A proposal for an e-voting system and its legal consequences

STAVROS VALSAMIDIS
KALLIOPI KALAMPOUKA
SOTIRIOS KONTOGIANNIS
THEODOSIOS THEODOSIOU

Department of Accountancy
Kavala Institute of Technology
Agios Lucas
GREECE

pkalab@teikav.edu.gr
youremailaccount@xxx.xxx.xx    http://www.yourwebaddress.xx
svalsam@teikav.edu.gr,  pkalab@teikav.edu.gr, skontog@ee.duth.gr,
theodosios.theodosiou@gmail.com
http://ad2.teikav.edu.gr/ad_en/

Abstract: - In this paper we present a framework for conducting electronic elections over the web taking into consideration the legal consequences. The proposed system has to be based on open source software with its own security protocol. It will be an alternative and practical solution to existing e-voting systems applications not only for communities, universities and organizations but for national and communities elections as well.

Key-Words: - E-voting, Electronic Election Systems, Requirements, Types, Legal Aspects, Technical Aspects

1 Introduction

E-democracy is a term produced from the words "Electronic" and "democracy," and comprises the use of electronic communications technologies such as the Internet in order to enhance democratic processes and provide increased opportunities for individuals and communities to interact with government and for the government to seek input from the community [37]. E-democracy is at the convergence of traditional democratic processes and Internet technology [34]. E-democracy can also be deemed as the use of electronic communications technologies, in the policy-making process and the government-citizen relations in order to encourage a direct and more active citizen participation in public life and the decision-making process. E-democracy is also sometimes referred to as cyberdemocracy [59], teledemocracy [2] or digital democracy.

E-voting is a term produced from the words "Electronic" and "voting" and encompasses several different types of voting, embraces both electronic means of casting a vote and electronic means of counting votes [41]. Electronic voting is the option of using electronic means to vote in referendums and elections, including polling place e-voting and remote e-voting. Remote e-voting options include voting over the Internet and the use of personal digital assistants (PDAs) or telephones or mobile phones to cast a vote electronically. Electronic voting technology can include punch cards, optical scan voting systems and specialized voting kiosks. It can also involve transmission of ballots and votes via telephones, private computer networks or the Internet.

E-democracy includes within its scope electronic voting, but has a much wider span than this single aspect of the democratic process. Other premier web applications that offer a means of electronic democracy are: electronic elections, electronic debates, electronic pre-election gatherings, public speeches, electronic parliament, electronic government and others. Electronic elections are nowadays one of the most popular issues of e-democracy. This has led to the development of applications. The problem that arises is that such applications are created either on demand for a specific election process, or experimentally for scientific purposes.

Modern Electronic Voting Systems (EVSs) can be divided into two major categories: DRE (Direct
Recording Electronic) voting systems and Internet voting systems. DRE systems utilize touch screens, keyboards, NFC and smart card equipment for voter authentication and voting purposes. The voting process takes place in voting terminals, located at specific polling areas which are directly connected, or not, to a central station [13]. The votes are immediately added to a running tally stored at the remote central station, if this station exists, or, if not, in the DRE’s storage system (hard disk, memory card). Mail voting systems also belong to this category. DRE systems have two distinct characteristics: (1) DRE systems combine hardware and software to one embedded device, keeping the implementation hidden for both hardware and software and (2) utilize physical security in terms of specific voting areas (polling stations) in order to assure EVS system authentication and security requirements.

One of the first DRE EVSs used is SENSUS DRE, created by Lorrie Faith Cranor at St. Louis University, Washington in 1995 [12]. It uses blind signatures to assure that voters will vote only once. Its initial purpose was to replace voting by mail. Today it is considered quite old and it has been abandoned. The company TrueBallot, Inc has presented the DRE system [58], which is used by companies, organisations, universities, associations and by teams of users for the conduct of electronic elections. The Trueballot system offers 3 basic operations: ScanVOTE / TouchVOTE Ballot-On-Demand which imitates physical voting, WebVOTE which uses Internet and TeleVOTE which uses the telephone as a means of conducting the voting.

