A "step-wise refinement" approach for enhancing eVoting acceptance

Yannis Stamatiou [1,2]
istamat@cc.uoi.gr

Dimitris Sofotassios [2]
sofos@cti.gr

Anastasia Panagiotaki [2]
panagioa@cti.gr

Polyxeni Nakou [2,3]
nakou@cti.gr

Christos Manolopoulos [2]
manolop@cti.gr

Paul Spirakis [2,3]
spirakis@cti.gr

[1] Mathematics Department, 451 10, Ioannina, Greece

[2] Research Academic Computer Technology Institute, N. Kazantzaki, University of Patras, 26500, Rio, Patras, Greece, +30 2610 960 200

[3] University of Patras, Department of Computer Engineering, 26500, Rio, Patras, Greece

ABSTRACT

The successful transformation of eGovernment from a nice idea into a successful reality had been hindered by a variety of factors ranging from bureaucratic and legislative inertia to the inability of countries to achieve a sufficient IT penetration in their societies. Nowadays, the fall in IT prices, the development of innovative IT solutions and the rise in IT literacy in a number of countries has, at least tackled the latter issue. However, people still are not as enthusiastic, as it was envisaged by technocrats and politicians, in using IT solutions to pass from eGovernment to eGovernance, a notable example of which is *eVoting*. In this paper we argue that efforts to introduce complex eGovernment and eParticipation applications should be gradual and develop solutions hand-in-hand with in-field trials that increase (also gradually) in complexity and people inclusiveness, so as to handle the various forms of social inertia successfully. We present our experience in the eVoting domain and suggest that a similar approach in eVoting (and other demanding eGovernment/eParticipation applications) could fare better to success than introducing to people a system that suddenly appears and claims to be the "perfect", all-in-one, solution.*

Categories and Subject Descriptors

D.2.1 Requirements/Specifications - Elicitation methods (e.g., rapid prototyping, interviews, JAD), Languages, Methodologies (e.g., object-oriented, structured), Tools

D.2.4 Software/Program Verification - Assertion checkers, Class invariants, Correctness proofs, Formal methods, Model checking, Programming by contract, Reliability, Statistical methods, Validation

K.4 COMPUTERS AND SOCIETY - K.4.0 General, K.4.1 Public Policy Issues, K.4.2 Social Issues, K.4.3 Organizational Impacts, K.4.m Miscellaneous

K.5 LEGAL ASPECTS OF COMPUTING - K.5.0 General, K.5.1 Hardware/Software Protection, K.5.2 Governmental Issues, K.5.m Miscellaneous

General Terms

Experimentation, Security, Human Factors, Verification

Keywords

eVoting, eGovernment, computer security, IT penetration, cryptography.

1. INTRODUCTION

It can be reasonably argued that currently available Information Technology (IT) innovations, in conjunction with the increase of technological minded citizens, provide the ideal conditions that can lead to the flourishing of the eGovernment concept in any facet of a citizen's life. What we witness, however, today is that the concept of eGovernment applications is mainly limited to, merely, providing information or simple form downloading or filling in services [4]. One should expect that, given the maturity of technology, many more useful services, such as automatic changes in a citizen's property status after a purchase or sale of an apartment or automatic update of a citizen's family status after the birth of a child. Such services would relive citizens from having to repeat numerous times the same information each time a form needs to be filled in. One of the reason why such drastic eGovernment services have not been widely available today is that eGovernment heavily relies, apart from technology, on citizen's trust and acceptance [10]. The currently adopted model for advancing eGovernment services is to provide simple, localized (e.g. at a municipality level) services that people understand well and trust that they do not leak any sensitive information about themselves. The next step is to provide more complex (and more useful) services, such as the ones outlined above. This smooth process seems to work well due to the following main reasons: 1) it matches bureaucratic and legislative inertia (i.e. time is given to the government to adjust to the new IT-based, governance model), and 2) time is given to citizens to

* This work has been partially supported by General Secretariat of Research and Technology of Greece, under the project ΠΝΥΚΑ (project code ΔΕΛ_2, decision 8948/04.05.06), Operational Program of Western Greece, 3rd Community Support Framework.

ICEGOV2008, December 1-4, 2008, Cairo, Egypt

increase their IT literacy and understand current, simple services (both in terms of technology and usefulness) before using more complex ones.

