UNIVERSITAT JAUME·I

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

plan avanza

FONDO SOCIAL EUROPEO

VtUJI
Telematic Voting System

Executive Information

Id:	VT-D01
Version:	1.0
Date:	May 09 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.

The aim of VtUJI is not to introduce the latest technologies in e-voting and complex algorithms which would require elaborate preparations or substantial investments on infrastructure when deployed, both for the voter and the organizer, and often failing to resolve the issues of real world usage.

We believe that a voting system has to be easy to use and adaptable, while not losing its integrity and guarantees, offering different use experiences to fulfill the needs of every kind of user the simplest way, getting so to the biggest share of the electorate. If a voting system requires to purchase expensive machinery or to have specialized knowledge for the average user, it will never be used.

VtUJI has been designed to provide a considerable amount of guarantees and robustness through an integral design, protecting from all feasible attacks at all levels while keeping it transparent to use fro the voter.

About telematic voting

Elections are key elements of our society, as they are among the main warrants of our democratic system. That is why it is our duty to work persistently on refining all those mechanisms involved in ensuring the integrity and anonymity of elections, as well as nearing them to the voter, in order to achieve a greater participation and easing the process to all those citizens who, due to impairment, illness or residence issues have greater difficulties on casting their vote. This is the reason for the imperative need to develop telematic voting.

Furthermore, telematic voting provides substantial improvements on administration and logistics. Such a system will enable us to minimize bureaucracy and physical document generation, also zeroing production, distribution and manual verification of paper ballots, envelopes, recount records and elector rolls, also reducing the risk for human error on any of these steps. Vote centralization also obliterates the common issue of voters being enrolled to a single polling station, and drastically reducing the number of mobilized polling station officials or, even in those situations they are needed, reducing their service time.

Besides, deployment of a telematic voting system helps reducing voter coercion, since an elector would be able to cast his vote from any place in the world where there was an Internet connection available.

Features

The main barrier against telematic voting popularization is the lack of confidence shown by the voter, mainly because he is asked to trust an obscure and unknown system, developed by unknown people and operated by unknown and untrusted technicians. In a classical election, the voter places his trust on the personal integrity of the polling station officials, who represent the wide interests of all the electorate. VtUJI has been developed trying to emulate the trust structure of classical elections, also minimizing the number of trust depositories across all the structure by all logical and administrative means. The following are the design guidelines used on vtUJI to achieve its high quality standards.

Integrity

The main priority of any voting system must always be to protect its outcome from third party or inner manipulation, reflecting faithfully what voters have casted.

As in classical voting systems, vtUJI integrity is maintained by the structure and strength of the system itself and the surveillance of voter's confidence depositories. VtUJI is deployed using a LiveCD structure. This means that the system will be running from a source that cannot be altered by any attacker, storing its data on an encrypted storage facility where it can't be stolen nor tampered, and completely sealed. This way there will only be a single access point, guarded solely by those voter's confidence depositories.

Uniqueness

Secondly, any reliable voting system must assure that any voter will be able to cast a single vote, keeping this way the power balance among the electorate.

VtUJI achieves so by authenticating the voter by distribution of personal credentials and relying on trusted third party identity providers.

Authenticity

Thirdly, and closely related to the preceding, a voting system must assure that every single cast ballot comes from a single elector and has not been manipulated nor forged by third parties or inner members of the system committed to the interests of a party.

VtUJI uses the highest standards in cryptographic methods and algorithms to assure that a cast ballot was not forged nor manipulated by anybody from the moment it left the elector's computer.

Anonymity

Above all the preceding guidelines, the most valued property of a voting system for an elector is anonymity, since it lets him exercise his right without pressure, coercion nor fear of reprisals. In physical world voting systems, anonymity is clearly verifiable by the same elector, since he can choose his ballot in isolation, put it in an untraceable envelope and mix it in a closed ballot box. When electronics are involved, this physical verification of anonymity fades away. Many electronic voting systems base their anonymity only on the architecture of the whole system or at least make you trust some specific parts.

VtUJI combines this approximation with full support of the eSurvey Latency Controlled Network. A related project which enables the voter to take control of his own anonymity, relaying on a network of servers hosted by trustful and independent institutions who securely transport the ballots masking both their origin and the real moment they were casted, protecting the voter on his own terms, not on the organizer's.

Single Trust Point

The switch from classical to electronic/telematic voting systems cause the appearance of new actors in the form of computer technicians involved in the development and operation of such systems. Due to their scarcity or mobilization costs, it is impossible to substitute all voter's trust depositories with technical personnel able to survey the electronic/telematic systems and protect the interests of all the electorate. This situation provides the few technicians involved with full and unsupervised access to critical data, hardware and software. Since this personnel is often poorly committed with the democratic process, it is a potential source of mercenary tampering, disenfranchisement and forgery which usually could go unnoticed. Placing trust on them would degrade electorate's confidence on the whole system.