The DRE Diebold AccuVote-TS system [13], used in US elections, constitutes an embedded device with both hardware and software so that a user by using a touch screen with a card reader may authenticate and vote, after being authenticated by polling officials (votes are cast at specific poll sites) [4]. The SureVote company [56], provides a similar system, in which the users authenticate themselves and their right to vote using a numeric personal identification code and a numeric ballot code [4]. It also offers a web-based Internet EVS system.

Internet EVS systems, on the other hand, use a computer or digital television or a mobile phone (by any hardware means) with custom software provided by a central voting station or stations over the Internet (using Internet software technologies), for voting purposes. Elections are held everywhere using remote Internet voting, thus increasing EVS system’s availability usability and scalability. This, of course, may be contentious because it is difficult to verify that the voter is who they claim to be. Both anonymity and privacy may easily be compromised. This opens the door to voter coercion and vote buying. Such drawbacks lead to the implementation of more strict security mechanisms on Internet EVSs. Such systems are presented in the next paragraph.

Safevote is a software company which offers a variety of products supporting both public and private elections using Internet voting [51]. The Rijnland Internet Election System (RIES) is a system designed for voting in public elections over the Internet [22]. Moreover, browser based Agile E-Voting system is another effort to provide a practical, voter-friendly e-voting system [55]. The Global Election Company provides election.com [20], which is global election software. It offers poll site voting and remote electronic voting. Finally, GNU FREE (Free Referenda and Elections Electronically) [21] is an Internet based system which started being developed in 1999 as a free electronic voting EVS system. Its implementation is database and platform independent. Today this project has been abandoned.

Various publications have addressed the benefits and risks of e-voting systems [41, 44, 1]. Electronic forms of voting have been implemented at some scale in many different countries, though in very different ways [46, 48]. The first electronic election scheme was proposed by [8] who is the inventor of eCash. He describes a unique method where voters can positively confirm their ballots, both at the polling station and also after the election; to be sure they are correctly entered into the tallies, without revealing their choices. This groundbreaking work may eventually form the basis of secure and auditable future elections [10]. Mercuri has been investigating a wide range of electronic voting issues and addresses usability issues [38].

A paper which thoroughly surveys issues relating to usability of electronic voting systems and reports on a series of studies was written by [4]. It was an early indication of machine failures with the Diebold equipment. Another interesting paper, which details the requirements, design and implementation of a special type of electronic voting system, the remote on-line voting system, suitable for a university setting where students can cast their votes anytime, anywhere, using either fixed or mobile electronic devices including personal computers, personal digital assistants and smart and regular phones, is proposed by [47]. The usability issues in various election systems, with the conclusion that newer technologies are not necessarily an improvement for voters is proposed by [49]. The use of distance electronic voting
systems, in the support of non political elections, has been researched in many studies [16, 57]. An overview of voting security threats and vulnerabilities along with an assessment of strengths and weaknesses of potential solutions is presented by Fischer [18].

The paper is organized as follows. Section 2 describes the problem formulation with the requirements of an e-voting system, the existing EVS (Electronic Voting System) technologies along with their corresponding applications and the legal aspects. Section 3 presents the problem solution in terms of technical design and legal consequences. Finally, section 4 deals with the discussion related to advantages and disadvantages of such a system. In section 5 useful conclusions are drawn after the presentation of the proposed system.

2 Problem Formulation

In this section the legal issues, the requirements and the types of EVS systems are described in detail.

2.1 Legal Issues

According to Article 51 para 3-5 of Greek Constitution "3. The deputies are elected by direct universal suffrage and secret ballot by citizens who have the right, as provided by law. The law can not restrict the right to vote unless there has completed a minimum age or legal incapacity or as a result of irrevocable criminal conviction for certain crimes. 4. The parliamentary elections held simultaneously throughout the Territory. As for the voters, the principle of simultaneous elections shall not prevent the exercise of their right to vote by postal vote or other appropriate means, provided that counting and announcement of results is carried out whenever possible and throughout the State. 5. The voting is compulsory.".

This provision establishes the following basic, essential and fundamental principles of: (a) Universality, is deliberate on the part of the State minimization of the skills required in order for a person to participate as a voter in elections. (b) Immediacy is the non-interference will or intermediate body between the expression of the choice of the voter and the enactment of the electoral outcome. (c) Secrecy is to ensure non-disclosure of the content of the vote in another person outside of the voting [30].

