Principles and requirements for a secure e-voting system

Dimitris A. Gritzalis [1,2]

[1] Dept. of Informatics, Athens University of Economics and Business, 76 Patission Ave., Athens GR-10434, Greece (dgrit@aueb.gr).

[2] Data Protection Commission of Greece, 8 Omirou St., Athens GR-10564, Greece.

Abstract

Electronic voting (e-voting) is considered a means to further enhance and strengthen the democratic processes in modern information societies. E-voting should first comply with the existing legal and regulatory framework. Moreover, e-voting should be technically implemented in such a way that ensures adequate user requirements. As a result, the aim of this paper is twofold. Firstly, to identify the set of generic constitutional requirements, which should be met when designing an e-voting system for general elections. This set will lead to the specific (design) principles of a legally acceptable e-voting system. Second, to identify, using the Rational Unified Process, the requirements of an adequately secure e-voting system. These requirements stem from the design principles identified previously. The paper concludes that an e-voting capability should, for the time being, be considered only as a complementary means to the traditional election processes. This is mainly due to the digital divide, to the inherent distrust in the e-voting procedure, as well as to the inadequacy of the existing technological means to meet certain requirements.

Key words: Electronic voting, Secure voting, Digital divide, Functional requirements, Rational Unified Process, Use cases.

Acknowledgements:This work has been supported in part by the European Commission, IST/e-vote project ("An Internet-based electronic voting system"). The author wishes to thank C. Lambrinoudakis, L. Mitrou, as well as the anonymous referees, for their valuable comments and suggestions. References on pp. 552-4.

1. Introduction

The emerging Information Society has enabled people in the developed countries to perform several of their activities in a direct, electronically automated and efficient way. To keep up with the need to provide citizens with the ability to benefit from services over networks, as well as to reduce the cost and bureaucracy of public administration, governments are striving to transfer an increasing number of their activities to the new medium.

E-voting can be an efficient and cost effective way for conducting a voting procedure and for attracting specific groups of people (e.g. young or disabled electors) to participate [1]. The term e-voting (electronic voting) is used hereby to denote a voting process, which enables voters to cast a secure and secret ballot over a network. In this paper, e-voting refers to general elections and/or referenda, at state and/or local level, with binding effects.

Many public authorities are, in general, concerned with the compliance of electronic voting systems with the existing legal (i.e. constitutional) framework. The first aim of the paper is to discuss whether an e-voting scheme could meet the legal requirements, as these are laid down in the modern information societies. The paper discusses how an e-vote process should be designed and implemented, in order to comply with the democratic election principles and rights, as well as to the other human rights, which constitute the cornerstone of the international legal civilization. Along these lines, the requirements of an electronic voting system are considered as the design principles, which are essential to comply with, in order to conform to the legislation framework, which is governing general elections [2]. Although technology moves at a pace faster than the legal system does, technological evolution should be pursued as a means to improve human life, as opposed to an end by

ELSEVIER ADVANCED TECHNOLOGY

Computers & Security
Vol 21, No 6, pp 539-556, 2002

0167-4048/02US$22.00

Dimitris Gritzalis

Dimitris Gritzalis holds Ph.D. (Information Systems Security), M.Sc. (Computer Science) and B.Sc. (Mathematics) degrees. He is an Assistant Professor of Computer and Network Security, with the Dept. of Informatics of the Athens University of Economics and Business (Greece), where he leads the Infosec Research Group. He is, also, an Associate Data Protection Commissioner of Greece.

itself. In this respect, the technological developments — and in particular those affecting fundamental principles — should be carefully reviewed with an eye towards ensuring their contribution to the improvement of the quality of the citizen life.

The second aim of this paper is to discuss confidence upon technology. Information system developers face e-vote systems with an eye towards ensuring their adequate level of security [3-7]. In recent literature, a distinction is often made between different types of e-voting systems requirements [8]. In literature, requirements are usually identified as legal, technical and user-oriented — the latter in the form of conditions the system should meet (e.g. "the system *shall* allow online-voting from home"). Other authors select a specific election procedure (e.g. the paper absentee ballot process [9]), deriving requirements for electronic voting systems based solely on this procedure. Although such approaches may produce acceptable e-voting systems in given contexts, they have not yet led to the specification of a complete system. This paper focuses on the elicitation of the legal and functional requirements of an e-voting system, through a User Requirements Specification suitable for providing information system designers with the essential information for designing a valid and complete system. A milestone, towards this end, is the development of a generic e-voting model by depicting the principles and practices to be followed during an election procedure.

The paper is structured as follows: section 2 refers to the main issues regarding e-voting for general (public) elections and summarizes the generic constitutional requirements and the corresponding design principles such an election process should meet. Section 3 analyzes further a voting system design principles. Section 4 presents briefly the methodology, which will be used to identify and describe the user requirements of an e-voting system, while Section 5 overviews briefly the traditional voting model. Section 6 provides the reader with the functional security requirements of an internet-based e-voting system, while Section 7 describes the non-functional security requirements. Section 8 argues why an e-voting system should be considered only as complementary to traditional systems. Finally, Section 9 concludes the paper.

2. E-voting main issues

A fundamental challenge of electronic democracy is to improve and develop representative democracy and strengthen processes aiming at the empowerment of citizens [10]. The new civilization, brought about by the Information Society, should comply with the principles and values of democracy. The introduction of an e-voting system should conform to this rule, since voting is one of the functions "e-citizens" may wish to see performed online. In this respect, a phenomenon, which should be taken under consideration, is the digital divide. Affordable access to the Internet is a key to fight the digital divide between the "info -rich" and the "info-poor" in an Information Society. Specific policies should be adopted towards this end. The European Union, for example, has adopted three key actions: a) to adapt the existing regulatory framework to communication industry needs in the Internet, b) to boost competition in local access networks, so as to encourage widespread Internet take-up and high-speed Internet access in Europe, and c) to ensure a high standard of user rights and privacy protection.

An election system may, by itself enforce unequal access of an individual to the electoral process [11]. It is a matter of democracy, equality, and equity to guarantee that the traditional and the e-voting technologies are equivalent, with respect to ease and opportunity of access. Parliamentary elections have to be free, equal and secret. At the same time, the

election procedure has to be transparent and subject to public scrutiny.

