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

UNIVERSITAT JAUME·I

FONDO SOCIAL EUROPEO

VtUJI
Telematic Voting System

Usage guide for the
Key Custody Committee Member

Id:	VT-D05
Version:	1.0
Date:	June 30 2011
Authors:	Francisco Aragó Monzonís Manuel Mollar Villanueva

Table of Contents

Presentation

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.

The present document will describe your duties and the procedures you will have to execute while holding your charge.

Your role

The position you are holding is the key of the functioning of VtUJI. You and your companions are the holders of the confidence of all the electorate and candidates. They trust that you will be overlooking and you won't let a single interest party take control over the voting system, tampering it against the interests of the segment of voter you are representing.

Besides your common surveillance and verification duties, you also will be the proxy between any of the voters or candidates who you are representing and the voting system. Any time they wish to reassure their confidence on the voting system, they will do it through your action.

Neglecting on the proper execution of all the security procedures both when deploying the system and when operating it would produce a breach in the solidity and integrity of the system.

Duties

This is a comprehensive list of all the duties you will take with this position:

- To produce a reliable copy of the VtUJI CD to be used on the server.
- To guard a personal verification copy of the CD.
- To guard the Clauer containing a piece of the cyphering key, using and remembering a secure password and keeping it in a safe place.
- To be available to review and renew periodically the cyphering key.
- To start the voting system after any eventual power failure.
- To authorize and watch over the legitimacy of the system administrator's operations on the system in case of contingency, even requiring the need of an independent technician.
- To perform/order auditories on the system in case of suspected fraud or CD substitution.
- As long as they are the holders of the electorate's confidence, they can be addressed by any voter or individual representing a set of them. As far as possible, it is their duty to fulfill their demands on system auditing and calm their concerns on procedure compliance.
- To be available to be summoned to authorize emergency maintenance operations or restarting the server in case of a failure. The urgency of these gatherings will depend on each situation, varying from some days to some hours.

Procedures

Now we provide a description of all the procedures you may face. They are distributed in three categories.

The ones in the *setup procedures* section are those you must perform when deploying the server. They must be executed in the order they are described here.

Those in the *regular procedures* section are intended to be performed during the normal operation of the system, either periodically or as a response for some unwanted situation.

Finally, the *emergency procedures* are those designed as a contingency response to unexpected situations, developing either from a deliberate attack or from a severe system failure.

Setup procedures

Selection of the operating disk

To be executed prior to the deployment of the VtUJI server.

The system administrator or any other supplier must provide a set of VtUJI disks equal to the number of committee members plus one (you can ask them to get VtUJI and record the disks in front of you if you are suspicious about their origin).

- The whole committee and the system administrator will gather on the room where the server is allocated.
- A random committee member will shuffle the disks and another random member will select a random operating copy. Each committee member will handwrite his personal signature over it, using a permanent marker. This way, it can be visually verified or forensically analyzed in case of suspected disk substitution or signature forgery.
- The rest of the disks will be distributed among the commission. With the only purpose to allow performing auditories over the working copy.
- Each member will sign his disk and the ones on his left and right. This way, each disk is verified by different members and no one possesses all the signatures, thus hardening the forgery work for an external attacker.
- Each member is responsible for the protection of his copy against robbery or substitution from an attacker.
- If desired, any member can now verify that his copy is identical to the working one (see SE-03, 'operating disk verification' procedure).

Voting system establishment

Once the operating disk is chosen and signed, the system administrator will proceed to do the deployment and setup of the application.

Read this section before starting this process.

- You are here to overlook the actions of the system administrator and avoid him to do anything irregular. If you believe you don't have the required technical skills, obtain the counseling of a third party qualified technician, who will advise you on your moves.

- Don't forget to verify that the used disk is the one you have signed, ask to check your signature before it is inserted. A substitution here would be catastrophic.
- At the beginning of the installation, you must check if the **VtUJI CD is copied on system memory (RAM) or not**. It will do it automatically if enough resources are detected, but sometimes it won't be done. If not, you shouldn't allow the usage of the server for elections and complain to get the server machine upgraded to allow it. This must be done every time the server is started.

