VtUJI
Telematic Voting System

Administrative Information

Id:	VT-D02
Version:	1.0
Date:	Mar 15 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 contains a comprehensive collection of all the elements involved on the deployment and operation of VtUJI from an administrative point of view. There's a list of all the roles involved, specifying what involves and who should fill it. Procedures are defined trying to cover the right way to face the wide spectrum of common and emergency situations that may occur during its execution. There's also a list of the appointments and decisions you will have to take before starting the deployment.

Information will be classified according to several criteria, trying to make it quickly accessible and useful to handle different situations.

Roles

This is the complete list of roles involved in the implementation and operation of VtUJI. Most of them can be overlapped on a same person, thus simplifying their appointment on smaller corporations. Each role is defined by its duties and the profile that must follow its holder. All the roles in VtUJI are compatible, since none of them has powers to act alone with impunity.

There is a role that is not listed here, the **Election Authority**. On every electoral system there is a supreme organism that holds control over all the process, resolving incidences and unexpected situations, and ensuring the correct development of the elections. Even though it is named several times throughout this document, it is not defined for one big reason: each electoral system will have a different superstructure, a different procedure set and different sharing of responsibilities. Since they don't have any interaction with VtUJI and their procedures don't collide with the security procedures of VtUJI, they are left out, only naming them on those moments we need interaction with them to provide data input, resolve conflicts or apply to legal prosecution.

Each organization will have its own legislation for this upper part of the electoral system. On big systems, this body would be a separate one, even hierarchical, but on small organizations, this role can easily be merged with the key custody committee. We will differentiate them on this text for the reasons above.

Key custody committee member

This role is the key element of the reliability of this system. The number and composition of the committee formed by them must be carefully determined, since it will be the depository of the electorate's confidence in VtUJI.

Profile

An eligible candidate to this role must be a person of notable integrity among the community, compromised with the democratic system and/or any person representing the interests of a sector of the electorate. Depending on the situation, this committee could be the same 'election management body' or a mixture of them with party comptrollers. The candidate for this role should have, to the possible extent, the legal knowledge to detect irregularities on the administrative process and the technical knowledge to detect malicious actions from the technicians operating the system. If not possible, he should bring with

himself an advisor to fulfill this requirements.

Amount

There must be at least two of them, but at least three should be used to provide some fault tolerance. We'll later describe some guidelines to set this amount for each case, but they must cover all the interests of the electorate and making sure that a faction won't be able to retrieve the key on his own.

Attributions

To produce the reliable working copy of the CD.

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 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.

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.

Availability

The required availability is variable. Their tasks are minimized, but are highly critical. The span from mid to long term response times (between one day and one week) when there are not ongoing elections, to high alert periods (between one and a few hours) when polls are open.

System administrator

His duty is to provide technical support for the deployment and operation of VtUJI.

Profile

VtUJI is a highly autonomous system, but needs to be set up and maintained on contingency. The holder of this role doesn't need to be an individual with special integrity or reliability, since all of his critical actions will be either monitored or limited, and always need to be authorized, but he needs to be keen on system administration and be able to set up by himself (or coordinated with other members) the environment where VtUJI will be deployed (network configuration, domain name, external authentication methods, etc.).

Amount

One of them should be enough, but depending on budget and personnel availability having more than one would be interesting, due to shifts, illnesses or other issues that may happen during the celebration of critical elections. The technicians provided by the committee members to monitor the actions over the system also fall into his role and, if part of the organization, could be named deputy administrators.

Attributions

To read the technical documentation and learn about the configuration and functioning of VtUJI.

To set up the environment the server will be deployed on, both physically and logically.

To set up the system and configure it, adapted to the needs of the organization.

To monitor the status of the server and warn the committee about any need for management operations.

To perform all the management operations required by the situation under the approval and monitoring of the committee.

Availability

His availability must be always short term ()between one hour and a fer hours). He is responsible of checking the status of the system and coordinating the response to each situation.

Election administrator

The holder of this role will create and administer the elections, setting up the elector rolls, ballots and polling post committees.

Profile

This role must be assigned to anyone with experience in administration, specially of electoral processes, competent and trustworthy. If elections were being held before deploying VtUJI, there must be for sure somebody that took care of all the attributions of this role. The main part of the work will be performed outside the system, since candidate lists and elector data are gathered and classified using different ways in each case, but once all this data is present, it must be inserted on the system.

Amount

Depends on the size of the organization, but one should be enough. VtUJI doesn't support concurrence, so only one administrator can work on creating a polling post at a time[1]. If various non-exclusive elections are being prepared at a time, they can be managed by different administrators. Else, previous work could be distributed among all the administrators and only one would be

1 To understand these concepts see section 'Election management tool' (page 20)

responsible of inserting all the data on the system.

Attributions

To gather all the information about the election dates, ballot composition (candidates, options, parties, etc.), elector rolls (names, Id numbers, email addresses, etc.) and polling station officers in the accepted format by VtUJI (see page 21).

To insert all this data in the system to create a polling post using the application.

To schedule the election as soon as the election management body gives its approval.

To notify the officers and/or the voters about the scheduled election using the application.

In case of need, delay the closing time for an election.

When the elections are over, to destroy the ballots and the rolls according to your electoral law.

In case of officer absenteeism, act as an officer to open the ballot box and verify the results of the election.

Availability

The required availability for him is variable. During elections, he must be available on call to add/delete voters, but outside these periods, his duties have low priority and are widely spaced in time.

Voter registry operator

His duty will be to register voters, correct their personal data and distribute authentication credentials among them.

Profile

Anyone holding this role should work in public-facing desk, since he will have to attend electors (secretaries, help desks, doorkeepers, etc.). He should be someone not directly or strongly related to any partisan interests inside the organization.

Amount

At least one of them is needed if the local authentication method is going to be used, since he will be distributing the temporary password to access the web application, but the amount depends on the size of the organization, percent of dedication of all these administrators to this task.

But there's another factor that could be more critical. The biggest concentration of voters using this service will be before their first election.

Depending on the size of the electorate (if it is a general election for the whole organization the workload will be greater than if small elections are held for each department, for example) and the time available between the schedule of the first election and its celebration.

There are some ways to stagger this distribution, such as asking everybody to go on a determined date.

Attributions

To check the voter's identity by physical means (comparing him to a photograph on an official ID card).

To look him up in the system and fill in any missing or mistaken information.

To let him pick up a random voter card and register it in the system as the voter's temporary password.

To brief the voter about the correct following procedure and solve any concerns he may have.

To report to the election authority any denounced or observed irregularity, like coercion, impersonation attempt or credential theft.

Availability

The required availability for it is continuous during the periods of service (desk hours), but its workload is sparse and can be merged with other desk tasks.

Polling post official

This role is a reminiscence of classical voting systems, kept to provide the voter with a little extra confidence. His duty is to provide extra monitoring of the election process and record any voter's complaints and incidences. Despite his name, it doesn't imply that a physical polling post is going to be established, what's more, they can do their work without even physically reuniting.

Profile

Such as in classical voting systems, any elector can be drafted to hold this role. His actions are harmless, and will be double checked, since there will be various officials.

Amount

It can be as big as desired. Usually they will represent each interest group on the electorate and the interests of the organizers. The amount should be decided depending on the size of the electorate and the expected incidence rate, since they will have to process the complaints and incidences from the voters.

Attributions

If chosen as an alternate officer, be on hold just in case any of the main officers is absent. In that case, take over his position.

Between the time the election is scheduled and the time the polls are opened, to review the census and the ballots to check for mistakes or missing electors and candidates. Each found anomaly has to be recorded on the system.

During the election, to attend every voter who addresses him with incidences or complaints (disenfranchisement, coercion attempts, impersonation, etc.). They should be solved if possible.

After the polls are closed and the recount is done, to review the results and to record every incidence he has treated.

If they have the means, to digitally sign every reviewed record, to provide extra integrity.

In case of board chairman and alternate chairman absenteeism, to take over his role an perform his actions (the chairman is just another official with some extra attributions)

Availability

The required availability for it is continuous during the periods of service (election period), but its workload is sparse and can be done remotely most of times.

Polling post board chairman

Just like the officer role, but with the duty to coordinate the other officials and allow the polls opening and closing.

Profile

He must follow exactly the same standards as a polling post official.

Amount

One per polling post[2], and an alternate one on hold, in case the first one is absent or incapacitated.

Attributions

The same ones for the plain official (see page 10).

To coordinate the other officials in reviewing the rolls and the ballots.

When all of them have given their approval or are declared absent, to write the definitive polls opening record and start the election.

To coordinate the other officials in reviewing the results of the election.

When all of them have given their approval or are declared absent, to write the definitive results record and close the election.

2 Just as stated above, not a physical polling post. See 'Election management tool' (page 20) for clarification.

Availability

Same as the polling post officer's.

Voter

This role covers each member of the census willing to participate in the election.

Profile

Each country has its own legislation about who is eligible to become an elector. Those willing to participate will also become voters.

Amount

As many as are listed in the census for each election..

Attributions

To reach a voter registry post, identify himself by the required means and obtain his temporary authentication credentials on a voter card.

To authenticate on the voting system before the credentials' expiration date and obtain the definitive ones and write them down on the voter card.

To properly guard the voter card with the credentials from any suspected hijacker.

In case of credential leak or loss, to return to a voter registry post to invalidate the previous credentials and get some new ones.