VtUJI design emphasizes the need to concentrate all the trust on a reduced set of notables, fully committed with the electoral process and who represent the wide spectrum of interests. In this sense, the system is designed to work autonomously and remain sealed to any technical access. Technicians will be granted access only under supervision of the members of the committee and the most common maintenance tasks have been implemented as a selectable menu to minimize hazards, letting full system access only for the worst and most unlikely failure situations.

This committee will hold the task of guarding one fragment a person of the key that seals the server. Using a sophisticated algorithm, there can be a subset of members that will be able to reconstruct the key by themselves. This is fully customizable, and it allows to establish in any case the perfect equilibrium between redundancy, to avoid critical failures or losses, and a minimum number of members to assure all interests are represented at the moment of unlocking the seal.

The committee will be tasked with granting access to the technicians and overlooking the correction of their actions, even providing their own trusted technicians to legally check every step taken by the working one. This way, it provides a solid structure with a few and well known trust depositories, enhancing system's *Integrity and trustfulness.*

Auditability

Some theoretical telematic voting schemes are mathematically auditable, thus theoretically eliminating any chance of forgery or selective disenfranchisement, in exchange for a considerable loss of anonymity or relying on user-end cryptographic capabilities. Reality tells that a dramatic majority of users won't be able to perform this audit for themselves, neglecting it or placing their trust on uncontrolled or dubious third parties.

VtUJI optionally offers partial auditability, to let interested voters check their vote has been taken into account. Furthermore, through its architecture and administrative and procedural measures it offers the possibility to let anybody check the legitimacy of the working copy on the system by proxy, through his trusted member of the committee. This way, we obtain considerable auditability capabilities without any loss of anonymity nor requiring any special knowledge or material from the user.

Open source

As we've stated above, we offer a wide level of system audit. This couldn't be achieved without the full access of the auditors to all the used code, to check every single bit of it.

There has always been an open debate on closed source code and open source code about which one is more prone to present detected vulnerabilities be stronger over time. Since it's not a closed question and there's not a proper answer, we've chosen to disclose it, so the number of users and auditors will grow making the system stronger and more reliable for everyone.

User-friendliness

As we've appointed above, many theoretical telematic voting schemes require end users to have additional software installed on their computers in order to be able to use them, such as Java Virtual Machine or to have digital certificates, or in some cases smart cards or specialized cryptographic hardware. Specialized hardware is hard to obtain, distribute, set up and operate, additional software is not so hard to obtain but usually is hard to set up for standard users and digital certificates usage and capabilities are unknown or greatly confusing for a great majority of the population. These allow voting systems to achieve greater levels of security, uniqueness and auditability, but on the real world, only a marginal part of the electorate has access to this elements. Since the main purpose of telematic voting is to achieve a wider participation, you cannot leave behind all those who are out of this minority. So you have to fall back to softer authentication and client distribution and operation methods, leaving those schemes redundant and useless.

VtUJI tries to offer a wide variety of authentication methods, highly customizable to every election and situation, and different levels of client code distribution.

VtUJI can be used from any popular web browser without the need for any additional software. Users worried about being under a directed attack on them or more reluctant to trust the VtUJI server can use the special client developed for Mozilla Firefox. It offers special measures to assure anonymity and avoid tampering, and both Mozilla Firefox and the special client are easy to set up.

VtUJI includes a highly competent and secure native credential distribution, but is flexible enough to support any external authentication system in case the organizers decide to allow its use. Also, STORK support is offered natively. STORK is an ambitious project driven by the European Union on trans-border authentication, where a wide range of identity providers are interconnected by trustful servers, making it a powerful authentication tool.

Simplicity, flexibility and efficiency

VtUJI is designed to be operated the simplest way, intuitively and with big amounts of help, both for the elector and the operators. The election manager lets you easily create any kind of referendums, from simple dichotomous pollings to complex electoral lists of candidates with single or multiple selections.

The program has been put under heavy testing, with thousands of concurrent voters and proved itself capable of handling great amounts of electors and ballots, in magnitudes of millions, while mounted on medium performance PCs.

VtUJI is distributed on a liveCD based on Ubuntu GNU/Linux, a reliable, secure and widely used operative system which supports most of the hardware in the market. This presentation allows for an easy and straightforward setup process and operation under a tested and secured environment.