Simultaneity means that the expression of individual electoral preference expressed without the possibility of knowledge of other results in the same election.

2.2 EVS Requirements

Electronic Voting Systems requirements fulfil generic functionalities and attributes of an electronic voting system [3, 32, 50, 11]. System requirements define electronic voting system functionality. These capabilities apply to three different phases of the voting process: Before the voting process occurs, during the voting process and after the voting process completion for a voter x [19, 40]. The pre-voting process requirements of an electronic voting system are the following:

Authenticity: This means that only selected voters may vote and the electronic voting system must provide proof with the use of appropriate authentication mechanisms that a selected voter is the one that cast the vote [23].

Freedom: The electronic voting system must provide the ability to all selected voters to vote for whatever candidate they wish, or none for an election process [23].

Eligibility: Only eligible voters are permitted to vote [12, 15, 17, 23, 26].

Practicability: No extra skills are required to vote and no additional equipment is required [12, 26, 33, 35].

During election processes, an electronic voting system must maintain a high standard of the following capabilities:

Robustness: The electronic voting system must provide all the necessary mechanisms to prevent interruption of the election process or system’s denial of service. A malicious voter cannot frustrate or disturb the election [17, 9, 27].

Security: During an election process the electronic voting system must maintain vote integrity, voter anonymity when casting the vote and encrypt the vote in order to prevent eavesdropping [52, 53].

Uniqueness: The electronic voting system must provide appropriate mechanisms that ensure that voters are uniquely identified for an election process and vote only once [12, 15, 17, 23, 26, 33, 35, 36].

Verifiability: The electronic voting system must provide the voter a proof receipt that his/her vote drop at the tally was acknowledged. This receipt may be used after the voting process by the voter to confirm that his/her vote was accounted by the election committee [7].

Fairness: The electronic voting system must not provide any information about the outcome of an election process during the election process. No one can learn the voting outcome before the tally [17].

Democracy: All votes are equal and have the same weight. The principle: “One voter- one vote”
must be sustained by the electronic voting system during an election process [40].

After an election process, there are also electronic voting system requirements that must be fulfilled:

*Privacy (anonymity):* When the votes are verified by the election committee, the electronic voting system must provide anonymity mechanisms so that the voter cannot be traced back by his/her vote. There is no way to derive a link between the voter’s identity and the marked ballot. The voter remains anonymous [9, 12,15,17,23,26,33,36].

*Accuracy:* All valid votes are counted correctly. The electronic voting system must count all votes and must count them as cast. A voter’s vote cannot be altered, duplicated, or removed. Of course in a real electronic voting system appropriate error thresholds must be set that will indicate the validity of an election process [53,9,12,15,17,27,26,33,36].

*Integrity:* The electronic voting system sustains the vote integrity [53].

*Uncoercibility:* The electronic voting system may use appropriate mechanisms to prevent a user proving how he/she voted [5,12,23,25,43]. There are also system-specific requirements that must also be taken into consideration for the design of an electronic voting system. Such requirements are the following:

*Accessibility:* The electronic voting system must be accessible to voters regardless of their geographical location or electronic equipment they use, so as to access the electronic voting system (computers, PDAs, cable TV, mobile phones et al. [52, 4].

*Availability:* During a voting process, the electronic voting system must maintain the same availability response for all voters. Today, availability problems of Internet services are less network link related and more erroneous service availability problems of Internet services are less [26, 33].

*Reliability:* Electronic voting system reliability is identified by a set of performance metrics.

*Efficiency:* The computations can be performed within a reasonable amount of time [26, 33].

*Mobility:* There are no restrictions on the location where voters can cast their ballots. The electronic voting system must provide methods to cache user voting sessions in case a voter faces roaming problems or interacts with the electronic voting systems over network interfaces with latency problems (satellite links, mobile phones, wearable devices [12, 26,33].

*Multi language support:* The electronic voting system must provide multi-language support for voter registration, election process and election results display [38].

*Care for Special Needs:* The electronic voting system must provide ways of interaction with the system for people with special needs [4].

There are also election-specific requirements depending on the conditions of conducting the electoral process, e.g. the exclusion of a candidate from the electoral committee of the elections.