When the polls are opened, to log in the voting system using a secure and private computer on which he trusts, to cast his desired ballot.

If the election provides auditory codes and if desired, to copy or print it and later to verify his participation has been properly received.

To report the board of officers about any irregularity or election law violation he may suffer or observe.

Concept overview

Even though some of the information in this section may at this point be confusing, we need to introduce it now. It will be clearer after reading the procedures section.

Key Custody Committee

This is probably the most delicate component of VtUJI, since it is the key to the integrity, reliability and all the guarantees of the voting system. Thus, it is absolutely critical to determine the optimal setup for this committee in each deployment case. Here we will provide guidelines to help on this process and take the proper decisions in each situation.

Note that the electorate needs to know the composition of this committee in order to trust them. You'll need to make an effort to advertise this among the

electorate, so they will know who to address in case they need further confidence

The composition of this committee is based on four parameters: The number of members (N, from now on), the number of opposed parties (P), the number of members per party (Pn) and the key reconstruction threshold (T).

N is the number of pieces in which the key will be fragmented, and T will be the minimum number of members that will be able to rebuild the complete key. Thus, the greatest the difference between N and T, the greater the redundancy of the key.

This way if some fragments get lost, due to a hardware failure or to the actual loss of the physical support storing the fragment, the key still could be recovered, allowing a maximum loss of (N – T) fragments. Remember that losing more than that amount would lock down the voting system forever.

N can be as big as wanted, but you have to remember that during setup and maintenance, all these members must be on a same room overlooking the actions of the technician, so a big N would slow down all actions requiring authorization since all of them would have to use their flash drives on the same computer on a row.

T is trickier to set, since it allows for multiple combinations of members and none of them must be dangerous for the integrity of the system (a T of 3 and each party (P) having 3 members (Pn) would be an awful setup, since an interested party could take control of the system on its own). We'll analyze the basic setups.

Committee of notables setup

The simplest setup. All the members are notable members of the community, independent and committed with the electoral system. There are no factions and no interests among them and the only threat would come from individuals acting alone, but a group of them acting in collusion is unlikely. (This can be interpreted either as 1 P with N Pn, or N P with 1 Pn).

The size of N is a straightforward decision depending only on the needs of the organization. The only tricky parameter to determine would be T, which would have to be big enough to discard collusion but letting some redundancy (for example, to allow reconstruction even if a piece is lost or some members are off duty, work on different shifts or are far away or on medical leave).

Usually, a T value corresponding to the 50-70% of N would be enough, but it depends on the collusion threat on each case.

Multiple party setup

Here, a number P of parties will be part of the committee, representing the whole spectrum of interests among the voters, not proportionately to the number of supporters but all with an equal share of the committee. This is vital, to avoid stronger parties having more power over the election system.

In this scheme, all the parties must always be involved on the reconstruction of the key, so T must always be greater of equal than P. Otherwise, any party left aside could complain on conspiration against them.

Having a Pn of 1 is highly discouraged, since it would require a T value of P, hence T=P=N, so no redundancy.

The only secure distribution of fragments is determined by the formula:

$$N = P*Pn \ , \ T = (P-1)Pn + 1$$

This means that, for P parties with Pn members each, the minimum number of presents should be all the members from all the parties except one, and a member from this last party. This, although the only secure setup, us highly impractical, because for a Pn of 2, the redundancy would be just one fragment, but as long as the number of parties grows, increasing the number of Pn would greatly increase the amount of people involved, since each party had to provide one more member in each case increasing mobilization costs, making it difficult to coordinate all of them while poorly increasing redundancy.

We must note that the party concept is not necessarily attached to real world parties. If we make this assumption, we can cook a smarter yet more delicate scheme. Here, the party concept represents opposed interest groups. This means that two real world parties prone to cooperate shouldn't be given differentiate party status in the committee since they could have enough combined power to operate the system on their own.

For a two party setup having Pn = 2, the proper T value would be 3, like in the secure scheme. Assuming P>2, a proper Pn value would be 2, with T=P. It would provide enough redundancy and assuring every party is represented on the reconstruction, assuming of course that no party would allow another one to provide two fragments except in case a party was deliberately absent or had lost both fragments.

All this is done under the assumption that all the parties are independent and have opposed interests. It is your duty to foresee if any factible combination of parties with a common interest (also with the **common interest to impair a third competitor**) could have combined control of T or more fragments and, in such case, rearrange the party setup.

Mixed setup

In some cases, a combination of both schemes would be better. This is, party representatives and independent and notable officers to oversee them. This group of officers could be considered as another party, but since they are considered reliable on their own, we can use them in a special way. As in the previous secure scheme, T should be (P-1)Pn + 1, considering the officers as another party, but while Pn could be 2, the minimum, the number of members of this party could be as big as T-1 (this way we give some guarantees to the parties that the officers can't operate the system without considerating at least one party representative). This officers would be used as redundancy providers, thus allowing to reduce the Pn number. Formally:

$$P' = P + 1 \ , \ Pn = 2 \ , \ T = (P'-1)Pn + 1 \ , \ N = P*Pn + (T-1)$$

Pn = 1 could be used if the number of parties is too big to be feasible to use 2, but parties would have to accept that in case their representative was absent,

an officer would fill his position without the posibility to complain.

Authentication

VtUJI, on behalf of its versatility offers multiple methods of authentication. It is a feature with complex implications that requires in-depth analysis.

Integrity and security requirements of VtUJI require it to be a fully autonomous system to guarantee that no third parts can tamper with it. On the other hand, integration with other corporative systems is quite appreciated among users. VtUJI allows such integration on user authentication.

VtUJI offers a fully autonomous local authentication system, recommended in any use case. It also has native support for the STORK authentication infrastructure, which is an European project aimed at providing reliable trans-border authentication. Finally, it allows up to ten different personalized integrations with external login services. We'll discuss them in depth.

To provide greater security, VtUJI uses a score system. Every time a user logs in using some method, he adds one point at the score; he can use different methods to earn more points. Depending on the user role and how critical is the task he is performing (a simple voter won't earn any further functionality for increasing his score, but an election administrator won't be able to create an election with the lowest score), he will need a higher score to gain clearance.

Local authentication

Authentication won't depend on any other system. User data will be loaded previously by the organizers and the user will be given a user name and a password to log in (see Credential Distribution section). The user name can be the same as on the corporate login system, but the password won't be related.

This method provides additional points, if the password login was successful:

- The first time a user logs into the system, his IP address will be recorded. It will be considered the 'usual address', so, logging in from this computer will award an extra +1.
- If he is using Internet Explorer (on Windows) or Mozilla Firefox (on Linux) and *Clauer* software is installed, the first time he pins a *Clauer*, the system will read its identifier and store it as the user's *Clauer*. If this *Clauer* is connected during any login, it will award an extra +1.

This is the preferred method, since it is invulnerable to third party services failure. Even if some other method is used, this one should also be available as backup.

It uses passwords as authentication tokens (instead of certificates, smart cards and so) because it is the most widely spread authentication method, which any voter can obtain and use without further knowledge or performing complicated operations. Its aim is to be available for all the electorate.

VtUJI allows being operated without a server SSL certificate (this will be discussed on the technical documentation), but is completely discouraged if planning to use local authentication, since the user's passwords would travel in plain text and any eavesdropper could capture them.

External login services

External login services can be connected to VtUJI through the development of a small interconnection layer that is explained in the technical documentation. They are the easiest way to authenticate users, since they don't require credential distribution, but they are dangerous.

First of all, they are new and uncontrolled depositories of the voter's confidence. Unlike VtUJI, the voter doesn't know who is operating this authentication system and there's no way to know if malicious actions have been performed over it to alter the outcome of the election. The main threats are selective voter disenfranchisement (if you don't login, you don't vote) and impersonation (since the administrator can login himself as anyone).

The risk is much higher when this is the corporate login system, since it is close to the organization and its administrators can be corrupted by any party.

As stated above, it is useful as an extra security for credential distribution, or some low impact referendums, but should never be used on any serious affair. At least not as the only login method.

STORK

Integration of certificate authentication is quite a difficult task, for the wide variety of certification authorities to trust in the world (including some local certification authorities the organizer would like to trust) and the non standard way of identifying its owner for each authority.

SAML Identity Providers offer a standard interface to relay the authentication process to a trusted third party, but you still need to configure a list of the trusted Identity providers.

Stork is an European project aimed at creating a network of servers that abstract the identity provider selection. Each of them is linked to a country and, has its own list of trusted identity providers. A request is relayed on the network and is attended by the corresponding server, returning the results to the original server who will hand them to the solicitor, VtUJI.

Even though it is an external authentication service, STORK is a multi-national government initiative, loosely related with any organization, and we have a high degree of confidence that nobody related with it will cheat us.

But we can't forget it is externally maintained and depending on the importance and scope of the election, it should be dismissed (for example, in a general election, where the government is an interested party of the election).

Checking URLs

To access a voting server, the voter will need to know its address: that is, its URL. The main threat to the voter is that he may be tricked to access an illegitimate voting system while believing that he is accessing the legitimate

one. The main point is to not trust blindly what he sees or what he is told, to avoid being cheated.