It has been designed to adapt to different operation modes. Even though the main operation mode is using a permanent and centralized server with a general committee and per election board of officials, it is also possible to setup a temporary server to serve an eventual election using committee serving only for the span of this election (and possibly acting also as officials).

Guarantees

Summarizing all the information provided above and from a legal point of view, these are the guarantees vtUJI offers to its users.

To the voter

1. *Connection to the server is private, secure and the server can't be*

impersonated by an attacker. Private data enabling this security features can't be stolen nor extracted without the consensus of the whole committee.

2. *Ballot box can't be opened before the end of the election*, thus nobody can obtain partial recounts, violating this way the privacy of the electoral process.
3. *No information relating a voter with a ballot is stored*. And as we've told earlier, any voter can easily guarantee this by his own means.
4. *Once a ballot is cast, it can't be tampered*.
5. *Election outcome records can't be tampered nor forged after they have been checked and accepted by the polling station officials*.

To the organizer

1. *All received ballots belong to registered electors*. Since the system allows for a variety of different source and strength authentication methods to be used alternatively or jointly per election, different authentication requirements can be implemented for each case in order to minimize password sharing, selling or voter impersonation.
2. *All cast ballots have been emitted between the ballot box opening and closing times*.
3. *Nobody is able to forge ballots and inject them*.
4. *No elector will be able to cast more than one ballot on an election nor participate in an election on its census he is not counted.*
5. *Election outcome records can't be tampered nor forged after they have been checked and accepted by the polling station officials.*

Benefits

VtUJI not only offers benefits over classical voting systems, but also over electronic voting systems and other telematic voting systems, both theoretical and currently working schemes.

Against classical voting systems

Benefits against classical voting systems are quite obvious. First of all, recount results are available immediately, since it is completely automated. Secondly, and more crucial is the huge save in infrastructure, materials and personnel. There's no need to print and distribute ballots at all, also avoiding risks during this process. The need to establish polling stations is greatly minimized if not eliminated, since most voters have access to a network connected computers. The number of mobilized officials is also greatly reduced; or even when they cannot be eliminated, their service time can be greatly reduced. Even if we must deploy polling posts, there's another benefit: voter centralization allows any voter to use any polling station, eliminating all the bureaucracy and problems of exclusive polling post assignment.

In a common VtUJI deployment, all the voters will participate from their homes. Just one polling station board of officials is preserved to act as observers of the whole election, verifying census and ballots, initiating the election, starting the recount and acting as recipients of all the voter's complaints and observations during the process. They can perform all these actions from their own homes and a with minimal loss of time.

Against electronic voting systems

Electronic voting systems follow a classical voting scheme but the casting is aided or fully performed by machines. These have been used for decades on great populations like the USA, but their only advantage is a quicker and less industrious recount process, but they share almost all the disadvantages of classic voting systems along with those new problems caused by the use of machines.

First of all, it still needs the deployment of all the polling posts, as in paper elections, and since there isn't any centralized register, voter single polling post assignment is unavoidable. Furthermore, deployment of this machines require a great economic effort since they are highly specific pieces of machinery, which despite all the redundant elements they may contain still could break down and need technical intervention, stopping the election. VtUJI is deployed on a central server, whose performance can vary on a wide range to fit the needs of the election. And if a polling post is eventually needed it can be deployed using a cheap PC with little technical support needed. But the greater concerns are on the operation and construction of the voting machines. Let's analyze each kind.

Automatically Processable Ballot Generators

These systems take user input on their polling choices and produce an automatically processable ballot, punchcards on the older ones and barcodes or similar on newer ones. Some others just perform a direct recording of the cast votes.

Automatic recount process involving paper ballots is prone to suffer the effects of physical world, such as badly punched, wrinkled or damaged cards, poorly printed ballots or barcode read errors. The involvement of this paper trails would allow for a manual recount in case of suspected failure or an unexpected electoral rollover, but the difficulty inherent to this process could produce a high error rate and is a great source of controversy, as witnessed on USA general elections.

Even those systems where the user fills a human readable automatically processable form, there's still the possibility of physical failure during recount, which is also not verifiable. In this case, a manual recount would be much more easy than on the preceding.

Returning to the punchcards/barcode ballots if the card would include human readable information matching the encoded one, a proper recount must be performed by decoding this one, since the other one has no validity in the process and depends on your trust and the solid programming of the machine. This leads to the main concern, shared with direct recording systems.