The constitutions of many countries require that general elections should respect Generality, Freedom, Equality, Secrecy, and Directness. Adding to them the fundamental requirement of Democracy, the set of generic constitutional voting requirements stems with. This set reflects, in turn, to the set of the essential voting design principles (Table 1).

Table 1: Constitutional requirements and design principles

Constitutional requirements	Voting systems design principles
Generality	1.1 Isomorphic to the traditional
	1.2 Eligibility
Freedom	2.1 Uncoercibility
	2.2 No propaganda in the e-voting site
	2.3 Non-valid voting capability
Equality	3.1 Equality of candidates
	3.2 Equality of voters
	3.3 One voter - one vote
Secrecy	4.1 Secrecy
	4.2 Balance security vs. transparency
Directness	5.1 Unmonitored ballot recording and counting
Democracy	6.1 Trust and transparency
	6.2 Verifiability and accountability
	6.3 Reliability and security
	6.4 Simplicity

3. Voting systems design principles

3.1 Generality

Universal suffrage is a generic principle for democratic elections, requesting that every eligible voter can participate in the election process, and nobody can be excluded or discriminated. The consequences deriving from this principle are the following:

1. Every voter has the right to participate in an election process.
2. The ability to participate in an election process (eligibility) must be founded on and be controllable by the law.
3. Voting possibilities and technologies should be accessible by every voter.
4. e-voting should be considered as an alternative way of exercising one's voting rights.
5. The democratic principle (i.e. every eligible voter should be included in the election process) leads to publicly available appropriate infrastructure (e.g. public internet kiosks, internet voting in state offices, etc.), in order to allow citizens to exercise their rights.

E-voting improves the generality of election procedures by providing an additional option of participation to the electoral process [11]. An issue arising is whether participation in the election through e-voting should be subject to the proof of special conditions, as is the case with postal voting. In most countries where postal voting has been established, only specific categories of individuals are allowed to exercise this option.

Adopting an e-vote capability as an exception to the rule (i.e. on the ground of the proof of a special condition, which prevents the eligible voter from physically casting her vote) is generally considered acceptable. On the other hand, the evolution towards the Information Society has a significant impact on the ability of a citizen to exercise her rights. In the light of the political decision to improve e-government and e-participation, the introduction of an e-voting capability should be viewed as an *isomorphism* of the traditional voting system.

Eligibility can be ensured through the registration of eligible voters and their identification at the moment of registration. Registration and authentication are procedures,

which are essential to ensure that the principle of universal suffrage is being respected and that elections cannot be rigged. The purpose of keeping a voters' register is to guarantee that only people eligible by law to vote can do so, and that no one can vote more than once.

Another issue is whether there is a need for registration in the case of e-voting. E-voting is, in some way, analogous to postal voting. Where an e-voting system is introduced, registration and authorization procedures are usually required. These procedures do not conflict with the principle of general elections for the following reasons: a) supposing that there is no national online voter register, a pre-registration for e-voting is necessary, to avoid vote fraud and support the integrity of elections. On the other hand, an Internet-based voter registration system could be vulnerable to large-scale fraud [12], and b) in case e-voting is an alternative to the traditional procedure, registration or declaration that the voter wishes to use the e-voting option should not lead to exclusion or discrimination. Moreover, it should be ensured that it is easy for e-voters to register, identify and authenticate themselves, because complicated procedures could be a burden to them [13].

3.2 Freedom

The principle of free election requires that the election process take place without any violence, coercion, pressure, manipulative interference, or any other influence, exercised either by the state or by one or more individuals. Regarding postal voting, the voter may be asked to sign a declaration on the vote-by-mail certificate, promising that she has filled out the ballot personally. Providing such a signature is not trivial in e-voting [14]. E-voting procedures pose new threats to the freedom and integrity of a voter decision, beyond those that postal voting does. For example, in the case of the workplace, even if the employer, the supervisor or a colleague are not standing over the shoulder of the e-voting employee, system administrators can monitor or record the activity at each workstation and obtain a copy of the ballot [15].

Uncoercibility and prevention of vote buying and extortion can be ensured by an e-voting system designed so that no voter can prove that she voted in a particular way (untraceability on the part of the voter) [16]. Since the employment relationship is not power-balanced, it is suggested to avoid e-voting from the workplace. In any case, coercion can hardly be prevented by technology alone. One solution to this is to develop a publicly accessible infrastructure, allowing voters to exercise their rights free of the coercion of any third party.

The **freedom of decision** may be violated if a propaganda message is blended on the computer screen while the voter is casting her electronic ballot. In current election schemes it is not allowed to advertise in (the vicinity of) the polling place. The e-voting procedure should also make the advertisement of political entities on the e-voting website technically infeasible.

The **free expression of the preferences** of the voter should be ensured [17]. Therefore, the possibility for casting a consciously invalid (or "white" paper) ballot should be ensured.

3.3 Equality

The requirement of equality, in the context of general elections, is a reflection of the generic principle of equality and constitutes one of the cornerstones of modern democracies. Under the principle of equal suffrage, two major requirements are identified: a) equality regarding the participating political parties and candidates and b) equality regarding the voting rights of each voter.

A requirement deriving from the principle of equality is that electronic ballots should be edited and displayed in a way analogous to that used for the paper ballots. Electoral equality requires that there are no meaningful deviation

between the printed ballot and its electronic equivalent look. Furthermore, the placement of electronic ballots in the voting site (i.e. on a computer screen) should ensure equal accessibility. Thus, the "look and feel" of the e-voting website and ballots should not favor or discriminate against any of the participating parties. Another element of equality among the participating parties is that the ballot of the voter is transmitted and counted without any changes or/and interferences. A valid cast vote must not be altered or removed in the course of the voting process.

Transparency should also be supported. All parties should have the opportunity for equal access to the elements of the voting procedure, in order to be able to establish its proper functioning.

The principle of equality requires that each vote, either physical or online, be equally weighted towards the election outcome. In an e-voting situation, certain voters have an access advantage to the enabling technology and, therefore, to e-voting capability. Some argue that remote voting could be used to manipulate election outcomes by managing the access in a way favoring those who are the most network-connected [18].

Because of the emerging characteristics of the technology, the right to *equal accessibility to the voting process* should become the right of *equal accessibility to election technology* [19]. As a result, a non-discriminating procedure should be offered to the voters, allowing them to efficiently exercise their voting rights with no obstructions. Equal accessibility means, also, that the system should be user-friendly and independent of a voter education, age, and physical condition (to accommodate physically disabled voters).