### 2.3 E-voting types

There are many ways to categorize voting systems depending on the needs they have to fulfil, the technologies they use, the voting location, whether they are supervised or not. We could also subcategorize technologies according to the network and the equipment they use. We show the taxonomy of voting systems based on previous [42, 47, 61].

We divide the elections into the physical voting and electronic voting.

#### 2.3.1 Physical voting

It is divided into conventional voting and epistolary voting.

**Conventional voting**

It can be materialized either by the typical ballots or by the epistolary voting of absentee voters. **Computer counting**

It can be materialized either by optical scanning systems or by punch card systems. In the former means, the ballots are marked by voters in such a way that an optical counting machine can read them. In the latter, divots are removed from perforated cards. The ballot cards are then collected and tallied at a central polling station [45]. Computer counting systems are vulnerable to fraud and error.

#### 2.3.2 Electronic voting

It is divided into direct recording electronic voting, polling station voting, Internet/private network voting and phone voting. The latter could be a sub-category of remote voting, as will be presented later on.

**Direct Recording Electronic [DRE] voting**

Voters use touch screen systems or keyboards on PC based technologies to vote at a terminal which is directly connected to a central station [14]. The votes are immediately added to a running tally stored in a computer storage system. The final DRE tally is then moved to a central location where it is added to the tallies obtained from other DRE machines.

**Polling Station voting**

Voters use voting system clients to submit their votes electronically. The whole process is usually controlled by authorized entities. Subcategories of
this category can be the means by which the voting is achieved, such as poll sites, kiosks, or any digital equipment connected to the network. 

**Kiosk** e-voting consists of voting oriented machines being used in the polling station or elsewhere, to let electors cast their votes. Votes are cast using buttons or a touch screen and are stored in an electronic memory.

**Poll site** voting requires voters either to go to staffed polling sites and use computers to cast their votes or to use a network (Internet or private) to transfer ballots from each polling place to a centralized site, where votes are tallied and election results are published.

**Internet/private network voting**

It includes both poll site voting and remote voting.

**Remote voting**

Voters use a computer or a digital television or a mobile phone to mark their ballot. Elections held using remote voting can be contentious because it is difficult to verify that the voter is who he/she claims to be. Both anonymity and privacy are compromised because others can watch the elector vote. This opens the door to voter coercion and vote buying.

**Phone**

Phone voting also composes a separate category of electronic voting, when it is used independently of Internet/private network. Votes are cast either through a touch-tone system or through SMS text messages on mobile phones. Authentication is achieved through the use of PIN and access codes. Phone voting depends on highly centralised, private infrastructures which are also unreliable and insecure.

### 3 Problem Solution

This framework proposes an EVS (Electronic Voting System). It has to be a secure application for the conduct of electronic elections through the Internet. It has to be a web application based on its own security protocol. It has to be also modular and tolerant enough to resist anyone who would attempt to violate security mechanisms. It will offer a combination of new features, which renders it an alternative suggestion to existing and tested e-voting systems. With the proposed system we hope to attract developers, by offering the motive of the open framework, for further development. Since the proposed e-voting system will be implemented it has to be applied and tested real elections.

#### 3.1 Legal Aspects

As, e-voting is not prohibited by Greek Constitution, the procedure followed should require strict identification and authentication of the individual. A main tool in this technical system can be the digital signature for every voter, issued by the public administration, delivered in a secure manner to identified and authenticated citizens [62].

In accordance with the principle of technological neutrality, the electronic signature can also be made via other technical means, such as mobile phone, pc/internet [31].

The second fundamental principle of the protection of privacy and voter anonymity should be applied through (a) The unequivocal identification of the voter, (b) The establishment of an election committee in order to ensure verifiability and reproducibility of the election and (c) the protection from sabotage either by external attacks or by voters or candidates attempting to disturb the elections.

In order to guarantee free suffrage, firstly, the machine which the voter is using to vote must advise him/her that his/her vote has reached its destination. Secondly, the encryption of the data transmitted must be so designed as to ensure that no electronic ballot paper which has been altered will be counted. Thirdly, the way in which persons using electronic voting are guided through the procedure must not be such as to encourage them to vote precipitately or without reflection [31]. As a fourth requirement, the legislation states, that before voting, voters must have their attention explicitly drawn to the fact that, by submitting their vote by electronic means, they are playing a valid part in a ballot. Fifthly, it must not be possible for any manipulative message to appear during the process of electronic voting on the machine being used by the voter to cast the vote. Finally, as they vote, voters must be able to alter their choice before submitting their vote, or to break off the procedure.