> Although VtUJI can be operated without copying the CD on RAM, it is **highly discouraged**, because any attacker with physical access to the server computer could substitute the working CD for a tampered one and it wouldn't be noticed until the disk is verified.

- During the installation process, you will be required to set a password for a Clauer USB device guarding your fragment of the key. The password must be long and secure enough. This means:
  - 8 characters long at least.
  - Combine uppercase and lowercase letters and numbers.
  - No personal information on the password (dog's name, birthday date, number of sons, etc.)
  - Try not to use full words, to avoid being attacked with a dictionary. Break them and insert numbers in the middle.
- Keep the password secret at all costs, and guard the device safely and properly. Don not insert the device at any untrusted computer. Use it on the VtUJI server exclusively.
- This device will keep a fragment of the cyphering key. To do any sensitive operation on the server, a number of the fragments which will usually differ from the total number of fragments will be needed. This parameter is set during the installation and will have been decided by the election authority prior to this process. **It is your duty to check that this minimum number of fragments to rebuild won't allow a faction of the committee with common interests to access the server on their own accord**.
- Remember that when you and the rest of members of the committee insert your Clauers and type down the password, you are giving authorization to the system administrator to do dangerous changes and/or access sensible data or the system. **In a proper installation, you won't be required to insert the Clauer except when writing it**. Don't do it unless you know what is really going on.
- You should have been informed by the election authority of the parameters to be used and the people to be inserted as holders of the different roles of the system. Follow the installation process carefully and check all the parameters inserted by the administrator.

- Once the installation over the server is finished, the administrator will access the voting application through a web browser on another computer. Follow his actions too. To do so, the system administrator has **special privileges on the voting application**, and these must be withdrawn at least before starting to create an election.
- If he is done with all his work, **withdraw the privileges** now (either from the control on the voting application or accessing any menu entry on the server). Else, **remember to do it before starting to plan the first election**.

Regular procedures

Some of these processes must be done regularly and others depend on certain situations. Each of them will be marked. The election authority, with the advice of the system administrator, will settle a periodicity for them.

Key fragments integrity verification (Periodical)

This procedure must be done with a certain frequency (about once each six months or higher if the usage of the voting system is more intense), to detect lost fragments due either to hardware failure or human error (forgotten passwords, erased Clauer, lost Clauer, etc.).

- The committee will gather on the room where the server is allocated
- All the members must be present, not just the minimum number to rebuild.
- Each of them will be required to insert his Clauer and type in its password.
- When all of them are done, it will try to rebuild the key.
- If any fragment is faulty, you will be prompted to renew the key

Key renewal (Periodical)

This done should do with a low frequency, like yearly, but is quite important since will reduce the key loss probability and the success odds of any attack.

- The committee will gather on the room where the server is allocated.
- All the members must be present, not just the minimum number to rebuild.
- Failing to do so would generate complaints from the members excluded from the custody of the new key.
- Each of you will be required to insert your Clauer and type in its password. Old key will be rebuilt to check clearance.
- A new key will be generated.
- Each member will be given a new USB drive to be formatted as Clauer and protected with a password.
- A fragment of the new key will be written on it.

- Once all the key fragments are delivered, the old key will be erased and the old Clauer set can be stored for a future use or discarded (if faulty).

System reboot

This procedure must be executed every time the server goes down due to power failures or any other cause, planned or unplanned (like a hardware substitution).

- The committee will gather on the room where the server is allocated.
- All the members must be present, not just the minimum number to rebuild.
- Failing to do so would generate complaints from the members excluded from the custody of the new key.
- At the beginning of the installation, you must check if the **VtUJI CD is copied on system memory (RAM) or not**. It will do it automatically if enough resources are detected, but sometimes it won't be done. You shouldn't allow operation without copying the CD on RAM and if not possible by memory limitations, complain to get the server computer upgraded.
- Each of you will be required to insert your Clauer and type in its password. Old key will be rebuilt to check clearance.
- A new key will be generated.
- Each member will be given a new USB drive to be formatted as Clauer and protected with a password.
- A fragment of the new key will be written on it.
- Once all the key fragments are delivered, the old key will be erased and the old Clauer set can be stored for a future use or discarded (if faulty).