The voter must obtain the URL of the voting system from a reliable source and, at least, must look legitimate. This means that most of times it will be a sub domain of your own organization. Also, some attackers might use URLs that look similar to the expected one, allowing for a certain portion of the users to fail to uncover the trick. **The voter must always check the address at depth and try accessing by typing it himself, not trusting a link.**

A legitimate voting server will always work through SSL protected channel. This means that the URL will always start with **https://** (secure HTTP protocol) to keep privacy on communications. The voter must check this. Besides privacy, the server must provide proof that it is the computer the voter is expecting. Some sophisticated attacks can fool his computer to believe he is accessing the legitimate server when he is accessing another one. To this end, the server will provide a **reliable server certificate**. This means that it will provide a signed proof that it is the computer legitimately associated with this URL; and the issuer of the certificate has verified this point thoroughly. If the issuer is trusted by his browser, then the voter has the certainty that he is accessing the right server. **If the presented certificate is not trusted, he must not accept it.**

The browser will show **visual evidence that the accessed URL is presenting a trusted certificate**. Some browsers will switch the color of the address bar or some element around it. Most browsers will warn the voter if the presented certificate is not trusted, but with variable emphasis. He must be aware of those signals before performing sensible operations such as authenticating and voting.

If accessing through a link on an e-mail, he must be aware that e-mails are easily forged and the apparent sender may not be the real one.

Every time he inputs sensible information (mainly when authenticating and voting), he must be sure to perform the above verifications.

Credential Distribution

This topic will be detailed further on the procedures section, but here we will analyze the rationale for this set up and the hazards of not following strictly the procedures.

If using local authentication, the organizer needs a way to deliver the user his password. Moreover, the user must be a real world person, with real data, no duplicity, and the set of users is decided by the organizers, so not anyone can be registered and it needs to be done crediting the voter's real identity, so remote methods are useless.

The user interested in participating on the election must go in person to a convenient registry post. There, his identity will be checked and his personal data will be input in case it is not, but it should be previously loaded by the organizers (otherwise, they will need to provide some method to discern if a

user can be registered on the system or not). He will be given a random temporary password in the form of a card (randomly selected by the user from a pool of cards). Then, he has a period of 48 hours to log into VtUJI with this password and change it for a definitive one (which will be randomly generated, for security reasons).

In case the registry operator has to input information that he can't check on the voter's id card, this means must be asked to the voter (such as user name or email address), you should preferably set up a procedure to obtain them from a corporate source (like a lookup system). In case you can't set up this, the email address, although important, can be left blank, and the user name can match the id number.

Rationale

The use of a temporary password is essential for the process of credential distribution. Passwords are soft authentication tokens and degrade over time, since they can be revealed to others over the handling process. The temporary password dissociates between the user identification, where he is allowed to have a user and a password on the system and the definitive credential delivery. This way, only the user will see his password and its privacy will be absolute.

Moreover, this password must always be temporary to reduce the hazard in case this password is lost or the voter neglects to change it and is revealed to a malicious attacker (which potentially includes the registry operator).

A committed voter in case of loss, will surely return to the registry post and request a new one, thus invalidating the old one, but a neglecting voter might open the door to impersonation; the attacker could set up the definitive password and use it. An attacker won't risk to impersonate a committed voter, for he is prone to get caught. So, an attacker would wait until the last moment of an election to try impersonate the voter, to maximize the success options (if the voter hasn't done anything by then, he won't do it for sure). If we set a validity period of 48 hours, the attacker has to take the risk of changing the password while the legitimate user could still be interested, exposing himself.

Additionally, for further security in case of card loss, if your organization has a corporate login system, VtUJI can be configured to require this corporate login in order to change the VtUJI local password. This way, nobody will be able to impersonate the voter before setting the definitive password, since the attacker won't know the corporate login credentials.

Hazards

A registrar must give a password only to its legitimate owner, no proxies. Otherwise, a voter could take control of two accounts.

A voter not willing to participate in any election, should not request his credentials. By doing so, he opens a small chance to someone impersonating him. The registry operator handles the password cards, so he may copy the temporary password for this user and use it as stated above (despite the small chance he has for success).

A voter suspicious of credential leak or loss must go the registry post and invalidate the old password. Otherwise, he is likely to be impersonated.

If your temporary password should still be valid and doesn't work, or your definitive password seems to be wrong, there's a chance that a registrar is corrupt or has been cheated (either he has set your permanent password or reset it to a new temporary one without your request). You should contact another registrar (or administrators or any higher level members of the voting system). There's information about who and when last set your password. If it's not the time and place of your last request, a further investigation must be held to purge responsibilities.

Voter cards

Definitive voter passwords will be automatically generated, for security reasons (automated generation assures enough entropy and length). Voters will be encouraged to write down their password for several reasons. First of all, a secure automatic generated password would require a considerable effort to memorize. Secondly, if it was a user-set secure password, there's a big tendency to share passwords among different systems, which is also dangerous or, even worse, share them with other people. And finally, even if it was a brand new secure user-set password, the frequency a voting system is used is quite low. This would turn into a high rate of forgotten password incidences, needing a password reset request at a voter registration post, mainly concentrated on the few last days/hours before the election, collapsing the available posts.

To facilitate writing down and storing the voting credentials we'll distribute a previously printed voter card not related with the voter. You will have to design and order them, always having enough on stock. As we've stated in other documents, this is a flexible process, which could even avoid card distribution if you find other means to solve the aforementioned issues accomplishing the following requirements and its motivation:

- A printed random password, at least 8 characters long, alphanumeric (for simplicity, it can be just lowercase and numbers, since it is temporary)
- The same password in bar code, to ease its registering and exposing it too much to the operator (you will need a bar code reader per registry post).
- The card needs to be resistant enough to be used eventually for quite a long time. Thick cardboard, plasticized paper or other plastic materials should be fine.
- Regardless of the material, there must be an area suitable to write down the definitive password.
- A visible warning that it is a temporary password and it must be used to set the definitive one before 48 hours or it will be deactivated.
- Another warning telling to write down the definitive password and store the card properly and safely.
- If already known, the URL of the voting system could also be in the card.

Election management tool

The election management system is the web tool that enables us to create, manage and participate in elections. It has been designed with the aim to fit the most common electoral systems, and is prepared to create a wide variety of ballots. We'll explain the main concepts needed to understand how it works and to input data.

Main concepts

The core concept of the system is that of ***polling***. It represents a set of *options* among which the voter has to choose. The minimum and maximum number of *options* that can be selected for it to be a valid participation is set per polling.

Also, for a realistic recreation of th physical world elections, each polling can be configured to accept blank ballots and/or explicit null ballots (allowing for the voter to write down text as if he was voiding it by writing his opinion with a ball pen)

Each ***option*** represents an eligible item and can be formed by an image (optional) and from one word to several lines of text. The order in which the options will be showed is defined by the user, sorting them numerically. Each option can optionally contain one or more *candidates* and zero or more *alternate candidates*. If there's at least one candidate, the option text is also optional. Many *candidates* on a same option represent a closed list. To implement an open list we need to use *separators.*

Each ***candidate*** or ***alternate candidate*** represents one person, who must also be a user of the voting system.

Each option admits a ***separator*** that will be placed above it on the defined order. A separator can contain multiple lines of text and/or an image. An open list would use an option per candidate (one option with no text and only one candidate), sorted first by the order parties are shown in the ballot and last by list order inside the party list. It would use the separator of the first candidate of each list to put the party/list name.

An ***election*** is composed of a voter roll, and a set of one or more *pollings*, which reunited form a ballot. It is the minimum participation unit in the voting system, so a voter will have to take part in all the pollings defined in the ballot. If two different pollings, even though related, allow independent abstention, you'll have to put them in separate elections.

A ***polling station*** is loosely related with the real world one, as it is not a physical place where voters can cast ballots. It's just a concept to group various elections and there is only one per election. A polling station is composed by a board of officers, the start and the end of the period to cast votes and a set of one or more *elections*.

Different elections held on different periods must necessarily be part of different polling posts, but if they share the period, if they are minimally related it is wise to put them together, to reduce complexity.

The same way, VtUJI allows to hold different but related elections (called ***exclusive elections***) in which a voter is on multiple rolls but can only participate in one of them, automatically voiding his participation rights on the rest. This has to be done using a single polling post for all those elections. The

voter will first decide which one wants to participate in, by examining the ballots, and automatically will be drawn from the other rolls.

Data input formats

VtUJI needs census data to operate. For security and integrity reasons, this information cannot be accessed on demand from a remote server (like an LDAP). So, it needs to be previously loaded.

Census Data Format

Census data needs to be obtained in a strict format, which is the following (obviously, none of the fields may contain the character ! As part of its content):

username!idNumber!Surname, Name

or

username!idNumber!Surname, Name!emailAddress

- **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.

ID number format

This field requires a greater focus on it, since it is prone to some confusion

Depending on the country, corporation or organization, the format of this ID number ranges from a plain fixed cypher number to a combination of different fields, with numbers and letters, separators and redundancy fields.

Sometimes, there's not a unified format to write it. For example, Spanish 'DNI' may have a starting letter, declaring its type, an eight cypher number and a redundancy letter (for example, X12345678R). Some people would write it this way, while some others may write it this way: X12345678-R or this one: X 12345678 R, and so on.

Since voter registry operators are allowed to input new users to the system, this may lead to a chaotic registering, and confusion when using it as an identifier on authentication, causing even voter disenfranchisement (if the voter is counted with a wrong id number format on the roll and he is not able to deduce it), or even worse, duplicate entries, which could lead to some users voting twice (not likely, since it would probably be detected on census revision).