In any case the legal standards follow the pattern of the five basic principles of democratic elections and referenda: universal, equal, free, secret and direct suffrage. These five principles have to be equally applicable to e-voting as to traditional elections or referenda. However, e-voting is not ruled by specific provisions, in Greek Legislation, although the process is followed in elections collective management bodies (higher education).

#### 3.2 Technical Aspects

There are 3 main entities involved in the e-voting system: the Election, the Committee, and the Voter. The election authority is a group of administrators or system supervisors. The Election committee is a group of voters that have been selected by the authority and are responsible for interacting with the voters in order to give them access to the system.
The Voter must have 2 valid e-mail accounts in order to complete the procedure of casting a vote. The procedure consists of 10 steps which are presented next: (1) Enrolment, (2) Create Voter record, (3) System Login, (4) Enter election, (5) Apply participation to election committee, (6) Check and validation by the election committee, (7) Creation of digital signature, (8) Ballot fill-in and vote casting, (9) Ballot encryption and (10) Announcement of valid ballots.

Step 1: This step is mandatory for non-registered voters. In the case the voter must visit the election authority in person, and fill in the registration form. Moreover, the voter can choose a username and password with which s/he can login to the system as a simple user.

Step 2: During the voter registration process, 3 cryptographic keys are created, which are: passkey, public key, and private key. The passkey is sent to the primary e-mail account, and the public key is sent to the secondary e-mail account, while the private key is securely kept in the system.

Step 3: The voter logs in to the system, using the username and password, as a simple user.

Step 4: The voter enters the elections using his passkey.

Step 5: The voter applies for participation to the relevant election procedure. Also, the election committee is notified, and checks the voter’s record.

Step 6: The election committee gives the voter access to the relevant election procedure, while a random set of characters (message digest) is sent to the voter.

Step 7: The voter creates a digital signature, using the system with his public key and the message digest received from the election committee.

Step 8: The voter fills in the ballot, signs it with the digital signature, and sends it to the election committee, while he applies a crypt key.

Step 9: The ballot contents are encrypted using the crypt key which is not stored on the system, and are temporarily saved on the system. Once the ballot is successfully validated and counted a ticket vote is sent to the voter. The voter can use this ticket vote in order to make sure that the ballot was successfully counted.

Step 10: After the end of the voting procedure, all the ticketvotes that have been successfully counted are announced on the election bulletin board. If a voter does not find his/her ticketvote on this board, then s/he can fill in an application and send it to the election committee in order to reexamine the ballot.

4 Discussion
There are many advantages of this new technology in comparison to manual / paper-based voting [4]. The fundamental advantages include:

Accessibility
The participation is less limited by geography, disability or networks.

Accuracy
A high profile case of manual counting inaccuracy may occur. Using e-voting, human error can be eliminated in the tally stage. Since the votes are stored electronically, it totals the votes more accurately than a human would even if he or she were to recount the votes many times over [29].

Care for Special Needs
An additional feature that makes electronic voting more favourable is that it assists disabled citizens. With this feature voting would be a much easier task to complete for disabled citizens [63, 64].

Convenience
E-voting is more convenient for voters. For national election, more polling booths can be set-up using remote connection for ballot collection. This reduces voters' travel time and significantly increases voter turnout. Voters are allowed to vote from any location at their convenience.

Cost
The use of electronic ballot removes the cost of producing a physical paper ballot. The use of some remote communication mechanisms also minimises the cost of transporting physical ballots for aggregation of voting result. Ballot counting automation using a computer application minimises administration overhead and reduces the number of officials required for the counting process.

Efficiency
Using some electronic means (e.g. optical mark sense sheets, touch screen voting, remote connection), tally stage to reveal voting result is made more efficient. Ballots tabulation and the aggregation of results from different polling locations can be done electronically [39].

Facilitation
The citizens can access information and provide input which previously has often been restricted [38].

Multi language support
Another advantage is that it appeals to citizens whose main language is not English. Electronic voting is basically a digital voting system, so the characters on the screen can be easily changed to whatever is desired by the user [29].