An e-voting system should ensure that the **one voter - one vote** principle is respected, that is only eligible voters can vote, only once, either online or off-line. Therefore, an e-voting system should be designed in such a way as to prevent the: a) Duplicability of the vote (either by the voter herself or by someone else), b) reusability of the vote (either by voting online more than once or by voting both online and offline), and c) modification of the cast vote (after a voter has dispatched her vote).

Another issue is the **duration of the e-voting period**. The California Internet Voting Task Force suggests that Internet voting does not continue throughout the election day, i.e. that there should be a time in advance of the election day, fixed by law, when e-voting is cut off. On the other hand, and in order to facilitate e-voting, others suggest that the voting period be extended for more that one day. This possibility may result in two suggestions: a) In most European Union member States the general elections take place on one day only, therefore the relevant legal provisions should be amended, and b) the principle of equality is put in question, especially if e-voters could make use of this possibility for more than one day.

3.4 Secrecy

Secrecy and freedom are strictly related principles. Secrecy is the condition of the voter free political decision. In democratic elections the link between the vote and the voter should be irreversible to ensure that votes are cast freely. In traditional voting systems secrecy is physically protected, but e-voting may make e-voting vulnerable to violations of secrecy. As a result of the above, the following requirements are derived: a) The secrecy of the vote should be guaranteed during casting, transfer, reception, collection and tabulation of votes, b) none of the actors involved in the voting process (organizers, election officials, trusted third parties, voters, etc.) should be able to link a vote with an identifiable voter, c) there should be a clear separation of registration and authentication procedures, on one hand, and casting-transfer of the vote, on the other, d) no

voter should be able to prove that she voted in a particular way.

The electoral provisions which are applicable to postal voting and to the protection of communication secrecy could also serve as a basis for solving the problem of political privacy. However, there can be no guarantee of freedom from external influence by third parties during the casting of votes. This is an inherent risk of any form of remote or e-voting. To face this risk, measures should be taken on the legal and regulatory level, in order to impose adequate measures against coercion and to sanction illicit behavior.

Secrecy has to be in harmony with the democratic principles for general elections. Ballot secrecy should be reconciled with transparency and auditability of the entire voting process. The election system should allow the verification of the authenticity of the ballot before the votes are viewed or counted. In order to protect secrecy, the voted ballots should be decrypted and counted only after the authentication information is reviewed and removed. The e-voting system should make vote control and recount technically feasible, while ensuring the non-identifiability of the voters [20, 21].

3.5 Directness

The principle of direct election requires that there can be no intermediaries in the process of voting decision. This principle may be also adapted to fit with an e-voting procedure. The relevant requirement is that each and every online ballot is directly recorded and counted.

A problem may arise in case the voting period differs from the voting procedure (on-line or off-line) used to cast the vote. Online voting results may influence the outcome of the entire election process and limit the integrity and legitimacy of the whole process. To avoid this, a system can be developed allowing the recording and maintaining of the cast vote, while prohibiting any counting before the end of the (off-line) voting period.

3.6 Democracy

A democratic e-voting system should at least meet the requirements of a traditional election system. However, additional requirements should be also met, particularly due to the remote nature of e-voting. These requirements pertain to the preservation of attributes and properties such as transparency, accountability, security, accuracy and legitimacy of the system. E-voters should be able to understand how the elections are conducted. The traditional voting procedures operate in a way that is transparent to both, the voters and the other election actors. On the contrary, e-voting procedures are not transparent because the average voter does not have the knowledge necessary to understand how the system works. Therefore, in e-voting much more *trust in the technology* used and the persons involved (election officials, technology providers, etc.) is be required by the voters.

Verifiability conflicts with transparency. An e-voting system should allow its verification by voters (individual verifiability) or by election officials, parties and independent observers (institutional verifiability). However, verifiability is orthogonal to secrecy (confidentiality), in the sense that individual verifiability (i.e. the possibility of a voter to verify his vote and receive confirmation about casting and counting of the vote) is conflicting with the requirement of secrecy (as a condition of free choice).

Accountability is an additional requirement of an e-voting system, which is meant as the logging and monitoring of all operations related to e-voting.

Reliability and security requirements are derived by the democratic need, to ensure that the outcome of the election reflects correctly the voter will. A reliable system should ensure that the outcome of the voting process

corresponds to the votes cast. The ballot that is transmitted to the voting counting equipment should be an accurate and not modifiable copy of the voter choice (integrity). Moreover, it should be infeasible both to exclude a valid vote from the tabulation and to validate a non-valid one.

Security is a multidimensional notion in the context of e-voting. Security refers mainly to the technically guaranteed respect of confidentiality (secrecy), integrity and availability, but it also refers to a whole range of functions and election components, such as registration, eligibility and authentication. The e-voting system should be protected against accidental or intentional denials of service and be available for use whenever it is expected to be operational. Unavailability of the system (or of one of its components) may result to loss of the capability of a voter to exercise her fundamental political rights.

E-voting systems are inevitably complicated. Furthermore, they usually involve more actors than a traditional system. From the point of view of the voters, the system should be easy to use and should require no particular skills. Therefore, an e-voting system should be developed in such a way as to facilitate its usability and to preserve its controllability.

Simplicity and **accessibility** of a system are not merely technical issues. Proper training and election processes re-engineering (e.g. help desks, e-election officials, etc.) are required to fulfill these requirements.

Based on the above principles, the following requirements are derived: a) there should exist trusted certification procedures for hardware and software, b) the entire infrastructure, as well as any system functionality, must be logged (e.g. all non -interface software should be open source), c) all operations (authentication, vote recording, etc.) should be monitored, while secrecy is preserved, d) the infrastructure should be open to inspection by authorized bodies, e) voters, parties and candidates should be ensured that there has been no malpractice, f) adequate system security must be ensured, g) the system must be simple and user-friendly.

4. Methodology used

In this section, the generic constitutional requirements (and the corresponding design principles) will be facilitated as a basis for eliciting the functional user requirements. This elicitation will be based on the Rational Unified Process [22, 23]. The Rational Unified Process is the synthesis of various software development processes; one of its most important characteristics is that it is use-case driven. Use cases were introduced as a requirements capturing method. Each use case refers to a system functional requirement [24, 25]. Non-functional requirements, which are specific to a use case, may become part of its description, whilst system-wide non-functional requirements are usually specified as supplementary specifications [26].