It is very important to settle a canonical format to input this data and inform the users (by e-mail, on the voter card or any other means) and specially the registrars to use it every time they input an ID number.

Email Address format

VtUJI accepts various ways to set the email address:

1. *full email address*: username@domain, the classical way.
2. *User name*: if only the user name is given, VtUJI will assume that the domain is the default one. It can be configured during setup and changed any time (needs committee authorization). **Be careful when configuring it. The default value shown is just a suggestion, if you don't hit the update button, it will be empty and it won't work.**
3. @: 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.

Operation modes

VtUJI can be deployed using two different operation modes, depending on the needs and resources of the organization. The main difference between them lays on who are the holders of the voter's confidence (those who keep the pieces of the cyphering key).

Central Committee

This is the recommended operation mode. It is specially recommended for organizations who plan to use it periodically and it is nearly essential if some different elections are going to be held concurrently.

In this mode, the confidence depositories are a Centralized Key Custody Committee (see role information at page 6). This committee, if the organization has any legal structure for the elections, could be the Board of Elections, or some other board of officials tasked with overseeing the democratic process. They must be impartial, honest and/or represent the interests of all the factions among the electors.

This committee will reunite once to install the system, that will remain operative permanently, and eventually to allow maintenance over the server or restarting it after a failure.

Each election will be held over the same server and a *polling post board of officials* will be drafted among the electorate per election (see role information at page 10). Their attributions will be those described on the corresponding

roles.

Classical Polling Station

This mode is oriented to organizations with little resources. Holding small and occasional elections. It is also oriented to others that don't want to use the confidence scheme described above, namely scattered organizations, or those composed by very independent units who can't establish a central commission representing all the electorate.

In this mode, both roles referred above are blended into the same group of people. For each election held, the drafted *polling post board of officials,* will also be the Key Custody Committee. Therefore, a new installation of VtUJI will be needed for each election. This way, although bigger technical support is needed, the people the voters are trusting are nearer, and will trust them for shorter time. Different elections can be held on the same computer, but not at the same time (concurrent elections need to be held on different computers and accessed through different web addresses). When an election finishes, the computer can be given any other use.

Such as classical polling post official boards, drafted members should be combined with representatives from all the parties to provide confidence to all the parts.

Also if using local authentication, voter credentials will have to be distributed before each election, so it is not feasible for big populations.

This documentation will be oriented to the central committee operation mode. Procedures differ very little from one mode to another, so it would be redundant to specify them both. If you want to use this mode, you'll have to combine roles and consequently, combine procedures.

Prerequisites

Now we will present a comprehensive list of all the decisions, tasks and appointments that must be done before starting to deploy VtUJI.

Decisions to take

- *How many registration desks are being established*. Based on the size and dispersion of the population.
- *How many election administrators are needed*. Depending on their shifts and the amount of expected work (number and extent of the elections).
- *How often the key custody committee has to meet to verify the integrity of the key fragments.*
- *Whether if the registry operator must add user data or all data will be loaded when the system is set up or when elections are created, leaving him the only duty to set the temporary password.* Notice that it would be much safer to load them previously.

- *Whether if real polling stations are being established*. Depending on the capacity for all the population to have access to a secure computer connected to the Internet.
- *User name or ID*. If your organization has a corporate user system, and depending on your capacity to give this information to the registry operator (for example,a lookup service, or if it is present on the ID card).
- *Settle a canonical form for the ID number*. See page 21 for details.
- *Whether if the e-mail for the voter must be a corporate one and come from a reliable source or the voter can suggest his own*. It depends on your convenience.
- *Whether if user have to sign a contract*. Depending on the laws of your country, regarding personal data handling, or the electoral law, you might need them to sign a contract. Maybe they have already signed any contract that covers the issue.
- *Whether to set up a corporate or another external authentication system*. If you trust them enough to be used when holding elections. See the *System Administrator User guide* for details.
- *Whether to use the local authentication or not.* If not, you can dismiss all the appointments and procurements regarding credential distribution, but notice that you will create an external dependence and open the door for selective disenfranchisement by the authentication system administrator. Do this under your responsibility. See the *System Administrator User guide* for details.
- *Whether to use the corporate authentication as security support during credential distribution.* See the *System Administrator User guide* for details.
- *Whether to preset the IP addresses of the desks for each registry operator, or give them Clauers.* They need a support credential to gain the required authentication score to do their functions. You should use the IP if the operators are assigned to a specific desk and hardly ever move elsewhere, or the Clauer if they are frequently relocated on different desks.

Tasks

- Appoint the system administrator.
- Brief the system administrator on his duties (give him a copy of the *system administrator user guide*).
- Notify the **system administrator about his duties** before the deployment:
  - To coordinate the procurement and commissioning of the equipment described on the *System Administrator User guide*. Name and order as many deputies as needed to acquire and configure all the equipment as described on the guide and have it ready before the first gathering of the key custody committee.
  - To coordinate the execution of all the network configuration needs to deploy VtUJI, as described on the *System Administrator User guide.*
- Appoint **someone to coordinate the establishment of voter**

registration posts. He should be the system administrator, one of his deputies or some other person, but with his counseling regarding the technical needs. His duties before the deployment are:

- To decide which existing desks are suitable to take over this new duties.
- If more desks are needed, to procure and commission all the required materials (see *System Administrator User guide f*or a list).
- To appoint all the registry operators.
- To brief the registry operators on their new duties (give them copies of the v*oter registry operator user guide*).
- To produce a list of personal data for all the operators, to be registered during the system setup.

- If they are going to be used, appoint someone to **coordinate the establishment of real polling posts**. Again, he should be the system administrator, one of his deputies or some other person, but with his counseling regarding the technical needs. His duties are procuring the premises, and electronic and furniture equipment described on the *System Administrator User guide*.
- Appoint someone in charge of the design and procurement of the voter cards. His duties are:
  - Produce a personalized design for your organization of the voter card and adjusted to your needs and budget, but following the guidelines described at section '*Voter cards*' in page 19.
  - Outsource or settle the card production, at a rate adjusted to the population, while having always enough stock.
- If needed, Appoint someone in charge of drafting the contract that the voters must sign, regarding data cession and election participation legal assertions. He must decide if the contracts are bulk printed and distributed to the registry desks or they are printed on demand on each desk. In the latter, he must take care of procuring printing equipment and material for each desk.
- Appoint the election administrators.
- Produce a list of personal data for all the election administrators, to be registered during the system setup.
- Brief the election administrators on their duties (give them copies of the *election administrator user guide*).
- Set up a method (a criteria or a centralized lookup service), to discern whether a person showing up at the registration desk can become part of the election system or not.
- When the registry operator is allowed to insert user data, to set up a method (a centralized lookup service), to reliably obtain needed data from a user not shown on the ID card (probably the e-mail address and the user name).

- Brief the registry operators about the methods and decisions taken affecting their duties (the canonical form to insert an ID number, whether if they are registering a differentiated user name or they must use the ID number, etc.).
- If you decided to use an external authentication system, appoint some technician to develop a gateway between your corporate authentication system and VtUJI. See the *System Administrator User guide* for details.

Procedures

In this section we will provide a comprehensive list of all the procedures that conform the deployment and operation phases. Its purpose is to provide a quick and formal reference when facing any expectable situation while participating on the election system.

Each procedure will give information about when it needs to be applied, which role has to perform it, dependencies with other procedures and the list of steps that define it. This procedure list aims at covering all the situations that can be faced by any of the roles acting in any use case of VtUJI. This is an example of how the procedures will look like:

Procedure ID	Procedure's descriptive name
Roles	The role(s) involved in this procedure.
Triggers	- List of the scenarios which would require the execution of this procedure.
Prerequisites	- List of the needs to execute this procedure, including materials, infrastructure and the execution of other procedures.
Following procedures	- List of the procedures that would follow the execution of this one.
1. Numbered list with the steps to perform.	

We'll provide them sorted by their nature (emergency, common, setup, etc.), but we'll also provide them sorted per role, to allow for a quicker reference in oher situations.

Server setup procedures

Procedures associated with the deployment of VtUJI. These will be tho first ones to be performed, before operation.

(SS-01) Key custody committee settlement

SS-01	Key custody committee settlement
Roles	Key custody committee member, Election Authority (if not part of the committee)
Triggers	- Decision to deploy VtUJI
Prerequisites	- Technical assessment on the system requirements and parameters that must be established. - Legal assessment on the commission's composition.
Following procedures	- SS-02

1. Assemble the members of the Election Authority, who will take the decisions over the deployment.
2. Decide on the system operation mode. If 'classical polling station' mode used, end here and repeat this process for each election.
3. Decide on the composition of the committee, you can follow the guidelines described in page 12.
4. Appoint those present or absent who will be part of the commission and brief them on their duties.
5. Decide on the organizational parameters (see page).
6. Appoint the holders for each role and brief them also on their duties.
7. Decide on the technical requirements (see page).
8. Assign tasks to the proper actors so all the requirements are covered before deploying the voting system.

(SS-02) Selection of the operating disk

SS-02	Selection of the operating disk
Roles	Key custody committee member, System administrator
Triggers	- Deployment start.
Prerequisites	- SS-01 - A set of CDs, contaning the vtUJI system, enough for each member plus one. - A permanent marker.
Following procedures	- SS-03 - SE-03

1. The committee and the system administrator will gather on the room where the server is allocated.
2. The system administrator will produce a set of identical VtUJI disks (one per committee member plus one), either before gathering or in the presence of the committee.