Direct Recording Machines

These machines store all the casted votes on inner storage systems, which are collected at the end of the election to be sent to the central office and recounted. Some others deploy different voting booths with a central recording unit which receives cast ballots by wired or wireless channels. This method is by far more reliable than the previous ones, for it eliminates the entropy of paper ballot recounting, but they have a darker side; any of these share the problem that the voter can't check if recorded data matches his choices. On paper ballot generating machines, although less acute, there's the same problem since a voter is not able to interpret a barcode or a punchcard, but here it is absolutely impossible. You have to rely on the correctness of the recording algorithm and the physical support storing it. This wouldn't be a concern if these expensive voting machines weren't huge and obscure black boxes. Even though they have always been audited by the authorities, this process is quite faulty: not every machine is audited. Just a small sample is verified, so we have to rely on the manufacturer. Also, when a machine needs technical intervention, we rely on the technician not performing subversive interventions. Finally, authorities auditory may not be enough, since there are documented cases of private individuals denouncing severe privacy and integrity breaches on currently deployed voting machines.

VtUJI is compromised with transparency. Besides its single trust point centered on election officials and impermeability to attacks, because of its distribution on a liveCD and open source philosophy it can be downloaded and fully audited by anybody. But how can a voter check if the running system is the legitimate and not a forged one? By contacting his trustworthy official and performing a simple mathematical operation they will both be able to compare if their CDs are the same, thus verifying the legitimacy of the voting system.

Against other telematic voting systems

Most telematic voting schemes are straightforward ports of the previously described electronic voting systems but over a remote and centralized polling post, thus suffering from the same breaches and weaknesses. Most of them are obscure black boxes, with direct recording, where the chain of confidence can be broken at many points by isolated technicians, generating a high risk of election fraud, selective disenfranchisement, loss of anonymity or revelation of partial results. Voter confidence fades away since they don't know who are they trusting and which measures have been taken to secure their participation and the integrity of the whole system. The system could be hosted on a neutral institution, but as long as there are no measures for individual interaction of a technician with the system, we can't be sure he is not corrupted by any party. Physical, administrative or organizational policies could be enforced to avoid single actions over the system, as some currently used systems recommend, but since it doesn't provide any logical protection, confidence relies too much on the perfect enforcement of these policies, and any breach could be fatal.

Some other schemes, provide mathematical auditability and integrity measures, but all of them on the expense of anonymity, thus relegating them to very specific purposes where anonymity is not critical.

As we've stated earlier, one of the most competent theoretical voting scheme provides mathematical verifiability of the results, full auditory and multiple-party verification of the participation (by multiple signing the voter petition and the ballot), but they fail when implemented in the real world, since they require each voter to posses advanced and expensive cryptographic hardware, certain knowledge of digital certificates and its use. Despite all these requirements, it has critical confidence failures, since it also requires the user to trust the voting booth machinery and, most appalling, a determined party can force selective disenfranchisement possibly going, not undetected, but surely not convicted.

Besides all of these considerations, there's a big anonymity concern that any described scheme takes into account. On relatively low participation level moments, there's a temporal correlation between authenticated users and ballot submission. This way, a system administrator (in collusion with other administrator, if the authentication system is dissociated from the ballot box system), can guess who voted which at the time of the recount, even if the votes are ciphered with a key guarded by third parts. VtUJI tackles this problem with the aforementioned eSurvey Latency Network, which effectively dissociates a voter from his ballot by serializing trust on several servers hosted by several neutral organizations, and using redundancy to grant that the ballot will reach his destiny.

Deployment costs

One the main decision-making metrics is the economic effort needed to deploy a technology, so we offer a detailed break down of all the costs involved in deploying VtUJI on any environment. We will not provide amounts: they would be quite uncertain since different markets and scales would provide great and confusing variations. It will be a straightforward to translate this data into a real budget.

Personnel

VtUJI doesn't need full time personnel. All the activities described for all the roles can be blended into other roles present in many organizations or corporations, so the economic impact will be minimal.

VtUJI need at least **one technical administrator**, to set up the system and act on contingencies. If you already have one, he will need some training and really small dedication. Just during critical elections, a technician should be on call in order to detect and solve any unexpected situations. All the members in this position could be blended on the committee, if they matched the required attributes.

VtUJI needs a **committee** to guard the key to the server. With a minimum of **two**, its size can be as big as needed, and should be of great integrity, committed with the electoral system and represent all the interests. Their availability is only critical during elections because they are the ones giving access to the technician. Apart from this, this position doesn't provide any greater workload. If they are people usually located on premises, it won't be bothering for them and the minimum amount of officials present to open the server can be configured to match shifts.

VtUJI needs at least one **election administrator**, to setup elections and census, ballots and boards of officials. This task can be performed by any trustworthy administrative, who could even be a part of the committee. If your organization previously held elections, this position will be currently assigned, but this system will save a lot of effort, resulting in a saving rather than a cost.