A fundamental activity of the requirements elicitation process is the development of the domain model demonstrating current actors and processes. Initially, a business use case model is developed demonstrating current processes (i.e. *what* the business does). Further analysis leads to the business object model revealing *how* business processes are performed. In that way, system designers study the problem at hand, while at the same time they learn how users perceive the system to be developed. In parallel, a mutual understanding of objections, suggestions and proposed solutions is achieved.

A generic voting model is described in the next section. We have merged some business use cases and the corresponding business object models, in order to keep its size acceptable without limiting its value. Subsequently functional requirements are identified. This is actually equivalent to finding and describing the use cases *the system* will perform.

Table 2: Constitutional election requirements and e-vote user requirements

Constitutional requirements	User requirements
Generality	
All adult citizens, unless other-wise stated by adjudication, have the right/obligation to vote	1. Participation in the voting process should be confirmed.
Freedom	
Everyone is free to vote for the party she considers appropriate	1. Uncoercibility should be ensured. 2. Ability for consciously non-valid vote should be provided for.
Equality	
All votes are considered equal.	1. Only eligible voters should be able to vote (eligibility).
	2. Each eligible voter should be able to vote only once (un-reusability)
	3. No voter should be able to duplicate/change her or someone else's vote (integrity).
	4. The voter should be able to verify that her vote is calculated in the final tally (verifiability).
	5. Voters should be bale to have indiscriminating access to the voting infrastructure (accessibility).
Secrecy	
No actor involved in the voting process should be able to link a ballot to a voter.	1. Registration, authentication and voting procedures should be evidently separated. 2. Votes should be validated separately and independently from voter authentication.
Directness	
An elector selects her repre-sentatives with no interference.	1. No intermediaries should be involved in the voting process (i.e. no person can be authorised to vote for another person).
	2. Each and every ballot should be recorded and counted correctly.

A typical high-level use case description consists of the following: a) *Use Case*: The name of the use case, b) *Description*: A high-level narrative description of the use case, c) *Purpose*: The goals, which the actors achieve with that use case, d) *Related Business Use Cases*: The use case from which a system use case has been derived, e) *Actors*: The actors participating in the use case (actor is the coherent role a customer of a use case plays when interacting with a use case), f) *Type:* Use cases are categorised as *primary* (major system functions), *secondary* (minor or rarely used system functions) or *optional* (functions that may not be implemented), g) *Preconditions*: The conditions that must be met, should the actor be able to perform the use case.

As use case descriptions tend to become more detailed, the underlying essential conditions become more clear, turning thus into non-functional requirements. A set of requirements for a secure e-voting system is presented in the sequel. System use cases tend to coincide with the business use cases identified in the domain model, because the current functionality is not altered by the introduction of an electronic system.

5. The traditional voting model

The voting process can be generally reviewed in the context of general elections. However, there are other situations where voting plays a central role (e.g. internal elections [e.g. trade unions

elections], decision-making [e.g. referenda], polls of indicative or advisory nature, etc.). These procedures are conducted in a way similar to general elections, although usually governed by different legal framework.

Nevertheless, one can argue that the general election process is a superset of the others, even though specific activities may be different. In this paper, a voting model focused specifically on the general elections process will be presented. The level of detail of this model is generic enough to be applicable in several contexts. Slight variations may exist among different contexts, mainly due to differences between the applicable legal framework. We argue that such variations do not affect either the completeness or the correctness of the model.

Despite the wide variety of electoral systems, legislative framework, and infrastructure, the constitutional requirements (design principles) lead to the user requirements that appear on Table 2. These requirements refer to corresponding business use cases and their realizations. Their interrelation comprises the business use case model for the general elections voting process. The voting model does not cope with the mechanisms employed for determining the candidates or the participating criteria for voters. It is considered that candidates have been appointed and that information about the entire population is available.

The business use cases included in the traditional voting model (Figure 1) include [27]:

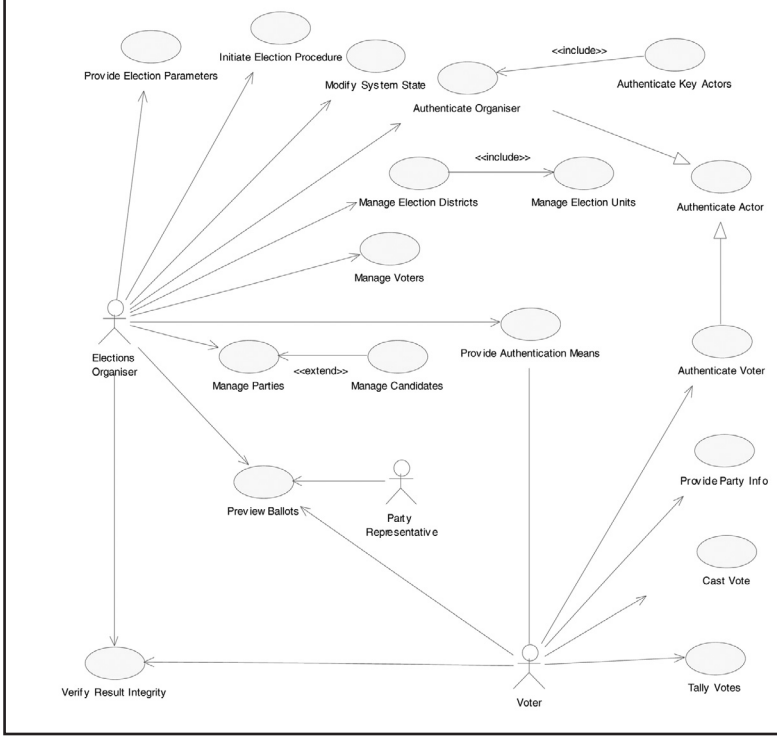
1. Define Election Districts: Performed before the start of the election process, in order to define the districts and the number of candidates to be represented in the governing body.

2. Determine Electors: Used to determine the participating electors. In general, all adult persons have the right/obligation to participate in this process.

3. Provide Authentication Means: Performed to provide the electors with adequate

Figure 1: Use cases for a general elections voting model.