3. 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.
4. The rest of the disks will be distributed among the commission. With the only purpose to allow performing auditories over the working copy.
5. 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.
6. Each member is responsible for the protection of his copy against robbery or substitution from an attacker.
7. If desired, any member can now verify that his copy is identical to the working one (see SE-03, 'operating disk verification' procedure).

(SS-03) Voting system establishment

SS-03	Voting system establishment
Roles	Key custody committee member, System administrator
Triggers	- Deployment start.
Prerequisites	- SS-02 - All the requirements to deploy are covered. - a USB drive for each member and the administrator plus one to store the certificate request (if using HTTPS, but optional).
Following procedures	- SS-05

1. The committee will gather. Each one can be accompanied by a technician to overlook the actions of the system, administrator.
2. Each committee member will be given a USB drive (He can provide one of his own if he wants to)
3. All the members will verify their handwritten signature on the disk to rule out any forgery attempts.
4. The disk will be inserted on the server machine and it will be powered on.
5. The system administrator will follow the setup wizard inserting the previously determined parameters.
6. Each member will be prompted to input his USB and type in a new secure password. The USB will be blanked and formatted as a Clauer. A fragment of the key will be written on it.
7. If it was decided to use HTTPS to access the server from the beginning, the administrator will need a USB drive to write down the certificate request (also, the certificate request is published through the web server and he can get it from there at any moment). It will work with a provisional certificate until it gets signed.
8. The administrator will also be able to create a Clauer formatted USB drive for himself (if he doesn't have one yet), as it is used as an additional measure to gain access level on the internal login system. Otherwise, he won't be able to gain the level needed to configure the voting application.
9. From a different computer, the administrator will access the web voting

application. This computer should be his usual one, or one designated by the committee to be used for the voting system configuration, since its IP address will be used as an additional measure to gain access level on the internal login system. Otherwise, he won't be able to gain the level needed to configure the voting application.

10. This application, from the moment the system was set up, is in privileged mode. It allows the administrator to perform dangerous actions. It can be kept this way until the first election is prepared, but you may not hold elections while the administrator is privileged.
11. He must create the users for all the people appointed for administrative roles (election managers and voter registry operators and optionally the committee members) and set up temporary passwords for them.
12. The administrator will set up the remaining parameters on the web application.
13. If you believe the voting application setup is finished, either the administrator using the application or the commission using the system menu will revoke the privileges.

(SS-04) HTTPS mode setup

SS-04 SSL mode setup

Roles	Key custody committee member, System administrator
Triggers	- The need to switch on SSL access to the server after it was installed.
Prerequisites	- SS-03 - Server not currently working with SSL. - USB drive to store the certificate request.
Following procedures	- SS-05 - Obtain a signed certificate from a commonly trusted CA.

1. The committee will gather on the room where the server is located.
2. The minimum number of members to rebuild will be enough.
3. Each of them will be required to insert his Clauer and type in its password. Old key will be rebuilt to check clearance.
4. The administrator will follow the steps and type in the required information.
5. A new certificate request will be written on the USB drive (it will also be published on the web server).
6. The administrator will take care of getting the request signed.

(SS-05) SSL certificate installation

SS-05	SSL certificate installation
Roles	System administrator
Triggers	- The certificate is signed.
Prerequisites	- SS-03, SS-04 - A signed SSL server certificate on a USB drive, with its certification chain on a different file. - The full certification chain on a USB drive
Following procedures	

1. The system will be working with a dummy certificate, so the administrator won't need authorization to install the certificate.
2. Follow the wizard on the system menu.
3. The certification chain and the certificate will be verified. If the root CA is not trusted by the server or there's a gap in the chain, it won't be installed.

Regular server procedures

These are the procedures that will be performed during the operation of the system to keep it working properly and securely.

(SR-01) Key fragments integrity verification

SR-01	Key fragments integrity verification
Roles	Key custody committee member
Triggers	- Regular verification process. Periodicity must be decided.
Prerequisites	
Following procedures	- SR-02, in case of faulty fragments

1. The committee will gather on the room where the server is allocated.
2. All the members must be present, not just the minimum number to rebuild.
3. Each of them will be required to insert his Clauer and type in its password.
4. When all of them are done, it will try to rebuild the key.
5. If any fragment is faulty, the commission will be prompted to renew the key (SR-02)

(SR-02) Key renewal

SR-02	Key renewal
Roles	Key custody committee member
Triggers	- Faulty fragments found on (SR-01). - Key compromise (SE-01)
Prerequisites	- New set of USB drives to write the new key.

Following procedures	

1. The committee will gather on the room where the server is allocated.
2. All the members must be present, not just the minimum number to rebuild.
3. Failing to do so would generate complaints from the members excluded from the custody of the new key.
4. Each of them will be required to insert his Clauer and type in its password. Old key will be rebuilt to check clearance.
5. A new key will be generated.
6. Each member will be given a new USB drive to be formatted as Clauer and protected with a password.
7. A fragment of the new key will be written on it.
8. 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).

(SR-03) System reboot

SR-03 System reboot

Roles	Key custody committee member, system administrator
Triggers	- System goes down after power failure, technical shutdown or some unexpected behavior. - Forced shutdown for maintenance reasons.
Prerequisites	
Following procedures	- SR-04, in case system can't be rebooted properly - SE-03, in case of CD forgery and substitution.

1. The committee will gather on the room where the server is allocated.
2. The minimum number of members to rebuild will be enough.
3. The CD will be extracted and each member will verify his own hand signature.
4. If the CD seems to be forged, perform an operating disk verification (SE-03)
5. Put back the CD into the unit and power on the server.
6. Each of them will be required to insert his Clauer and type in its password.
7. Here, you can choose to perform some special maintenance operation or do a normal boot.
8. When all of them are done, it will try to rebuild the key.
9. During the Clauer insertion, if configuration data read from any Clauer differs, the administrator must examine both versions, select the proper one and discern if it was deliberate or data corruption.
10. If deliberate, legal action must be taken.
11. If configuration data was corrupted, perform a key renewal as soon as the system is started (SR-02).
12. If any error happens, the administrator must be called in to solve it (SR-04).
13. Else, the system will be running properly.

(SR-04) Maintenance operations

SR-04 Maintenance operations

Roles	Key custody committee member, System Administrator
Triggers	- Programmed maintenance actions. - Resolving envisaged anomalous situations (which can be resolved using the actions listed in the server's wait menu except opening a full access terminal).
Prerequisites	- Supervising technicians, if an election is ongoing
Following procedures	- SE-05, in case the situation could not be resolved using the actions on the menu

1. The committee will gather on the room where the server is allocated.
2. The minimum number of members to rebuild will be enough.
3. Each one can be accompanied by a technician to overlook the actions of the system, administrator, but it's not critical.
4. If an election is ongoing, it's a far more critical procedure, and technical supervision is required.
5. The administrator will choose the action he needs to perform.
6. Each of them will be required to insert his Clauer and type in its password.
7. When all of them are done, it will try to rebuild the key as a clearance check.
8. The administrator will perform the operations he has been granted to.
9. Repeat from 5 to 9 for each action needed.
10. If the situation is not resolved, proceed to grant full system access through a terminal (SE-05). Here, meticulous technical supervision is critical

(SR-05) System health monitoring

SR-05	System health monitoring
Roles	System Administrator
Triggers	- Regular checks.
Prerequisites	
Following procedures	- SR-04, in case some anomalous situation is found - SE-02, in case of physical data support degradation. - SE-05, if the problem can't be solved with the menu options.

1. The system administrator will regularly check his e-mail for system status notifications, and the status graphics to search for anomalous patterns.
2. If detected, he will try to diagnose the origin of the anomaly (either it is the influence from a remote source or inner malfunctioning)
3. If remote, he will communicate with the people in charge of network administration to try to palliate its effects.
4. If local, he will evaluate the extent of the hazard and summon the committee as soon as needed.
5. The number of summoned members depends on the actions to be taken. If the situation requires to generate a new cyphering key, all the members must be present, otherwise, the minimum will be enough.
6. Proceed with the proper procedure according to the situation.

(SR-06) SSL Certificate renovation

SR-06	SSL certificate renovation
Roles	Key custody committee member, system administrator
Triggers	- The certificate has expired or is near expiration date. - Any reason to re-issue the certificate (revocation, key weakness, etc).
Prerequisites	
Following procedures	

1. If your CA requires private key renewal, the server administrator will need access to the server machine.
2. If your CA doesn't need or allow key renewal, you don't need to access the server room, since the certificate request can always be read from a URL http://YOUR_SERVER/server.csr
3. If the system is working with an invalid certificate (self-signed dummy or expired), the administrator won't need authorization to install the certificate.
4. If the system is working with a valid certificate (revoked certificates are still valid, since we don't check for it), the committee must be gathered to grant clearance the usual way.
5. If key renewal is needed, follow the wizard on the system menu to generate the new key and request (system will keep working with the current valid certificate).
6. The certificate will be handled and signed the usual way.
7. Once the certificate is signed, it has to be installed.
8. If the current certificate is valid, the committee must be gathered to grant clearance, else, server administrator can do it alone.
9. The certification chain and the certificate will be verified. If the root CA is not trusted by the server or there's a gap in the chain, it won't be installed.

Emergency server procedures

These procedures represent what needs to be done when facing unexpected situations that could threaten the security of the system, the confidence on it and to avoid data loss.

(SE-01) Key fragments compromise

SE-01	Key fragments compromise
Roles	Key custody committee member, system administrator
Triggers	- Any number of committee members have lost their Clauer containing the key fragment or suspect that its security has been violated.
Prerequisites	- New set of USB drives.

Following procedures	- SR-02, in case of minor security breach - SE-02, in case of severe security breach. - Legal action in relation with the incident.

1. The committee will gather. System administrator can give technical advice on the decisions.
2. The severity of the breach must be evaluated.
3. If the number of compromised fragments is smaller than the minimum to rebuild the key, it will be enough to invalidate the this key and replace it. Perform a key renewal (SR-02)
4. If there's a minimal chance that the key could be rebuilt by the attacker, a data relocation will be needed ton ensure the inner cypher key is renewed.
5. Legal action will be taken in relation with the incident.

(SE-02) Inner system key renewal and data relocation

SE-02 Inner system key renewal and data relocation

Roles	Key custody committee member, system administrator
Triggers	- Data physical support is faulty and there's risk of breakdown. - Outer cyphering key may be compromised.
Prerequisites	- New set of USB drives.
Following procedures	

1. The committee will gather on the room where the server is allocated.
2. All the members must be present, not just the minimum number to rebuild.
3. Each one can be accompanied by a technician to overlook the actions of the system, administrator, but it's not critical.
4. If an election is ongoing, it's a far more critical procedure, and technical supervision is required.
5. Each of them will be required to insert his Clauer and type in its password.
6. When all of them are done, it will try to rebuild the key as a clearance check.
7. The administrator will perform the necessary operations following the wizard on the server.
8. A new key will be generated.
9. Each member will be given a new USB drive to be formatted as Clauer and protected with a password.
10. A fragment of the new key will be written on it.
11. Once all the key fragments are delivered, data will be transferred to the new location.
12. Once data is transferred and verified, the old key will be erased and the old Clauer set can be stored for a future use or discarded (if faulty)

(SE-03) Operating disk verification

SE-03	Operating disk verification
Roles	Key custody committee member, system administrator
Triggers	- Any committee member wants or needs to verify that the working system CD is legitimate.
Prerequisites	- The CD copy from each member - Supervising technicians
Following procedures	- Legal action to prosecute those responsible for the forgery.

1. The member who initiated this procedure should perform an auditory on his copy of the CD to verify if it is legitimate.
2. If his copy is not legitimate, the process still should be done to determine the extent of the issue (perhaps the only tampered copy is his copy).
3. The committee will gather on the server room.
4. The minimum number of members to rebuild will be enough, but it is recommended to gather all of them.
5. 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).
6. Each member must bring his own copy of the CD
7. Each one of the remaining members can be accompanied by a technician to overlook and/or reproduce the actions of the previous.
8. The working copy will be extracted and handed to all the members, so they can verify their handwritten signature.
9. The verification process will be to obtain the hash value for each CD using different common secure hashing algorithms (SHA1, SHA256, MD5, etc.)
10. The working copy will be handed to the designated technician to obtain the hashes, they will be posted somewhere visible.
11. The working copy will be handed to the system administrator to obtain the hashes for confirmation.
12. The working copy will be handled to any other technicians brought by the commissioners, one at a time, to obtain the hashes them too.
13. 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.
14. If any of the results differ, all the different copies must be audited to check which is the legitimate one.
15. Legal action will be taken to discover who is responsible for introducing tampered copies.

(SE-04) Voter/Candidate system auditing

SE-04	Voter/Candidate system auditing
Roles	Key custody committee member, voter
Triggers	- A voter (or candidate) wants to verify if the working copy is

	legitimate.
Prerequisites	
Following procedures	- (SE-03)

1. The voter/candidate must obtain a legitimate copy of the system.
2. If wanted, he can order an auditory over it to check its legitimacy
3. The voter/candidate will contact a commissioner of his confidence.
4. The voter/candidate will check his copy against the commissioner's.
5. The commissioner will arrange a working copy verification (SE-03).
6. The voter/candidate may be present during this procedure, depending on his confidence on the commissioner.

(SE-05) Unrestricted access to the system

SE-05 Unrestricted access to the system

Roles	Key custody committee member, system administrator
Triggers	- Resolving system anomalous situations not envisaged on the regular operation of the system.
Prerequisites	- Procedure (SR-04) executed but not resolving the situation. - Supervising technicians
Following procedures	

1. The committee will gather on the room where the server is allocated.
2. The minimum number of members to rebuild will be enough.
3. Each one can be accompanied by a technician to overlook the actions of the system, administrator.
4. 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.
5. Each of the commissioners will be required to insert his Clauer and type in its password.
6. When all of them are done, it will try to rebuild the key as a clearance check.
7. 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.
8. The administrator will be prompted with a terminal.
9. 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.
10. The administrator will have to explain each action before performing it and give time for the technicians to take notes.
11. After solving the problem, the administrator will close the terminal session

and return to the idle state.

(SE-06) Administrator substitution or credential reset

SE-06	Administrator substitution or credential reset
Roles	Key custody committee member, system administrator
Triggers	- The system administrator forgot his credentials - The system administrator credentials' are compromised. - The system administrator needs to reset his support credentials (associated IP address and Clauer ID) - The system administrator is temporary/permanently disabled and needs to be replaced.
Prerequisites	
Following procedures	

1. The committee will gather on the room where the server is allocated.
2. The minimum number of members to rebuild will be enough.
3. The proper menu option will be chosen depending on what we need (new administrator or credential reset).
4. Each of the commissioners will be required to insert his Clauer and type in its password.
5. When all of them are done, it will try to rebuild the key as a clearance check.
6. If credential reset is being performed, the administrator will input his new password (it can be the old one if it's not degraded or compromised)
7. If a new administrator is being added, he will be asked to insert all his personal information (whether he already was a registered user or not).

Election setup procedures

These are the procedures related with the creation and set up of electoral processes, using the web application. Detailed information about the usage of the application will be provided later and on the role guides. Here we'll only describe the general procedure, focusing on administrative constraints, that cannot be represented on the application.

(ES-01) Election creation

ES-01	Election creation
Roles	Election administrator, election authority
Triggers	- Election Authority decides to hold one or more related elections.
Prerequisites	- A Ballot configuration, with the candidates or pollings the voter can choose among. - Polls opening and closing dates (elections can span over

	several days). - A drafted board of officers. - The census rolls, reviewed and correct.
Following procedures	- ES-03

1. The election administrator receives all the information he needs from the election authority to set up the elections.
2. He must only perform this procedure on their request. Organizing unscheduled elections on his own volition could be severely punished, depending on the current electoral law.
3. The election administrator logs into the system. He will need an access level of 2, so he must also use any corporate external login if available or do it from his usual computer.
4. The election administrator creates the polling post and inputs all the data specified above. Once it is done, he will set it as *programmed*.
5. An election can be configured to allow ballot admission verification or not, depending on the situation.
6. For each election, the authentication needs must be defined. You can choose to offer several ways to authenticate or require various methods at a time to allow the elector to vote. It depends on your needs, but it is always recommended to use the local authentication, since it is the only one that doesn't depend on external sources.
7. Using the notification interface, he will inform about the election to all the electors and to the board of officers. Additionally, all the electors without valid credentials will be notified with a different message and encouraged to obtain them before the election if they wish to participate.
8. The officials and the voters must be given access to the user manuals for their roles.

(ES-02) Credential distribution

ES-02 Credential distribution

Roles	Voter registry operator, voter
Triggers	- A voter wants to participate on an election, and he has no access credentials.
Prerequisites	- An accessible physical voter registration point. - Enough supply of printed voter cards - The voter needs an identifying document (some id card) with a photo. - An inner procedure to discern if a person can be part of this voting system. - An inner procedure to obtain reliable corporate data from the user (such as his user name and e-mail address).
Following	

procedures	

At the registration point

1. The voter will arrive at the registration point, acting for himself, not on behalf of a third one.
2. The voter hands over his id card to the operator.
3. The operator will visually check that the id card is consistent with his holder, by checking the photograph and asking him some of the data on the card.
4. The operator will check if this voter is allowed to be part of the system (through a procedure he will have been briefed, if applicable)
5. The operator will input the ID number to check if the voter is already on the system.
6. If he is on the system, he will check all the fields with the ID card and correct any mistakes.
7. If not, he will fill in the fields with the information found on the id card. Any information not present on the ID card (like the e-mail address) must be acquired through corporate procedures or left blank.
8. The user name is a special case. If not on the Id card and there's no corporate method to obtain it (maybe voters don't have one at all), the Id card number will be also used as user name.
9. The Id card is handed back to the voter.
10. The voter is informed about the user name he must use (either his ID number, the corporate or a new one).
11. A box of voter cards is offered to the voter, who will pick a random one and give it to the operator.
12. The operator writes the user name on the card.
13. The voter will sign now any data transfer agreement or contract your organization requires to.
14. The operator will input the password on the card using a bar code reader and write the data on the system.
15. The card is handed over to the voter.
16. He must finish this procedure within 48 hours, otherwise, credentials are void and the process must be restarted.

At the voter's computer (within 48 hours)

17. The voter will access the voting system from his trusted computer.
18. The voter will log into the voting system using his id number/user name and the temporary password.
19. He may also be asked to log in with a corporate login system, as a security measure.
20. The system will generate the new password, which must be written down on the voter card.
21. The voter must store and keep the card properly, until the election date.