VtUJI has Stork support and allows to configure several external authentication methods, such as a connecting to your institutional authentication server, but if you are planning to use the local authentication method, it needs at least one **voter registry operator**, tasked with distributing voting system access credentials to the voters and optionally, inserting their data. He must be located at a public post, since his service time should be extensive to allow voters to get by any time. Their workload depends on the extension and density of the population and how many of them are established. Many organizations have receptionists or concierges who already work at public service posts. Depending on their number and the demand, assigning this task to them shouldn't suppose a great deal of time.

For each election, a **board of polling post officials** will be drafted among the members of the corporation or elected by them to watch over the process. Their task will be to review the census and the ballots, to allow the start and to close the election, to listen to voter complaints and to allow and review the recount, leaving signed (if available) records of everything. Their service can be done remotely, so in the worst case it will give them a little extra work, but in most cases saving time because they won't be bounded to a physical polling station all day.

If any **physical polling post** is needed, it should be attended by the polling post officials drafted above, or if more than one is needed, this draft should be expanded. This dedication is temporal.

Training

VtUJI provides extensive documentation and manuals targeted at all the roles in the system. The same way, interfaces are designed to be easy and intuitive, especially for the voters. Most of them won't require direct training. Reading of his role's manual should be enough to most of the personnel, and the great majority of the voter won't need any training. In case they have trouble, they can be directed to the officials or any other help sources or desks established by the corporation, but incidence rate should be quite low.

Infrastructure

Here we specify all costs related to software and hardware purchase, and which facilities are needed to host all the activities related with VtUJI.

Software

VtUJI is **free software**, so it generates no additional costs.

For the proper and secure operation of the system, you need to purchase an **SSL Server authentication certificate**, from a trustworthy certification authority. Charges vary from authority to authority, but we recommend using one widely accepted by most popular browsers, to avoid voter discomfort.

Materials

In case you are planning to use local authentication, the process requires the distribution of previously **printed paper voter cards**. On further documentation we provide the requirements for this cards, but they are mainly indicative. The quality of the cards can be adapted to fit your budget, or even its distribution can be canceled if you believe you don't have this need or have other means to fulfill their function.

Hardware

Generally, if all the electorate has access to a networking computer (which will happen on most deployments), the only hardware need is the **Server**. The bad part is that it must be a **dedicated server**, only for this system. The good part is that this server can belong to many different market segments, but a relatively cheap mid-scale PC can handle elections in the order of thousands, or even hundred of thousands. If budget is a problem, as stated earlier VtUJI is **quite flexible**, and it could be launched just temporary over a machine with another purpose. Persistent data could be held inside this machine's data without damaging it or even on a remote location. This setup would lower the efficiency but could hold small and eventual elections without trouble.

If there's a need to establish old fashioned **polling posts**, this can be done using cheap old fashioned PCs without much trouble. Of curse these PCs don't need to be purchased for this occasion and don't need any special setup. In a failure situation, they can quickly be substituted or if needed, the polling post could be easily transferred to another location.

Facilities

Server needs allocation on some room. It could be allocated on a common

server room, but since all the committee must be on site when performing operations over the server, maybe it is a bit risky to stick them all in a room full of delicate hardware. Some multiple purpose room could easily allocate the server. Due to its protections, it doesn't need special physical security measures. It just needs to be protected from disconnection or destruction, so **any office or meeting room** could host it properly. A common location to keep it is at the committee's president office.

Polling station officials can perform their tasks remotely or, if some ceremony is desired, as in classical elections, they can gather on any **meeting room or office** in order to do it in person.

If there's need to establish **polling posts**, they must provide some intimacy for the voter to participate anonymously. They should be accessible locations, such as desks, concierge offices, etc. These are temporal.

To provide **voter registry points**, the same desks described above can be used, and almost any accessible post permanently hosted by an administrative.

Financial

We'll put everything in economic terms.

Personnel retribution for this overwork depends on the company standards, but on the worst case it won't suppose much extra work, and in case there's an already established classic election system, switch to VtUJI will suppose a save in effort, so retributions, at its best would be kept as they are.

Training costs will depend on how deep the company wants to train the employees, but usually posting informative webs and manuals will be enough. Most complicated tasks are limited to few people, and it won't usually amount more than a few hours for the administrators and a few minutes for the officials and voters.

Purchase of the server is one of the main financial efforts, it can be adjusted to the needs of the deployment and even tough it does not need to be a high profile machine.

Certificate purchase is essential to the proper and secure operation of the server. Some providers are quite cheap, but some others can be really expensive. It all depends on the needs and budget for this operation.