Figure 2: Business use cases of an e-voting system



authentication means, and to allow them to identify themselves during the voting process. The responsibility for the provision of authentication means can be either with the state or the elector. The process ends after voters have acquired the required authentication means in a non-discriminative way.

4. Set-up Election Centres: Performed after elections districts have been defined and before the voting time period. Its goal is to provide the infrastructure, which allows for the election process. During this process the authorized election centre staff, along with individuals authorised to supervise the election process for each election centre, is identified.

5. Create Ballots: Starts after elections districts have been defined. Each party provides a discrete ballot format and a list of representatives per election district. The state creates the ballots and sends them to all election centres.

6. Authenticate Elector: Performed when the elector appears to vote in the election centre she is registered to. Its aim is to ensure that the elector votes herself.

7. Cast Vote: After a voter is authenticated, she casts her vote in a way protecting secrecy. Then, the election records are properly updated.

8. Tally Votes: Performed to validate votes and to determine the number of votes each party has got. The process takes place in every election centre after the end of the election period and ends when all votes have been validated and tallied by the officials.

9. Consolidate Votes: Aims to consolidate tallied votes (along with the list of persons that have voted in the election centre) from election centres to a central repository. The process starts independently for each election centre after the tallying has finished.

10. Verify Result Integrity: Takes place in case an interested entity wishes to verify that the election procedures have been conducted properly. In this case, officials using the records kept during the corresponding procedure should demonstrate that fact.

6. E-voting user and functional security-focused requirements

The general election model described in the previous section provides the essential basis for an e-voting system requirements elicitation. In line with the business use cases of the general elections model, a number of system use cases have been identified. The business use cases, regarding a general e-voting model appear in Figure 2. A detailed description of all e-voting business use cases is described in the sequel, followed by the corresponding user and functional requirements, in particular those which aim at the security of the voting system.

[1]. Authenticate Actor:
Provides access to the system functions the actor is authorised to perform.

Related BUC	6
Actors	All
Type	Primary
Preconditions	None

User Requirements: a) *Voters*: The voters should be allowed a limited number of unsuccessful authentication attempts. In case that the limit is exceeded, their authentication means should be invalidated; in order to have the chance to re-participate in the voting process, a new authentication means should be issued and assigned to the voter. During the authentication process, the voters should not have direct access to the voting host system. The authentication process should lead to limited and controlled access to the voting system under the lower privileges possible, or no

access at all. Successful authentication should grant access to the voting system solely through the user interface. b) *Key actors*: Users should be authenticated only from specific terminals, within a redefined time window, using a combination of advanced authentication means, such as biometrics or/and smart cards. Key actors should not be privileged users at system level. Timeout between unsuccessful attempts should increase after every failure. A maximum number of attempts should be allowed (after that, special authorization should be given by authorized election officers in order to unlock the terminal). The system should be able to incorporate alternative authentication methods and means of equal strength as technology in the field advances. The system should provide a hook for an open API to easily incorporate new authentication means. c) *For all users*: The authentication data should be transmitted in a secure and reliable way even under Public Networks. Widely adopted security guidelines should be employed for user authentication. The authentication process must be treated as an atomic transaction. Abnormal interaction or unexpected input data to the authentication process should be treated properly. No application or system-specific information should be revealed during the authentication process, in case of abnormal application termination or during infrastructure failure. All authentication attempts, successful or not, should be logged.

Functional Requirements: Expose a well-defined authentication API (the system should be able to incorporate alternative authentication methods and means as technology advances). Validate actor credentials (in case of voter authentication an underlying trust-enhancing infrastructure should be in place, to successfully validate actor credentials). Log all authentication attempts, successful or not. Assigned privileges in actors are valid only at the voting system application level (the voting system should grant to authenticated actors only appli-cation-wide privileges, while system privileges should be disallowed for all actors).

---

[2]. Manage Election Districts:
Creates, views, and modifies different sets of election districts for one or more election procedures.

Related BUC	1
Actors	Election organizer
Type	Secondary
Preconditions	The actor is officially authorized to perform changes in selection districts. The actor has successfully completed the authentication procedure. The system is at the "election set-up" stage.

User Requirements: Abnormal interaction or unexpected input data to the district management process should be treated properly.

Functional Requirements: Verify input data (input provided by actors must be relevant and meaningful to the system). The system should log all actions.

---

[3]. Manage Election Units:
Creates, views and modifies election units for one or more election procedures.

Related BUC	1, 4
Actors	Election organizer
Type	Primary
Preconditions	The actor is officially authorised to modify election units of an election district. The actor has successfully completed the authentication

	procedure. The election district for which the election units will be modified, exist in the system. The system is at the "election set-up" stage.

User Requirements: Abnormal interaction or unexpected input data to the unit management process should be treated properly.

Functional Requirements: Verify input data (input provided by actors must be relevant and meaningful to the system). Logging (the system should log all actions).

[4]. Manage Voters:
Imports, inserts, views, and modifies voters for one or more election procedures.

Related BUC	2
Actors	Election organizer
Type	Primary
Preconditions	The actor is officially authorised to perform changes in the eligible voters list. The actor has successfully completed the authentication procedure. The election district where voters will belong has been specified in the system.

User Requirements: The system should be able to import an electronic list of voters from different sources and formats. The voter lists should be complete, correct, up-to-date, and should not be transmitted to the system, but delivered through secure physical means. The system should deal successfully with malformed interaction and/or unexpected input. The system should log all actions. Voters should be assigned to correct districts and/or election units. No voter should be assigned to more than one district and/or election unit.

Functional Requirements: The system should be in the Election Set-up phase in order to perform this operation; in order to perform this operation in the Election in Progress phase the appropriate use case must be activated. Require key actor authentication in voting phase (the appropriate procedure should be activated if the actor wishes to set/modify voters in a system phase other than the pre-election one). Import voters' list (the system should be able to import an electronic list of voters from different sources and formats. The voters' lists should be complete, correct and up-to-date. The list of voters should not be transmitted to the system, but delivered through secure physical means). Check voters list (the system should deal successfully with malformed interaction and/or unexpected input). Check input data (the system should deal successfully with malformed interaction and/or unexpected input). Store voters' list in a secure way (the list should be stored in a secure server other than the machine running the voting system). The system should log all actions.