Common Maintenance operations

When the system administrator determines that he needs to perform common server configuration changes, for any reason related to the functioning of the system or the changes on the network configuration or anything, he will arrange a meeting of the committee to do some maintenance.

The maintenance actions are those programmed on the maintenance menu, so the administrator will have little room for mischief. Even though, at certain moments executing this programmed actions can be still dangerous, so if you are not sure, ask a third party technician.

- The system administrator should inform you of his planned actions, so you can check with a technician or arrange to bring one to the session, so he can survey the actions. As the system administrator if you need more information.
- The committee will gather on the room where the server is allocated.
- The minimum number of members to rebuild will be enough.
- If an election is ongoing, this procedure is far more critical, and technical supervision is required, not suggested.
- The administrator will choose the action he needs to perform. Check that it is safe to perform it at this moment (consult the technician).

- Each of you will be required to insert your Clauer and type in its password.
- When all of you are done, it will try to rebuild the key as a clearance check.
- The administrator will perform the operations he has been granted to.

This process of authorization through the rebuilding of the key must be done for every action the system administrator wants to perform. This is the only way to assure that he can't execute anything by mistake.

If the problems aren't solved this way, you will have to give him unrestricted access to the system, that is an emergency procedure, very critical, and you will need to provide intense technical supervision.

Emergency procedures

The following procedures are those which you will execute as a contingency to respond to anomalous situations.

Key fragments compromise

If some commissioner reports that he has lost or believes someone had access to the key fragments by any means, you must execute this procedure to void the risk of key revelation.

Once the key fragment compromise is reported, the first step is to evaluate the extent of the compromise and the potential key revelation risk:

- How many fragments have been compromised?
- The attacker may have had access to an unencrypted copy of the fragments (like if the Clauer was used on a untrusted computer where the attacker was monitoring the password input) or it was just lost?
- The encryption password was secure enough?

As long as a number of fragments less than the minimum needed to rebuild the key was lost, there's no immediate key compromise danger. Unless, of course, that the attack wasn't organized by a part of the committee, who could use also the fragments under their control to rebuild the key.

Anyway, estimate the danger and arrange a meeting of the committee as soon as possible. **All the members must be present**.

The data is stored cyphered with an inner key, which is stored inside the drive encrypted by an external key which is the one fragmented on the Clauers.

If the risk of key revelation is low (not enough fragments were revealed), you will have to ask the system administrator to perform an external key renovation.

- A new set of Clauers with key fragments will be generated.
- The system will remain the same, no data relocation will be needed.
- You will be asked to input a new password for the Clauer. Use a different

password that on the previous Clauer.

If the risk of key revelation is from moderate to high (there's a minimum possibility that enough fragments could have been gathered to rebuild the key), the inner cyphering key should be changed (see next section).

The violation should be reported and legal action should be taken by the election authority if it was a deliberate attack.

Inner system key renewal and data relocation

The data is stored cyphered with an inner key, which is stored inside the drive encrypted by an external key which is the one fragmented on the Clauers.

For security reasons or if there's risk of storage hardware failure, VtUJI data may need to be relocated to a new device. This is the process

- The committee must be gathered. All the members must be present.
- It will require a new data storage area, and the relocation of all the data from the old one to the new one.
- The system administrator will stop the server if he needs to add new hardware.
- The new configuration will be applied. The new data area will be set up and all the data will be transferred. It may take some time, depending on the amount of data stored on the voting system.
- A new set of Clauers with key fragments will be generated with the key of the new area.

Operating disk verification

This procedure is essential to assure the confidence of any member of the committee on the VtUJI copy that is running on the server, and thus, the confidence of any voter or candidate.

First of all, if the last time the server was booted the CD was copied on RAM, you can rest assure that no one with physical access to the server machine could have tampered the working copy, even if he substituted the CD. Else, if the CD was not copied on RAM, you must trust that no one switched the CD.

