed by the eSurvey Sites authority.

To use eSurvey, you just need to distribute the client, modify your server to understand the eSurvey package format and register the server on the eSurvey Sites. VtUJI fully supports eSurvey anonymity system as a way to allow the mistrustful voter to take control of the situation and participate on the election with anonymity guarantees obtained by his own means.

The only way for a voter to be sure that he is not being cheated is by following these steps:

- Understanding the whole eSurvey system and why it will guard his anonymity.
- Obtaining the eSurvey Client from a reliable source and/or perform an auditory to check that it will work the expected way.

- During the voting process, to have the certainty that you are using the client you have obtained and trust and you aren't being cheated to use a tampered client.

eSurvey toolbar

VtUJI distributes the Javascript client, which is totally transparent to the voter, but is loaded from your VtUJI server, so a mistrustful voter has no guarantees that he is not being eavesdropped by the destination server itself (yet vtUJI servers, if deployed properly, are totally reliable, the confidence chain may not be clear enough for you). This is the rationale for the eSurvey Toolbar.

The eSurvey Toolbar is an independent eSurvey client, developed as an extension for the Mozilla Firefox web browser platform (works on all operative systems).

He can easily download and install it from the following address:

http://paco.nisu.org/eSurvey/eSurvey.xpi

Since it is a locally installed, wholly developed in Javascript client, the voter can get it from the source he wants and audit it as deeply as he wants.

It has been developed to counter any possible tampering attempt coming from the server and imposes itself clearly. It is designed to be clearly distinguishable from any attempt from the server to trick the voter into using a false client.

The bar can be activated by the voter at will, before or after marking the ballot, and use the bar to cast it after he is done.

Voting Booth computer securing

If you were to deploy physical voting booth, it would need a computer where an undetermined number of users could log into the voting system and cast their ballot without being supervised, due to their right to secrecy of vote.

The problem is that using a non-secured computer would open the gate to an attacker to access this computer while in the booth and tamper it to violate the secrecy of the voters that follow him or, what is worse, secretly alter the content of their ballot at will.

We need to alter the computer both physically and logically to close all the attack vectors. The following are the requirements a computer should fulfill to be suitable for this task.

There is a project for a Live CD that will satisfy all the logical security requirements but it is still under development.

Logical

- Protection on the access to the BIOS and the boot process, to prevent bootstrapping to a root terminal or any other dangerous actions.
- The only interface a user should be able to get after booting is a web

browser. No desktop, no terminals and no way to kill the application or launch any other system applications.

- The web browser should include the eSurvey toolbar as the voting Client, to provide higher security standards.
- The remote access to the computer should be totally locked using the system firewall.
- No superfluous local services and no updates.
- The capabilities of the browser should be reduced: No extension installation, no means to change the configuration or browser preferences, no cookie or cache storage or not accessible information.
- The only URL that could be loaded on the browser is that of the voting system.
- The browser should not be able to load local files, especially those which could reveal system flaws to .

Physical

- No available connection ports (USB, Firewire, CD drive, etc.). The central unit of the computer should be isolated from the voter, on a security box or outside the voting booth and guarded.
- The only elements available to the voter should be a mouse, a keyboard and a screen, with protection against vandalism.
- Don't use wireless keyboards, mice or network connection. They can be tampered or jammed.

External authentication gateway development

As we have stated previously, VtUJI can communicate with external authentication systems, but to do so you need to implement and host a gateway that will link the protocol that VtUJI can understand, with the wide variety of corporate authentication methods.

The protocol is the following:

- VtUJI will redirect the user to the gateway when asked to authenticate via this method, providing the return address in the parameter 'reto'.
- The gateway will check if the user is authenticated. If not, the gateway must do whatever he needs to authenticate the user (*show the user some authentication interface, query any other site, redirect the client to some corporate sign on page, etc.*)
- Once the gateway knows that the user is successfully authenticated, it must store the user name in session and redirect the user to the return address in VtUJI, sending the parameter 'reto_auth' with the session id.
- VtUJI will connect to the gateway again passing the session id (the name of the parameter is configurable, to avoid collisions with the interaction with the) and the gateway will respond with the user name of the authenticated user.
- Then VtUJI will check that the returned user name belongs to one of the

valid users of the system.

- When the user disconnects from VtUJI, it will call the gateway with the parameter 'exit' with value YOUR_DOMAIN (that is, the domain belonging to your VtUJI server).