[5]. Provide Authentication Means:
Provides voters and party representatives with authentication means.

Related BUC	3, 6
Actors	All
Type	Primary
Preconditions	The actor(s) exist(s) in the system.

User Requirements: Authentication means must be created, stored and communicated to voters/ party representatives in a secure way.

Functional Requirements: Provide an open API to easily incorporate new authentication

means (To allow the system to cope with advancements in authentication technology). Log all attempts to generate authentication means, successful or not.

[6]. Manage Parties:
Notifies the system about candidate parties for an election.

Related BUC	-
Actors	Election organizers
Type	Primary
Preconditions	The actor is officially authorised to perform changes in the candidate parties' list. The actor has successfully completed the authentication procedure.

User Requirements: The system should be able to import an electronic list of parties from different sources and formats. The list of parties should be complete, correct and up-to-date. The list should not be transmitted to the system, but delivered through secure physical means. The system should deal successfully with malformed interaction and/or unexpected input. The system should log all actions.

Functional Requirements: Verify input data (input provided by actors must be relevant and meaningful to the system). The system should log all actions.

[7]. Manage Candidates:
Inserts, modifies or deletes a party's candidates for a specific election district.

Related BUC	-
Actors	Election organizers
Type	Primary
Preconditions	The candidate's party exists in the system. The actor is officially authorised to perform changes in the candidate list.

User Requirements: The system should be able to import an electronic list of candidates from different sources and formats. The list of candidates should be complete, correct, up-to-date and every candidate should be linked to a specific party. The list should not be transmitted to the system, but delivered through secure physical means. The system should deal successfully with malformed interaction and/or unexpected input. The system should log all actions.

Functional Requirements: Alter candidate list in voting phase (the appropriate procedure should be activated in case the actor wishes to set/modify election candidates in a system phase other than the pre-election one). Import Candidates List (the system should be able to import an electronic list of candidates from different sources and formats. The candidates' list should be complete, correct and up-to-date. The list of candidates should not be transmitted to the system, but delivered through secure physical means). Validate candidates' data (the system should deal successfully with malformed interaction and/or unexpected input). The candidates' list should be stored in a secure server different than the machine running the voting system). The system should log all actions.

[8]. Preview Ballots:
Checks the content and format of the ballots that will be used in the election Related BUC 5

Actors	Election organizer, Party representative, Others
Type	Primary
Preconditions	The ballot logo for the parties and all candidates have been inserted in the system

References

1. Internet Policy Institute, *Report of the National Workshop on Internet Voting: Issues and Research Agenda*, March 2001 (http://www.internetpolicy.org/research/e_voting_report.pdf).
2. The Swedish Government, *Internet Voting - Final Report from the Election Technique Commission*, 2000 (http://www.justitie.regeringen.se/propositionermm/sou/pdf/sou2000_125.pdf).
3. Cramer R., Franklin M., Schoenmakers B., Yung M., "Multi-authority secret ballot elections with linear work", *Lecture Notes in Computer Science*, Vol. 1070, pp. 72-83, Springer-Verlag, Berlin, 1996.
4. Schoenmakers B., "A simple publicly verifiable secret sharing scheme and its application to electronic voting", in *Lecture Notes in Computer Science*, Vol. 1666, pp. 148-164, Springer-Verlag, 1999.
5. Buttler R., et al., "A national-scale authentication infrastructure", *Computer*, Vol. 33, no. 2, pp. 60-65, February 2000.
6. Hoffman L., Cranor L., "Internet voting for public officials", in *Com. of the ACM*, Vol. 44, no. 1, pp. 69-71, January 2001.
7. Jones B., *A report on the feasibility of Internet voting*, Internet Voting Task Force, State of California, January 2000.
8. CyberVote (IST-1999-20338 project), *Report on electronic democracy projects, legal issues of Internet voting and users requirements analysis*, European Commission, IST Programme, 1999 (http://www.eucybervote.org).
9. United Sates, State of California, *A Report on the Feasibility of Internet Voting*, January 2000 (http://www.ss.ca.gov/executive/ivote/)
10. European Commission, IST 2000 Programme, *The Information Society for all*, Final Report, Brussels 2000.
11. Tauss J., Kollbeck J., e-vote: *Die elektronische Briefwahl als ein Beitrag zur Verbesserung der Partizipationsmöglichkeiten* (www.tauss.de/bn/e-vote.html).
12. Internet Policy Institute, *Report of the National Workshop on Internet Voting: Issues and Research Agenda*, March 2001.

User Requirements: Only information relevant to the voting process should appear on the ballot.

Functional Requirements: Display ballot (the system should deal successfully with malformed interaction and/or unexpected input, should expose the minimum possible information, in order to facilitate the voting process; no system/application specific information should be disclosed through the ballot). The system should log all actions.

---

[9]. Provide Party Information:
Provides information about candidate parties.

Related BUC	-
Actors	All
Type	Optional
Preconditions	-

User Requirements: Only publicly available data regarding the party should be provided.

Functional Requirements: The system should log all actions.

---

[10]. Cast Vote:
Facilitates electronic voting.

Related BUC	6, 7
Actors	Voter
Type	Primary
Preconditions	The voter has been authorised to cast his vote.

User Requirements: No vote can be linked to a voter. No voter can vote twice. No one can duplicate or change her or someone else's vote. No one can disclose what others have voted. Voter casts vote alone with no pressure (uncoercibility). An undeniable proof (receipt) has to be delivered to the voter in order to prove that she has cast a vote. No one can achieve non-repudiation of vote casting. The voting system should be transparent to the voter, in such a way that he can virtually vote from everywhere. Logging of all actions should take place.

Functional Requirements: No ballot can be linked to a voter, no voter can vote twice, no one can duplicate someone else's vote, nor cast a modification of somebody else's vote, no one can see what others have voted, no one can vote on behalf of someone else, nor change what someone else votes, voter has the ability to cast an invalid ballot, voter has the ability to cast a blank ballot). Deliver proof of voting (it should not be possible to associate the proof to the choice of the voter). Store vote in a secure way (the voting system stores the vote cast in a different machine than the one that is running the voting system). The system should log all actions.

---

[11]. Tally Votes:
Calculates the election result.