- The aim of procedure is to check that the CD working on the server is exactly the same than the one in possession of the committee members who are doing it. The legitimacy of this copy of VtUJI must be checked earlier or later by a thorough auditory of its contents performed by an specialized technician.
- If the copy of any participating commissioner is revealed to be unfaithful, this process should be executed to determine the extent of the problem (perhaps the only tampered copy is his copy).
- The committee will gather on the server room.
- The minimum number of members to rebuild will be enough, but it is recommended to gather all of them.
- The member who initiated this procedure must bring his own trusted technician to perform the verification and his trusted material (a computer

with a CD drive).

- Each member must bring his own copy of the CD
- Each one of the remaining members can be accompanied by a technician to overlook and/or reproduce the actions of the previous.
- The working copy will be extracted and handed to all the members, so they can verify their handwritten signature.
- The verification process will be to obtain the hash value for each CD using different common secure hashing algorithms (SHA1, SHA256, MD5, etc.)
- The working copy will be handed to the designated technician to obtain the hashes, they will be posted somewhere visible.
- The working copy will be handed to the system administrator to obtain the hashes for confirmation.
- The working copy will be handled to any other technicians brought by the commissioners, one at a time, to obtain the hashes them too.
- This process will be repeated with all the personal CD copies. CDs have to be handled one at a time, to avoid substitutions or mix ups. Anyone must be able to see each result.
- If any of the results differ, all the different copies must be audited to check which is the legitimate one.
- Legal action will be taken to discover who is responsible for introducing tampered copies.

Voter/Candidate system auditing

As stated earlier, the commissioner is a confidence proxy between the voting system and the voter or candidate.

This way, any voter can obtain a copy of the VtUJI working on the server from the copy possessed by the commissioner, to perform or order his own personal auditory on it.

Otherwise, the voter can obtain his copy from any other trusted source and check it against the commissioner's in the way described on the previous procedure.

On a further step, the voter can request a working copy verification to the commissioner, to check that the CD on the server is the same he audited.

In an extreme case of mistrust, the voter can be present during the execution of the working copy verification.

Unrestricted access to the system

Most maintenance operations that the system administrator will have to perform on the voting server's life are implemented as common procedures and can be launched in a controlled fashion, but some situations are so variable or unexpected that can't be implemented this way and need to be solved by his experience and exploration of the system elements. That's why you have the option to give the administrator full system access.

You have to be aware that **this is a highly critical task**. The system administrator will have access to all the data and all the programs used on the voting system, and leaving him alone would let him tamper the system or steal data in such was that would be catastrophic for the voter/candidate confidence.

It is really important that you bring a trusted technician to monitor all the commands introduced by the system administrator. You must understand and evaluate every single command typed in by the administrator and evaluate its potential threats.

- The committee will gather on the room where the server is allocated.
- The minimum number of members to rebuild will be enough.
- This procedure is extremely dangerous, since the administrator will have the power to do anything over the data and the applications. At least one technician must be present to check the administrator's action.
- Each of the commissioners will be required to insert his Clauer and type in its password.
- When all of them are done, it will try to rebuild the key as a clearance check.
- After that, each interested member or technician will be asked to input his e-mail address, to receive a register of all the commands used by the administrator, so he will later be able to audit this log deeply.
- The administrator will be prompted with a terminal.
- Some dangerous actions may not be registered by the log system. This is why it is essential to have a second technician to oversee the administrator's work.
- The administrator will have to explain each action before performing it and give time for the technicians to take notes.
- After solving the problem, the administrator will close the terminal session and return to the idle state.

Note for the technicians.

All the commands of the session are registered and sent for a later analysis, but there are ways to execute commands avoiding their registration. That is, opening other terminals. On this machine all terminals are shut down, but if you execute this command (or something similar, changing the tty number for example):

```
/bin/bash >/dev/tty3 </dev/tty3 2>&1 &
```

It would launch a new terminal accessible on the TTY3 port which is accessible by pressing the key combination META+F3.

The commands executed on this terminal are not written on the session register and, when you end the maintenance session by closing the main terminal, this one will remain open, giving the system administrator a perfect back door.

Do not let the system administrator open any extra terminals and, if absolutely necessary, review specially the commands he executes on this terminal and make sure it is closed after the session is finished.