Timeliness
It is the opportunity to participate in voting when it takes place. A vote is instantly counted, so there is no time gap between casting the ballot and counting it [29]. The machines are also hard to tamper with, because of how they are connected [54].

There are also some disadvantages in electronic voting systems. They include:

Closed source code

One more flaw of the electronic voting system is that its source code is closed. This means that the public cannot examine the source code on the machine, so if a programmer of the code were to be bribed, threatened, or the manufacturer itself is willing to rig an election, they would have a high chance of hacking the vote [6].

Coercion Resistance

The electronic voting system has the appropriate mechanisms to prevent a user to prove how he voted. But this is also a flaw of the electronic voting system since there is no way for a voter to know what the machines record when they cast their vote and also there are no physical paper evidence available for a recount or a receipt to ensure that the voter voted for their choice [6]. This is quite a flaw, because if there is ever a crash in system, there will be no paper trail to follow. With no paper trail, there is not even the slightest chance in recreating the votes.

Privacy

One major obstacle to the success of e-democracy is that of citizen identification. For secure elections and other secure citizen-to-government transactions, citizens must have some form of identification that preserves privacy [10].

Security

Another drawback of the electronic voting system is the security. Software on the machines is checked only for logic-errors and vote-counting mistakes but not for security holes. Also, all the tests performed on the software were automated, and the hardware was not tested at all, which is quite a concern [10]. Basically there is no security on this software and hardware, allowing hackers to rig an election by attaching a standard keyboard to the machine and invoking supervisory commands [6]. Running under a public operation system such as Windows, which did not receive its latest security upgrades, it is vulnerable to certain viruses and worms if it should ever connect to the Internet [6]. A way around this problem would be to change to a different operating system, preferably open-source.

Additional disadvantages

Another flaw is that there are many vested interests that would be harmed by a more direct democracy. As technology advances, everyday things that we use become inferior. These inferior objects are then phased out of society until they show up in a museum. Though this can be a good thing, some advances can be too fast and leave the new technology very vulnerable to sceptics because of its flaws. When technology becomes involved in the voting system, it cannot be sure that the technology will even work right.

The e-voting experience in Ohio in 2004 [65] is one of the well-known examples which caused many discussions about vote miscount and modification. Therefore, it is not easy to say that an accurate and faultless e-voting is likely to become viable soon for governmental elections.

A quote attributed to Stalin says: “Those who cast the votes decide nothing. Those who count the votes decide everything.” It is clear that voting systems represent a critical component of a democracy.

When voting takes place in an electronic environment, possibility of fraud is unavoidable since ensuring the trust is not an easy task [28]. At any step in the e-voting process, e-voting results can be manipulated if there is lack of verification and validation. Majority of people may accept and use e-voting, but people have some doubts about the privacy, security and accuracy of the e-voting.

The deployment of e-voting systems has not to be done at the expense of conducting fair elections. It is instructive that some advocates of Internet voting [41] agree that the risks are too great for national elections where the fabric of democracy is at risk. However, they point out that there are a number of smaller elections (e.g. school boards) where participation is scanty and there is less at stake. These would be good potential candidates for experiments in Internet voting.

5 Conclusions

The application of such a system is hard to convince the parties, their candidates and the voters about its reliability and integrity. There is also skepticism about the security, the anonymity and the voting documentation procedures that the system fulfils. Their concern is to ensure that the results were authentic and not manipulated, and that the anonymity of each voter would be fulfilled. A drawback related to the e-voting systems in general is the uncoercibility, i.e whether the EVS has the appropriate mechanisms to prevent a user proving how he voted. On the other hand, the voter wants to know what the machines record when they cast their vote [6].
The design of e-voting systems must be treated as a socio-technical problem and indeed one that might with benefit be treated differently in countries with differing existing practices and attitudes [60]. In fact we believe that at least equal weight must be given to socio-technical issues such as (i) system understandability and usability, and (ii) the roles, both positive and negative, likely to be played by the various people and organizations involved in the overall voting process, as is given to any attestations by technical experts as to the trustworthiness of complex e-voting hardware and software.

As future work, the extension of the framework, so that other equipment such as personal digital assistances (PDAs), mobile phones, and cable TV will be applicable. Special consideration has to be given regarding disabled people.

References:


