

Σε ανταπόκριση σχετικού αιτήματος, υποβάλλω παρατηρήσεις σχετικές με το site www.eu2003.gr που αφορά στην Ελληνική Προεδρία της Ευρωπαϊκής Ένωσης το πρώτο εξάμηνο του 2003.

Στη διάθεσή σας για περαιτέρω σχολιασμό και διευκρινίσεις.

Depending on the location wherein the electronic ballot is cast, Internet voting systems¹ are grouped into three general categories²:

1. Poll site systems³
2. Kiosk systems⁴
3. Remote systems⁵

Research on the feasibility of Internet voting systems concludes that poll site systems offer benefits and could reasonably be fielded in the foreseeable future. The next step beyond poll site systems could be the deployment of kiosk systems in public places other than poll sites. Remote systems, though, pose significant risk to the integrity of the voting process and should not be fielded for use in public elections until substantial technical and social science issues are addressed⁶.

¹ **California Internet Voting Task Force (CIVTF)**, *A Report on the Feasibility of Internet Voting*, January 2000. According to CIVTF, Internet Voting System is an election system that uses electronic ballots that would allow voters to transmit their voted ballot to election officials over the Internet. But, see **Claude Bonard** (Secretary General of the Geneva State Chancellery), *The Geneva E-voting Project*, 2002, wherein Internet Voting is defined in relation only to remote voting through the Internet.

² **Internet Policy Institute (IPI)**, *Report of the National Workshop on Internet Voting: Issues and Agenda*, Sponsored by the National Science Foundation and conducted in cooperation with the University of Maryland and the Freedom Forum, March 2001.

³ It refers to the casting of electronic ballots at public sites wherein election officials control the voting hardware and software of the voting system. See also *ibid.* **CIVTF**, 2000, p. 3, which refers to poll site systems as Polling Place Internet Voting.

⁴ It refers to an intermediate voting system between poll site and remote voting, in which tamper-resistant voting terminals are located in convenient places—malls, public services sites, schools, etc—and the hardware and software of the systems remains under the control of election officials.

⁵ It refers to the casting of electronic ballots at private sites—home, office, etc—wherein the voter or a third party controls the hardware and software of the voting system. See also *ibid.* **CIVTF**, 2000, p. 3, which refers to remote systems as Remote Internet Voting.

⁶ *Ibid.* **CIVTF**, 2000, p.12, wherein the complete replacement of existing election processes is not feasible currently because of shortages in the satisfaction of the following prerequisites: (1) Digital Identification, (2) Voter registration, (3) Petition signatures, (4) Voter access. See also *ibid.* **CIVTF**, 2000, p.34, wherein the gradual introduction to Internet voting systems could rely on the use of kiosks and computers already installed in public facilities. See also *ibid.* **IPI**, 2001, p. 2, wherein it is also noted that remote systems might be appropriate in the near-term for special populations such as the military and government employees based overseas. See also **The Independent Commission on Alternative Voting Methods (ICAVM)**, *Elections in the 21st Century: From Paper Ballot to E-Voting*, 2001, p. 88, according to which The United States Federal Election Commission (FEC) states in its latest 2001 Voting System Standards (VSS) guidelines that: “At this time it is widely recognized that the technologies now used to develop Internet-based business systems do not fully address the requirements and risks associated with voting over the Internet. Consequently, the VSS do not promote Internet voting.” But, the United States FEC also states in its VSS guidelines: “The VSS allow for Internet voting systems operated in parallel with another voting system, and do not address or allow for a stand-alone voting system.” See also **United States Department of Defense, Washington Headquarters Services, Federal Voting Assistance Program (DoD-**

The Internet voting system that the 2003 Greek Presidency to the European Union has deployed through the URL <http://evote.eu2003.gr> (hereinafter, **evote2003**) resembles more to an Internet polling site rather than an Internet voting site. *E-poll* would have been more appropriate a name for the **evote2003** endeavour than *E-vote*.

The legibility of Internet voting systems depends on certain criteria. These criteria are based on traditional voting systems and their satisfaction is deemed appropriate for the deployment of any voting technology. These criteria are the following:

1. Eligibility & Authentication⁷
2. Uniqueness⁸
3. Accuracy⁹
4. Integrity¹⁰
5. Verifiability & Auditability¹¹
6. Reliability¹²
7. Secrecy & Non-Coercibility¹³
8. Flexibility¹⁴
9. Convenience¹⁵
10. Certifiability¹⁶
11. Transparency¹⁷
12. Cost-effectiveness¹⁸

FVAP), *Voting Over the Internet (VOI) Pilot Project Assessment Report*, 2001, prt. 6.3.1, according to which the VOI pilot project was a study that demonstrated that a stand-alone system for remote registration and voting over the Internet can be a secure, viable alternative to the by-mail process in a small-scale, tightly controlled environment. However, there are a number of security concerns in expanding remote voting to a larger population. These include the possibility of malicious software on citizen workstations and the susceptibility of Internet systems to denial of service attacks and hacking.

⁷ The system should be capable for allowing only authorized voters to vote.

⁸ The system should be capable for preventing authorized voters to vote more than one time.

⁹ The system should be capable for recording votes correctly.

¹⁰ The system should be capable for preventing any modification of votes as well as for detecting any attempt to modify or forge votes.

¹¹ The system should be capable for allowing verification that all votes have been correctly accounted for in the final election tally and for maintaining reliable and demonstrably authentic election records.