The situation changes dismally when one contemplates the status of more participatory facets of eGovernment and particularly eVoting, which lies in the heart of eDemocracy and eParticipation initiatives. Although several attempts have been made (e.g. in Estonia [5]) eVoting has not been received with the same enthusiasm by people as the "normal", everyday eGovernment services ([1]). In our opinion the reason is that technocrats attempted an abrupt, all-inclusive, all-by-themselves approach to introduce this important process. These attempts led to disasters that received much publicity [2], which was more than sufficient in order to provoke negative (or, at best, mixed) feelings towards eVoting in general among people.

Our viewpoint is that in order to enhance eVoting acceptance among citizens one should use a step-wise, stratified approach based on the following three axes, much like the introduction of more complex eGovernment services: 1) small-scale towards large scale elections, 2) less critical towards more critical elections, and 3) elections involving few people and on a voluntary basis towards elections requiring a more massive participation. Each attempt should be accompanied by suitable discussions before and after the attempt, involving as many stakeholders as possible in order to provide useful feedback that can lead to improvements in as many aspects of the eVoting process (e.g. legislative, technological, social etc.) This process is slow but it can fare better to success than previous, all-or-nothing approaches in the eVoting domain.

In this paper we present the set-up, operation and observation of a pilot operation of a complete eVoting system that was developed by our team. The pilot was targeted at introducing eVoting to people using the step-wise approach. We also discuss our conclusions based on our experience as well as participants' opinions and comments. Our next step is to contact an enhanced eVoting process both in terms of scale, criticality, and participation.

2. TOWARDS A STEP-WISE ADOPTION OF EVOTING

The application of IT security primitives and protocols as well as technologies lies at the heart of a reasonable eVoting implementation and deployment approach [6]. While strong IT security is a necessary condition for successful eVoting systems, it is by no means (unfortunately) sufficient. In what follows we present the components of a step-wise, trust-driven approach towards the adoption of eVoting by people. The approach involves all stakeholders at the same time and is targeted at convincing them of the usefulness and security of using the eVoting system (see Figure 1).

The principal axes of the approach are the following:

(i) *Proven technological excellence for the system components*. The system should use strong technological tools and computer science primitives, preferably scientifically proven and standard-based [9]. This ensures the sound operation of the system and its robustness against potential attacks. This aspect, though not easy to address, may be approached using the latest technological advances, especially in the field of security.

(ii) *Use of open source technologies and publicly available information.* System development and operation should be based on open source technologies to allow independence from existing vendors and increase transparency [7]. The system should be open to scrutiny by experts and auditors. An open call for attacks before productive operation is also useful, with an aim to prove system's robustness and attract citizens' trust.

(iii) *In field user assessment.* After the end of the voting process, users/voters should be motivated to assess the system and the whole procedure, in terms of various aspects: user-friendliness, efficiency, perceived trust, etc. This feedback should be taken seriously into account for improving the system and the organization of the voting procedure, for further applications. Apart from the in-field assessment process, users should receive later another assessment form that the system stakeholders should design so as to take into consideration the in-field assessment process as well as the fact that the users have had some time at their disposal to think about the whole election process (off-line user assessment).

(iv) Organize pre- and post- application information campaigns. Information campaign before an eVoting event improves stakeholders' understanding of the system's capabilities and operation as well as use, while information days after the eVoting event help stakeholder understand each other's views and propose improvements on the operation and usability of the system. These information days should include technical people, voters, legislation officials, social scientists etc.

The aforementioned aspects should be accompanied by a step-wise, *gradual application* of the system, as described in the introduction. For instance, the eVoting system should be applied, first, in simple eVoting scenarios (e.g. expression of opinion, polling etc.) and then applied to scenarios of increasing criticality and complexity (e.g. election process in scientific interest groups, elections in societies and organizations, local elections for representatives, and finally to national elections). This gradual adoption effort has multiple benefits: first of all, it allows for thorough, in-field evaluation of the system, using increasingly more complex eVoting scenarios. In addition, time is given to stakeholders to develop opinions and views about the system that will contribute to its improvements in order to face a more demanding eVoting procedure. In this way, eVoting will be gradually established and trusted by citizens as well as the involved stakeholders, something which could not be achieved (and has not been achieved, as witness by documented cases of eVoting failures) if one attempted to penetrate eVoting technology to the whole population of a country and for a critical eVoting process.