Example implementation in PHP

Now, we provide a commented PHP implementation that will illustrate what we stated above. The **red colored code** is that specific for this implementation and must be changed for your code. The **green colored code** are the variables and request parameters that can be renamed in case you have collisions with the code to contact the corporate authentication server. Make sure to change all the occurrences of the word that are in green.

The beginning of the code must always be the session establishment. If 'sid' parameter is passed, then that previous session will be used. This will be done by VtUJI when coming back to ask the user name.

```
<?php


if ($sid=$_GET['sid'])
    session_id($sid);
session_start();
```

After that, you must check the case that VtUJI is coming back to ask the user name. Just get the stored user name for the authentication session he has provided and print it alone on the page. (If the user did not successfully authenticate, return an empty page). Don't write any HTML code. Destroy the session information when done. The session parameter name

```
if ($sid) {
    $arr['login']=$_SESSION['login'];

    echo serialize($arr);
    session_destroy();
    session_unset();
    die();
}
```

Now, it's time to include all the libraries you might need to perform the authentication on the corporate server.

```
require_once("lsm/lsm.inc.php");
```

At this point, you must treat the logout case. The value of '**exit**' parameter will

be the domain who is calling this (the domain of your VtUJI server), because your corporate authentication server might need it to selectively invalidating authentication to sub-domains.

```
if ($url=$_REQUEST['exit']) {
    lsm_logout($url);
    die();
}
```

Now you must do what you need to authenticate the user. This may require redirecting the user to another service and bringing him back, showing a form or contacting another service directly. Anyway, there are some restrictions you must follow:

- Have the '**reto**' GET parameter available at the end of this phase. Either by propagating the gateway URL with at least this parameter on it, or by not overriding the value of this parameter while implementing the authentication. Feel free to change the source of the value of this parameter always that you know what you are doing.
- The '**exit**' GET parameter is reserved for the logout procedure. Do not use it on your communications with the corporate authentication server.
- The '**sid**' GET parameter is also reserved for the solicitor to query the user name, but can be changed for any other, since the gateway is sending both the value and the name of the parameter in the response. Just make sure you don't use this parameter in both communication sides.

In this example, lsm_get_login() will query the corporate Single Sign On (SSO) to check if the user is already authenticated. If not, it will perform a redirection to the SSO login page and then it will be sent back to the gateway. He will check again and, as he gets the user name, the process will go on.

```
lsm_login("");
$login = lsm_get_login()
```

If the authentication was successful, you have got the user name of the authenticated user; store it on the session (in this case, we store it on the login field, but you can change it) and prepare to go back to the return page that your VtUJI server provided on the first request (on 'reto' parameter).

The destination address (the return address to VtUJI) expects one more parameter: '**reto_auth**'. The structure of the content of this parameter must be the following:

?sid=THE_CURRENT_SESSION_ID

That is, the session id for this authentication process, which is needed by VtUJI to later request the user name. The name of the parameter, 'sid', can be changed if it is already used in the communication with the corporate authentication server.

After that, the user will be redirected th the original solicitor, your VtUJI server.

```
if ($login) {
   $_SESSION['login']=$login;
   if ($url=$_GET['reto']) {
      $rah='reto_auth='.urlencode('?sid='.session_id());
      header("Location: $url$rah");
      die();
   }
   header('Content-type: text/html; charset=utf-8');
   die('Call');
}
header('Content-type: text/html; charset=utf-8');
die('Error');
```

An implementation consideration

For the sake of simplicity and clarity, this implementation is a bit loose. You should notice that if the return address already has parameters on it, the 'reto_auth' parameter will be attached without the separator '&'. Most navigators and web servers can negotiate and recover from this situation, but if you want a failsafe application, insert some conditional code before the *Location* line to determine whether to put the separator or not.

Here is the above code in one piece. It is a working gateway to a currently used corporate authentication system:

```php
<?php

if ($sid=$_GET['sid'])
    session_id($sid);
session_start();


if ($sid) {
    $arr['login']=$_SESSION['login'];
    echo serialize($arr);
    session_destroy();
    session_unset();
    die();
}


require_once("lsm/lsm.inc.php");


if ($url=$_REQUEST['exit']) {
    lsm_logout($url);
    die();
}


lsm_login("");
$login = lsm_get_login()


if ($login) {
    $_SESSION['login']=$login;
    if ($url=$_GET['reto']) {
        $rah='reto_auth='.urlencode('?sid='.session_id());
        header("Location: $url$rah");
        die();
    }
    header('Content-type: text/html; charset=utf-8');
    die('Call');
}
header('Content-type: text/html; charset=utf-8');
die('Error');
```