(ES-03) Election revision and validation

ES-03	Election revision and validation
Roles	Election authority, Election administrator, Polling post official, Polling post board chairman
Triggers	- An election is created and programmed.

Prerequisites	
Following procedures	- EC-01

1. Once the election is set up, it needs to be reviewed and accepted before polls are opened.
2. The board of officials is required to log into the voting system between the set up date and the celebration date.
3. Each member will personally (or with the help of others) check that the ballot contains the expected choices, candidates and configuration, and that the voter rolls contain the expected names, according to the interests they represent.
4. Any irregularities or incidences found can be reported to the chairman using the voting application.
5. The chairman must report any incidences found by him or by other officers to the Election Authority.
6. The election administrator will correct any mistakes reported by the Election Authority (addition and deletion of voters or candidates and ballot layout or content corrections).
7. Once the board is notified that the deficiencies are fixed, they must check them again.
8. If everything is as expected, they will mark the election as reviewed, adding any desired comment, which will be seen by the chairman.
9. The chairman will read their comments and put or summarize them on the comments section of the election opening records.
10. By the end of this process, all the officials must have reviewed the rolls and ballots or must have a legitimate excuse for avoiding this duty. The chairman is in charge of checking this periodically until the polls opening day.

Election celebration procedures

The whole of these procedures will be performed during the normal course of an election. They represent the proper way of holding an election with vtUJI from the point of view of all the actors involved, filling the procedural gaps not covered by the application.

(EC-01) Polling station aperture

EC-01	Polling station aperture
Roles	Polling post official, Polling post board chairman, election manager
Triggers	- Less than 30 minutes left to open the polls.
Prerequisites	- ES-03
Following	- EC-04

procedures	- EC-03

1. The chairman will log into the voting system.
2. If some official hasn't checked the rolls and the ballots yet, he must contact him to get an explanation. This incidences will be recorded on the polls opening record.
3. When all the officials have been checked or dismissed, the chairman will write and review the opening record and open the polling station.
4. If the chairman is the absentee, the alternate chairman can take his position. To avoid collisions, if the chairman logged into the system but didn't do his duty, the alternate chairman won't be able to take the position before 10 minutes.
5. If both chairmen are absent, any other officer can take their position. They will be able to do so one hour after the expected polls opening time (also with a 10 minute exclusion period if the chairman is logged, but not if the alternate chairman is).
6. If no officials are available, the election manager will contact the election authority and set up an emergency board of officers.

(EC-02) Polling station closure

EC-02 Polling station closure

Roles	Polling post official, Polling post board chairman, election manager
Triggers	- The voting period is over
Prerequisites	- EC-01
Following procedures	- EC-03

Tallying

1. The chairman will log into the system.
2. The polling station panel board will show the status of the election, number of cast votes and number of received votes, etc.
3. If the election is over and all the cast votes already are in the ballot box, there will be a button to open the ballot box. He must push it.
4. If some votes were cast using the LCN, they need an extra period to arrive to the ballot box. At the end of this period, the button will appear.
5. After this period, if all the cast votes are not in the ballot box, the system will lock its aperture for one more hour and warn the chairman.
6. After this new period, if there still are missing votes, or If any problem or irregularity was warned by the system, the chairman will contact the election authority to get instructions. Ballot box can be opened, but he must do so only if instructed to by the election authority.

Verification

7. Each officer will log into the system when they are notified that the tallying is finished.
8. There, they must check the census again, to verify that no illegitimate voters were added during the election by the election administrator (they are marked for clearer identification).
9. They will check the results of the tallying for irregularities or unexpected

patterns.
10. When done, they will check it as reviewed and write down any observations or complaints, and all the incidences they received from the voters during the celebration.
11. The chairman will review all the comments an contact the election authority if necessary. A selection and summary of the incidences will be put on the records.
12. After a reasonable period, the chairman will contact any officers who haven't reviewed the results and the added voters. Anyone without legitimate reasons to avoid this duty will be reported as absent on the record.
13. The chairman will fill in the record and close the polling station. He can send the records to anyone interested in it.
14. Records can be sent again any moment.
15. Like on the aperture, if the chairman is absent, any officer can take his position after one hour past the closing time, with a 10 minute exclusion period if the chairman logged in (of course, the alternate chairman is now unable to operate, since he was excluded at the opening).

16. This whole process can be performed by the election manager 24 hours after the closing date if all the officers are absent or incapacitated.

(EC-03) Election records signature

EC-03	Election records signature
Roles	Polling post official, Polling post board chairman
Triggers	- An election is done and tallied, records are settled and accepted and there's a need to distribute legitimate and verifiable copies of them.
Prerequisites	- EC-02 - Each officer who wants to sign them has a digital certificate and knows how to use it.
Following procedures	- EC-06

1. Each officer will log into the system any time (preferably short) after the election.
2. This operation is exclusive. Two members can't do it at the same time. The system is failsafe, but to avoid confusion they should arrange themselves to avoid collisions.
3. The officer will access the polling station and the signing interface.
4. He must choose the method he wants to use, depending on the software available and on the medium he stores his certificate.
5. He must follow the steps to sign all the records (one for the aperture and three for each election held on this poling station)

6. This procedure can be performed just once after the election period or once at the beginning to sign the aperture record and once at the end to sign the results, voters, and verification codes records.

(EC-04) Participation in an election

EC-04	Participation in an election
Roles	Voter, Polling post official
Triggers	- An elector wants to participate on the electoral process.
Prerequisites	- EC-01 - ES-02 if local authentication is being used (recommended)
Following procedures	- EC-05 if the election was configured to allow it.

1. The voter connects to the voting system.
2. If he is following a link from an e-mail, he must check this URL to avoid phishing (see section '*Checking URLs*' at page 16).
3. If he is redirected to a default login method, he should use it. Before typing any private information, he must check the URL to determine if it is safe enough.
4. If by any chance he doesn't want to, he can access again the voting system and he will be directed to the login selection page.
5. He will log into the system using any method available. Again, he must check the URL to determine its security (although irresponsible, the server could be working without SSL).
6. On the pending elections section, a pending election will initiate.
7. If any number of elections are mutually exclusive, he will be prompted to select which one he wants to participate in. This decision is indefeasible.
8. He can choose to vote or to skip to another pending election.
9. If any election has different authentication needs (more or different authentications), it won't let him vote until he has gained such access level.
10. Once he is allowed to vote, he will be shown a ballot, which shall be filled with the desired options.
11. Predefined ballots can be offered. The voter is allowed to use them and edit its content before sending it.
12. Once the voter has filled the ballot, he must hit the send button. He will be presented with the real text to be sent to the ballot box, for a last check. If he is not happy with it, he can restart the process by hitting 'Cancel' and editing the ballot again.
13. Once he has accepted the ballot, he must wait until the button shows that the ballot has been admitted. Closing the browser before that, would discard the ballot and make him loose his right to vote.
14. A log area may appear beside the button. This area shows errors and important messages about the ballot sending. The voter must read them and act as instructed.
15. After sending the vote, if the election allows it, a participation verification code will appear. If the voter wants to, he can copy or print it to verify that his vote was correctly admitted once the election is finished (EC-05).

---

16. Once the vote has been cast, the voter must hit 'Continue'. If there are other pending elections, another one will initiate.
17. If he wants to abstain from voting in a pending election, he must hit 'Abstain', and the next pending election will be loaded.

Unexpected situations

18. If he can't authenticate or gain the level he needs, he must perform the EE-02 procedure immediately.
19. If he didn't establish a permanent password, he must request his credentials (ES-02).
20. If the election he intends to vote in is not shown as pending but it is listed on the past elections section, and he hasn't participated yet, it is a case of impersonation. He must denounce this to the board of officers (EE-05) and then reset his credentials (EE-02). The board will act as needed by the situation.
21. If the election is neither on the pending nor past election section, he has been accidentally left out of the rolls, and he must contact the board of officers (EE-05) to demand a census addition (EE-03).
22. If there was an internal problem during the voting process, the application will show a password. The voter must write it down immediately if he doesn't want to lose his right to vote. When problems are solved, he must restart the voting process. He will be asked to provide the password to unlock his voting rights.
23. If the voter has been the victim of or knows of coercion attempts, or is aware of vote selling cases, or any other irregularities that could have an effect over the election results, he has the duty to report them (EE-05).
24. At any moment, the voter can contact the board of officers to resolve any doubts or questions he may have (EE-05).

(EC-05) Participation verification

EC-05 Participation verification

Roles	Voter
Triggers	- A voter wants to verify that his ballot was admitted.
Prerequisites	- EC-04 - The election must allow participation verification.
Following procedures	

1. After the polls are closed and the results are published, if the election allows it, there will be a link to the verification codes list.
2. The verification code shouldn't be handled unwittilnlgy. Eventhough the voting system is totally locked, it is the only link between a voter and his ballot. In the remote event of a server leak, it could be used to reveal what were the choices of the voter.

3. The full list of codes will appear.
4. The voter will search for his code visually or using the browser built-in search tool, but it shouldn't be typed on any web page form.
5. If the code is on the list, his vote was properly admitted and was not manipulated at all.
6. If not, he should contact the board of officers to be instructed about what to do (EE-05).
7. The absence of this verification code is not a legally binding proof that the vote was deliberately discarded or rejected, since there's no way to verify that the vote was ever sent, for privacy reasons.