Related BUC	8, 9
Actors	Election organizers
Type	Primary
Preconditions	The election procedure has ended

User Requirements: It must be impossible to tally the votes before the voting process officially ends. Votes and relevant evidence should be stored in a secure way. Logging of all actions takes place.

Functional Requirements: Check election phase (the system should be able to identify the current election phase and should be in the election Concluded phase in order to

perform this operation). Prohibit tallying before election end time (it must be impossible to tally the votes before the voting process officially ends). Isolate the voting system (after the election has finished, the voting system must be isolated from any external or/and public network (if applicable). Prohibit election information provision before tallying end time (it must not be possible to provide election information before the tallying process ends). The system should log all actions.

---

[12]. Verify Result Integrity:
Verifies that system use cases have performed the required actions as expected and in a timely manner.

Related BUC	10
Actors	Election organizers
Type	Primary
Preconditions	-

User Requirements: It must be impossible to verify the election results before tallying process officially ends. Verification of the integrity of the voting result should be ensured by the participation and active involvement of interested parties' representatives during the verification process. Verification evidence and results should be stored in a secure way. Logging of all actions takes place.

Functional Requirements: Provide reasonable assurance for the election result integrity. Verify Vote Calculation (the system should be able to demonstrate that all votes have been tallied correctly). The system should log all actions.

---

[13]. Modify system state (States: 1. Election set-up; 2. Election in-progress; 3. Election concluded):
Performs the system transition from one state to another

Related BUC	1
Actors	Election organizers, Party representatives (optionally)
Type	Primary
Preconditions	The actor is authorised to change the state of the system. The actor has successfully completed the "authenticate key actors" procedure. Transition from state 2 to 3 is automatic and based on the election end-time specified during the election set-up.

User Requirements: The election parameters should be stored in a secure way. The updated election parameters should be distributed to all interested entities and parties for clarity.

Functional Requirements: Display confirmation dialog (this dialog, along with extra information about confirmations performed so far, will be displayed to the rest of key authors participating in the use case). The system should log all actions

---

[14]. Provide election parameters:
Specifies various parameters for the election that is going to take place

Related BUC	1
Actors	Election organizers
Type	Primary
Preconditions	The actor is authorised to set parameters for the election to the system and has successfully completed the authentication procedure. The system is at the "election set-up" stage.

---

13. California Institute of Technology - MIT, *Voting: What is, what could be*, Voting Technology Project, July 2001.
14. e-VOTE (IST-2000-29518 project), *Legal and regulatory issues on e-voting and data protection in Europe*, Deliverable D3.4, European Commission, IST Programme, January 2002.
15. Kim A., *"Ten things I want people to know about voting technology"*, Democracy Online Project's National Task Force, California Voter Foundation, January 2001.
16. Adler J., *Internet Voting Primer* (www.votehere.net/adacompliant/whitepapers/primer).
17. Rüß O., *Wahlen im Internet, quelle multimedia und recht* (http://www.Internetwahlen.de/project/ruess.html).
18. Phillips D., von Spakovsky H., "Gauging the risks of Internet elections", in *Com. of the ACM*, Vol. 44, no. 1, pp. 73-85, January 2001.
19. Burkert H., *"Elektronische Demokratie: Einige staats und verfassungsrechtliche Anmerkungen"* (http://www.gmd.de/People/Herbert.Burkert/ARCHIV).
20. International Working Group for Data Protection in Telecommunications, *Common Position on the Use of the Internet in the Conduct of Elections*, Berlin, September 2001.
21. Schoenmakers B., *Compensating for a lack of transparency.* (http://citeseer.nj.nec.com/schoenmakers 00compensating.html).
22. Jacobson I., Booch G., Rumbaugh J., *The Unified Software Development Process*, Addison-Wesley, 1999.
23. Rational Corporation, *The Rational Unified Process.* (http://www.rational.com/products/rup/index.jsp)
24. Jacobson I., *Object-oriented software engineering - a use case driven approach*, Addison-Wesley, 1993.
25. Simons A., Graham I., *37 things that don't work in object-oriented modelling with UML*, Technical Report TUM-I9813, Technical University of Munich, 1998.
26. Larman G., Applying UML and patterns, Prentice-Hall, 1998.

27. Ikonomopoulos S., Gritzalis D., Lambrinoudakis C., Kokolakis S., Vassiliou C., "Functional requirements for a secure electronic voting system", in *Proc. of the 17th IFIP International Information Security Conference*, M. Hadidi, et al. (Eds.), pp. 507-520, Kluwer Academics, May 2002.
28. Mitrou L., Gritzalis D., Katsikas S., "Revisiting legal and regulatory requirements for secure e-voting", in *Proc. of the 17th IFIP International Information Security Conference*, M. Hadidi, et al. (Eds.), pp. 469-480, Kluwer Academics, May 2002.
29. Mercuri R., "Voting automation?", in *Com. of the ACM*, Vol. 43, no. 2, pp. 176, February 2000.

User Requirements: The election parameters should be stored in a secure way. The election parameters should be distributed to all interested entities and parties for transparency.

Functional Requirements: Check system phase and notify actor (in order to set/modify election parameters, the system should be in the pre-election phase). Define the alterable election parameters in the voting phase. Check election parameter data (the system should deal successfully with malformed interaction and/or unexpected input). Store the election parameters in a secure way (the parameters should be stored in a secure server, different than the machine running the voting system). Require key actor authentication in voting phase (the procedure should be activated in case the actor wishes to set/modify election parameters in a system phase other than the pre-election one). The system should log all actions

Typical election parameters include an output distribution list, party or other interested parties representatives, election start/end dates, election start/end times, maximum number of parties, maximum number of voters, maximum number of voter choices, exact number of voter choices, ballot format, invalid ballot requirements, maximum number of unsuccessful/ uncompleted vote attempts without re-authentication, etc.

7. E-voting non-functional security requirements

In addition to the user and functional requirements expressed through the system use cases, the system will exhibit a number of non-functional requirements. Non-functional requirements can either be specific to a use case or they may pertain to the system as a whole. These requirements have been grouped into the following categories:

Security: Aim to support the main security properties, both in application and system level; they also provide for non-repudiation, anonymity and source verification.

Performance: Deal with speed, efficiency, availability, accuracy, throughput, response time, recovery time, or resource usage, etc.

Reliability: Include attributes as frequency/severity of failure, recoverability, predictability, accuracy and mean time between failures (MTBF), etc.