¹² The system should be capable for robust operation without loss of any votes or other data.

¹³ The system should be capable for preventing any attempt to determine how any individual voted.

¹⁴ The system should be capable for allowing a variety of ballot question formats, compatibility of a variety of standard platforms and technologies including technologies used by people with disabilities.

¹⁵ The system should be capable for allowing voters to vote quickly and with minimal equipment or skills.

¹⁶ The system should be capable for allowing testing that certifies satisfaction of predetermined necessary criteria.

¹⁷ The system should be capable for allowing access to clear and understandable information upon its operation.

¹⁸ The system should be affordable and efficient.

All of the above-mentioned criteria should be met to guarantee for a trustworthy E-Vote endeavour¹⁹. Which of the aforementioned criteria does the **evote2003** satisfy to guarantee for its trustworthiness?

The most difficult task for the implementers of Internet voting systems is to gain the electors' trust regarding the deployment of Internet technologies in the voting process. Trust to **evote2003** is not a matter of strategically designed and implemented political marketing aiming at promoting the idea of E-Voting, but rather it's a matter of information available to the electors which addresses the Internet voting system's characteristics that meet the aforementioned criteria and make it trustworthy, consequently. Even in an E-Poll endeavour, which is of a different nature than an E-Vote endeavour, the implementer should provide its target audience with information addressing the following issues, at least:

1. Accessibility²⁰
2. Authentication²¹
3. Undue Influence²²
4. Protection of the communication link²³
5. Protection of the server²⁴
6. Scrutiny²⁵
7. Speed and Accuracy²⁶

¹⁹ The aforementioned criteria for the legibility of Internet voting systems were set by *ibid.* **ICAVM**, 2001. See also *ibid.* **Claude Bonard**, 2002, for the necessity of (1) Voter's identification, (2) Voter's ID check, (3) Protection of ballots from interception and manipulations, (4) Secrecy of ballots, (5) Auditability of the process. See also **The CALTECH-MIT Voting Technology Project**, *Voting: What Is & What Could Be*, 2001, and *ibid.* **DoD-FVAP**, 2001, and *ibid.* **IPI**, 2001, and *ibid.* **CIVTF**, 2000.

²⁰ The system should cater for overcoming the "digital divide" by allowing accessibility to it from electors irrespectively of their access to technology. For example, does the **evote2003** system offer an alternative technological means for participation such as an 800-telephone line or does it require participation from Internet users only?

²¹ The system should allow some sort of authentication for legitimate participation. For E-Voting systems, three methods of authentication have been proposed: (1) Biometric identification, (2) Username-PIN identification, (3) Digital signature identification. Does the **evote2003** allow any authentication which prohibits a participant from participating under different names as many times as he/she deems necessary to affect the project's final results?

²² The system should prohibit undue influence upon participants such as bribery and vote-buying & -selling by allowing multiple entries to the system and multiple voting with the knowledge that the final vote would replace any previously cast.

²³ The system should protect the communication link between the client and the server. The system should alleviate the danger of unauthorized interception or reading of ballots between the vote being cast and being received by the system. Does the **evote2003** use any encryption to solve this problem? Does the **evote2003** plan to make use of PKI technology and electronic signatures or SSL technology to enhance the solution to this problem? Does the **evote2003** provide the participant with any kind of verification message as a reassurance for his/her participation?

²⁴ The system should protect the server of the **evote2003** against malicious actions such as spoofing and denial of service attacks. In addition, the system should not be totally dependent on any one element or part of it to operate smoothly. In the event of malicious action against the said critical part for the system's operation, the **evote2003** could be set out of order.

²⁵ The system should allow for transparency of the voting and counting processes. The presentation of current results during the process of participation in the **evote2003** does not guarantee transparency, but merely indicates speed and—probably—accuracy in the results of E-Voting.

In addition to information addressing the above seven issues, an E-Poll/E-Vote endeavor should:

1. Be cost-effective²⁷
2. Keep open to the public its source code²⁸

The goal of the present analysis is to a concisely comment on the **evote2003** and its experimental deployment within the 2003 Greek Presidency to the European Union, thus contribute to the evolution of Internet voting systems and their favourable use by both electors and elected. Therefore, the present analysis does not elaborate upon the following issues despite them being of vital importance for the incremental deployment of Internet voting systems:

1. Government regulation²⁹
2. Other means of technology capable for enhancing civic participation in governmental affairs³⁰

²⁶ The system should allow for fast and accurate vote counting because this is one of the two main reasons why electors would opt for an Internet voting system—the other one is convenience. See also **Derek Dictson & Dan Ray SecurePoll.com**, *The Modern Democratic Revolution: An Objective Survey of internet-Based Elections*, 2000, p. 5, according to which the most compelling factor in favor of Internet voting is the convenience factor.

²⁷ The cost of participation should amount to less than 1 € for each participant. This amount may represent the cost of using the telecommunications network to connect to the **evote2003**.

²⁸ See *ibid.* **CALTECH-MIT**, 2001, pp.42-47, according to which the source code for all vote recording and vote counting processes should be open and the source code for the user interface proprietary

²⁹ For an E-vote endeavor to exist, government regulation must cater for its legal existence. If government regulation does not make any provisions upon Internet voting systems, then even the best Internet technology would not suffice.

³⁰ It is expected that Professor Giorgos Papadimitriou will elaborate upon the issue on Sat., June 14, 2003. Once the opportunity is given, comments and additional information could be inferred to support Professor Giorgos Papadimitriou's approach.