(EC-06) Ballot deletion

EC-06	Ballot deletion
Roles	Election administrator
Triggers	- Most electoral systems require the destruction of ballots after a determined period of time.
Prerequisites	- EC-02
Following procedures	

1. Most electoral systems require the destruction of ballots after a determined period of time, but this may vary from one to another.
2. Additionally, ballots should be kept for some time after the tallying as a last resource for election auditory (it could be exceptionally opened and the ballots extracted for a third party tallying).
3. After the election is closed, the election administrator has a control to destroy them, from the election setup interface.
4. This destruction can technically be done at any moment, but he must do it only when he is allowed by the current electoral law.
5. Otherwise, investigation and prosecution may be applied.

(EC-07) Physical polling post establishment

EC-07	Physical polling post establishment
Roles	Election administrator, polling post official
Triggers	- The need to establish a physical polling post, to give service to voters without access to a reliable Internet connected computer.
Prerequisites	- ES-03
Following procedures	

1. Voters are not assigned to a single polling station, so they can use any on to their convenience.
2. The needs are: a computer, a connection to the Internet, a voting booth

---

and a board of officers for this polling post, a set of voter liveCD discs (one more than the number of officers), technical help on call and a room to hold all the people and the material.

Board setup

3. The selected personnel to attend the post combines part of the roles of the polling station officer and the key committee.
4. As the key committee, they must represent the interests of the organizers plus the interests of all the parties. Their number and composition isn't as critical as the key committee's, since they must be all present during all the voting period.
5. They don't have any duties nor special roles on the voting application, they are plain voters.

Facilities setup

6. The Internet connection hardware and the computer must be located in a way that has to be easy to guard and hard to access by the bystanders, to avoid sabotage.
7. The computer is the polling machine, and has to be inside the booth, but only the peripherals. The processing unit must be outside and guarded at all times by the board. Any other physical protection measures are welcome.

Post setup

8. A representative of the election authority, will provide the board with the set of discs.
9. The board will perform a disc selection procedure (SS-02), but with this discs.
10. The system will be started with the operating disk and the accessibility to the voting system will be checked.

Post operation

11. During the election, the duties of the officer board will be to watch over the integrity of the computer, ask for technical assistance and provide assistance to the voter in case they ask for it.
12. If they detect that a voter is trying to tamper with the voting computer, they just need to reboot it and all the configurations will default.
13. They will report on a record any incidence that may happen.

Post Closure

14. After the polling post is closed, they will send the operating disk to the election authority, as a proof of the reliability of the post.

Emergency electoral procedures

These procedures represent what has to be done to handle undesirable situations that may occur, in a way consistent with the voting system. Failing to follow these procedures may lead to an anomalous situation on the voting system that when detected could be interpreted as malicious and require further investigation and in some cases, prosecution.

(EE-01) Administrative user's support credentials reset

EE-01	Administrative user's support credentials reset
Roles	System administrator, key custody committee
Triggers	- When an administrative user (system administrator, voter registry operator, polling post official) needs the support credentials (usual IP address, Clauer ID) to gain certain access level and these credentials have changed.
Prerequisites	
Following procedures	

1. The user will contact the system administrator as soon as he knows he will need the reset.
2. The system administrator will add him to a list of pending resets, since this operation requires authorization from the key committee..
3. The list of pending resets will not be processed at regular periods of time. It will depend on the urgency of each incoming request, while trying to minimize the frequency. The administrator will have to take this decision.
4. The administrator will gather the committee as soon as possible.
5. The minimum number of members to rebuild will be enough.
6. They will perform a maintenance procedure (SR-04)
7. The administrator will reset the desired parameters for each user.

(EE-02) Voter credential reset

EE-02	Voter credential reset
Roles	Voter, voter registry operator
Triggers	- A voter wants to but is unable to access the system (due to credential loss or theft).
Prerequisites	
Following procedures	

1. The voter will go to the registry point and identify himself with an ID card.
2. If the voter suspects that his credentials were stolen, the registrar is a potential culprit, so he should go to a different registry point.
3. The registrar will ask him his motives to reset the credentials and will check if the voter was doing things the right way.
4. He must ask the voter if he succeeded at logging in. If that's the case, he must ask if he could see the expected election on the past elections section (possible impersonation) or if he could see at all (accidental disenfranchisement, see EE-03).
5. He must check if the voter properly performed ES-02, to discern a misuse from a credential theft.
6. If the voter or the registrar suspect there was a credential theft, the registrar will search the voter on the system and write down which operator last set his credentials and when.
7. If the voter can assure that he was not present at that location on that

precise moment, all this information will be sent to the election authority to start an investigation about the incidence (suspects are the same operator or an impersonator).
8. After this, or if it was a simple credential loss, they will perform an ES-02 procedure to reset them.

(EE-03) Elector addition/deletion during an election

EE-03	Elector addition/deletion during an election
Roles	Election administrator, election authority
Triggers	- The election authority has admitted a claim from an elector that he was mistakenly left out of the rolls and he has the right to participate. - The election authority has admitted a claim that an elector was mistakenly on the rolls while he has no right to participate, and he didn't vote yet.
Prerequisites	- EC-01
Following procedures	

1. The election administrator will receive a warrant from the election authority along with the user data.
2. He will log into the system and get into the election configuration interface.
3. He will add/delete the voter (if still possible, since you can't delete a voter who has yet voted).
4. Doing such actions without authorization from the election authority will be detected after the tallying and the administrator would face prosecution.
5. If the voter that was not authorized to, had already voted, the election administrator will notify the election authority about the incidence, so they can apply the election code measures.

(EE-04) Closing time delay

EE-04	Closing time delay
Roles	Election administrator, election authority
Triggers	- For some reason (for example, technical problems to access the voting server), the participation time was not enough and needs to be extended.
Prerequisites	- EC-01
Following procedures	

1. The election administrator will receive a warrant from the election authority

and the new close date.
2. He will log into the system and get into the election configuration interface.
3. He will change the closing date.
4. Doing such action without authorization from the election authority will be detected after the tallying and the administrator would face prosecution.

(EE-05) Issues and irregularities reporting

EE-05	Issues and irregularities reporting
Roles	Voter, polling post official , election authority
Triggers	- Any voter wants to denounce any irregularity or difficulty suffered or witnessed while exercising his right to vote.
Prerequisites	- EC-01
Following procedures	

1. The voter can use any communication channel established by the current election law.
2. Alternatively, he can communicate with the board of officials who will advise and direct him to the proper destination for his complaints.
3. The user can use the election related form, on the active or past election section, where he will have to tell the official he wants to communicate with (or all of them).
4. Also, if the voter has lost his authentication capabilities, the user can use the unauthenticated form on the login page, where he will also have to input his ID number (an identifier, but not an authenticator) and select the election he is concerned about.

(EE-06) Unexpected issues/situations

EE-06	Unexpected issues/situations
Roles	
Triggers	- Any situation that may happen and is not treated above.
Prerequisites	
Following procedures	

1. To solve any not expected situation, any actor must contact the election authority, since it is the highest decision organism.

By role

For your convenience, we present here a list of the procedures arranged by role instead of by phase. This way, any actor can have an overview of all the procedures he is involved in.

Key custody committee member

(SS-01) Key custody committee settlement
(SS-02) Selection of the operating disk
(SS-03) Voting system establishment
(SS-04) HTTPS mode setup
(SR-01) Key fragments integrity verification
(SR-02) Key renewal
(SR-03) System reboot
(SR-04) Maintenance operations
(SR-06) SSL Certificate renovation
(SE-01) Key fragments compromise
(SE-02) Inner system key renewal and data relocation
(SE-03) Operating disk verification
(SE-04) Voter/Candidate system auditing
(SE-05) Unrestricted access to the system
(SE-06) Administrator substitution or credential reset
(EE-01) Administrative user's support credentials reset

System administrator

(SS-02) Selection of the operating disk
(SS-03) Voting system establishment
(SS-04) HTTPS mode setup
(SS-05) SSL certificate installation
(SR-03) System reboot
(SR-04) Maintenance operations
(SR-05) System health monitoring
(SR-06) SSL Certificate renovation
(SE-01) Key fragments compromise
(SE-02) Inner system key renewal and data relocation
(SE-03) Operating disk verification
(SE-05) Unrestricted access to the system
(SE-06) Administrator substitution or credential reset
(EE-01) Administrative user's support credentials reset

Election administrator

(ES-01) Election creation
(ES-03) Election revision and validation
(EC-01) Polling station aperture
(EC-02) Polling station closure
(EC-06) Ballot deletion
(EC-07) Physical polling post establishment
(EE-03) Elector addition/deletion during an election
(EE-04) Closing time delay

Voter registry operator

(ES-02) Credential distribution

(EE-02) Voter credential reset

Polling post official

(ES-03) Election revision and validation
(EC-01) Polling station aperture
(EC-02) Polling station closure
(EC-03) Election records signature
(EC-04) Participation in an election
(EC-07) Physical polling post establishment
(EE-05) Issues and irregularities reporting

Polling post board chairman

(ES-03) Election revision and validation
(EC-01) Polling station aperture
(EC-02) Polling station closure
(EC-03) Election records signature

Voter

(ES-02) Credential distribution
(EC-04) Participation in an election
(EC-05) Participation verification
(EE-02) Voter credential reset
(EE-05) Issues and irregularities reporting
(SE-04) Voter/Candidate system auditing