Usability: Deal with consistency in the user interface, online and context-sensitive help, quality of user documentation, training materials, etc.

Supportability: Requirements related to system maintenance, adaptation, installation, etc.

In this paper, we will refer only to those non-functional requirements, which deal with security. These requirements are described on Table 3, where every security focused requirement is first associated with its aim and then briefly described.

8. Suggested use of an e-voting system

We argue that e-voting systems should be viewed, for the time being, only as a supplement to - and not a replacement of - the existing paper-based voting systems. We base our suggestion mainly on the following:

1. The *digital divide*, i.e. the lack of equal access opportunity to the Internet and to the ICT infrastructure means. Offering new means and possibilities of participation, based on ICT, could in such a case lead to the opposite effect, namely the exclusion of "ICT illiterate" voters from the political process. An election system itself may structure unequal access of an individual to the electoral process. It is a matter of democracy, equality, and equity to guarantee that the different voting technologies are equivalent with respect to ease and opportunity of access.

Table 3: Non-functional security requirements

Aim	Attribute details and constraints
Abnormal action	The system should treat properly abnormal interaction or unexpected input data in all system functions in a way such that the system functionality is preserved and no sys-tem/application specific information is disclosed.
Accountability	All voting system-related actions, successful or not, should be logged. Only the ab-so-lu-tely necessary entities should have logical and/or physical access to the voting system. Adequate segregation of duties must be enforced between the authorised personnel.
Physical control	Application of physical security measures such as door locks, guards, physical site planning, etc.
Assets	Data assets must be protected from unauthorised disclosure, unauthorised modification and fabrication and denial of authorised access. All hardware assets must be protected from becoming lost, stolen, unavailable, or unusable. All software assets must be rea-son-ably protected from becoming deleted, lost, stolen, modified, or fabricated. In-dividuals responsible for vital system operations must be carefully selected.
Audit logs	All internal system operations related to voters must be logged without sacrificing voter's confidentiality. Detailed application and system logs should be kept in a process call level.
Availability	The availability of the voting system while the election is in progress must be ensured. Alternative general support (e.g. back end facilities) and election sites should be avail-able in case of failure, caused by deliberate, or accidental actions. The MTBF should be minimum during the election process. Updated voting system backups should be readily available in order to restore the system in case of a disaster.
Communications	Information regarding any of the above functions should be private even if transmitted over public networks
Data protection	Information processing should be compliant with national and international data pro-tection legislation framework. Adequate controls should be in place to ensure with reasonable assurance that data protection principles are enforced in an effective and efficient way.
Encryption	The system should be able to use all necessary cryptographic services. Sensitive data and information exchanged between computers of the voting system must be in an encrypted form.
Integrity	Users should administer the system only from specific terminals, within a predefined time window, using a combination of strong authentication means, such as biometrics or smart cards. The minimum necessary software and hardware components should be installed on the host of the voting system. The maximum possible level of operating system security enhancement should be applied to all machines of the voting system. It should be impossible for a user to escalate his/her system privileges. It should be allow-ed, under certain emergency circumstances, to modify selected parts of the system when in use. Breaches to the security of the client should not have an impact to the security of the system.
Storage media	All data and information used must be stored (when and if needed) in secure (protected and tamper-proof) storage media.
Uncoercibility	Voters should cast their votes alone, under no pressure.

2. The *inherent distrust* in an e-voting procedure, which is due to the lack of transparency - in the context of visibility - of the election process. Some of the basic elements and requirements of the traditional voting procedure and participation are different in an e-voting setting. The level of trust and public support for e-voting should be measured in relation to all potential voters, not just to those who are likely to utilize this form of voting. We argue that if Internet voting is viewed skeptically by a large number of voters, then the fundamental trust in the democratic process may be compromised (for example, the California Internet Voting Task Force recommended that any use of the Internet for voting purposes should be phased in gradually, in order to ensure that election officials and members of the public are confident with the technology).

3. *Security risks and protection mechanism inadequacy*. These constitute another argument for the supplementary character of e-voting systems. The risks to the security of the e-voting

process appear not to be adequately dealt with by the existing technologies.

As a result, it is considered that, until all relevant technical, legal, and social issues and concerns are adequately addressed by modern information societies, e-voting could not be fielded for use in public elections, and therefore not be imposed as obligatory.

9. Conclusions

Information and Communication Technologies are powerful instruments in the hands of politicians and legislators, who have the duty to actively promote the democratic process and encourage citizen participation. Technology could help overcome the crisis of confidence, that representative democracy is experiencing nowadays. The right to vote is a part of the democratic process, which remains deeply embedded in the modern constitutions. Moreover, it is considered to be one of the primary foundations of democracy. Electronic voting, in contrast with other electronic transactions, will be only acceptable if it guarantees the fulfillment of all relevant constitutional principles. Furthermore, an e-voting system should be implemented in a context ensuring equal access to the underlying technological infrastructure, which should be open, user-friendly, interactive and secure, in order to enable citizens to participate in political life and have a direct impact on it [28, 29].

In this paper we have identified the generic design principles of an internet-based e-voting system, which stem from the relevant constitutional requirements. In addition, we have produced the set of functional requirements for e-voting systems, which integrates the requirements imposed by the existing (traditional) general election systems. To do so, a software engineering method (i.e. the Rational Unified Process) was used, which is based on the facilitation of use cases. As a result, an e-voting system has been conceptualised in its entity, in a way that confines the number of possible subsequent designs, yet does not dictate a particular one. This set of requirements is the outcome of the first iteration of the requirements elicitation process. We are currently in the process of validating and enhancing this set, including non-functional requirements, expecting to incorporate it into an e-voting system development phase.

Prophets and proponents of e-voting have not, as yet, the power of the technology-driven market on their side, although there is a significant shift from PC-computing to Internet-computing. It appears that certain requirements posed by legislation (e.g. uncoercibility) are really difficult, if at all possible, to be met with by the existing technology. In the current socio-technical context, the ultimate result of our work is that - for the time being - electronic voting systems should be considered as a complementary means to the traditional general election systems, under the condition that all essential legal and technical requirements are adequately met. Therefore, the traditional voting system is expected to remain the principal means for conducting a general election process, whereas the complementary e-voting capacity will be introduced only gradually.