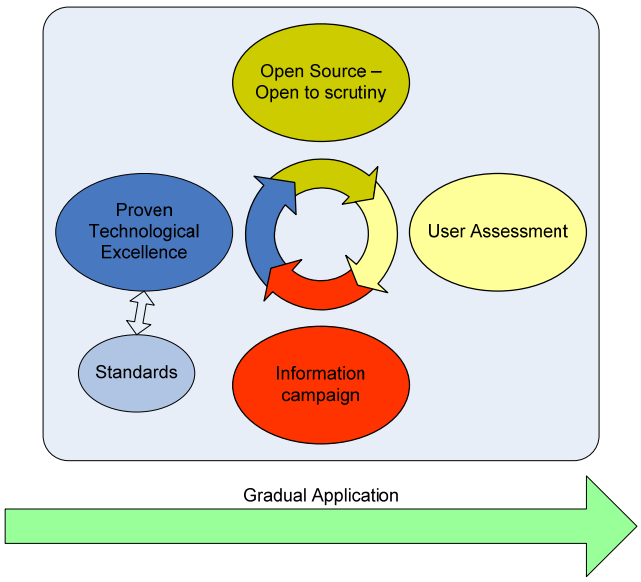

Figure 1. Gradual application model

This approach was used for the first, real-life application of an eVoting prototype/system that was developed by our team, as described in the following section.

3. SETTING-UP A PILOT

The objective of the pilot was to assess first of all sound operation of the system, to validate the selected architecture and to test the interconnection between different third-party open source tools that complemented the core system functionality (Open CA, Open VPN, etc.). A further objective was to receive a first feedback from actual users/voters, regarding system functionality and perceived security and eVoting in general. Finally, this pilot was meant to be a first step of a gradual application of the system to larger scale scenarios.

First of all, a small scale, non-critical scenario was selected for the pilot. The idea was to perform a poll among 200 of the members of a local professional organization (local Technical Chamber). This group was selected for the following reasons. It is a well defined group, with easy access to its members (email, address, etc.). What is more, its members, being engineers, are familiar with ICTs and are a good testbed for the first application of such systems. Finally, the Technical Chamber is anyway interested in modernizing its voting processes (e.g. attempts had already been made to automatically scan and tally votes in their last elections for representatives).

The organization of the pilot follows the 4 aspects described in section 2.

(i) *Proven technological excellence.* The eVoting system used applies strong, state of the art technology and scientifically proven cryptographic elements. A brief description of the system is given below.

The selected target platform is an eVoting system that was developed within a nationally funded research project. It is an Internet-based system and supports a wide range of voting processes, from polling procedures to large scale election processes and referenda. Its main features include: (i) A highly distributed architecture for efficiency and control sharing: an hierarchy of central and local Election Authorities (EA) with distributed computations within an Election Authority, as depicted in the Figures 2 and 3. (ii) A robust voting protocol that ensures the basic voting security requirements (secrecy, receipt-freeness, uncoercibility, verifiability, etc.). The protocol is based on strong cryptographic primitives, including zero-knowledge proofs that, essentially, provide the guarantees (without violating the vote secrecy requirement) that votes are correctly received and included in the voting outcome. The protocol uses Elgamal homomorphic encryption and it is based on multiparty computations and threshold cryptography, involving mutually distrusting agents, called keyholders, who control the voting process. The interested reader may consult [11] for the technical details and proofs of security of the protocol.

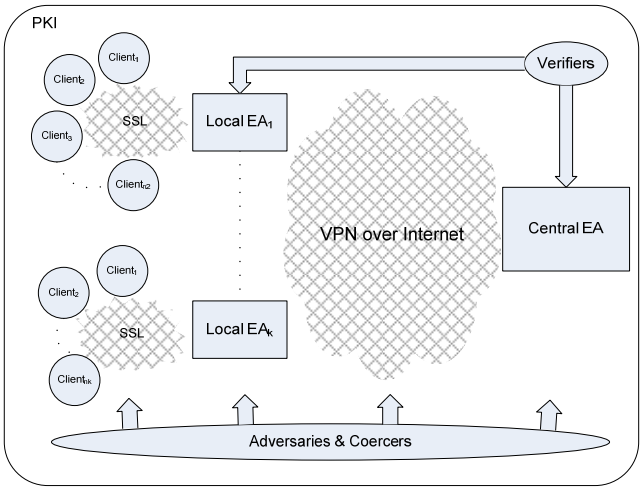

Figure 2. eVoting system architecture

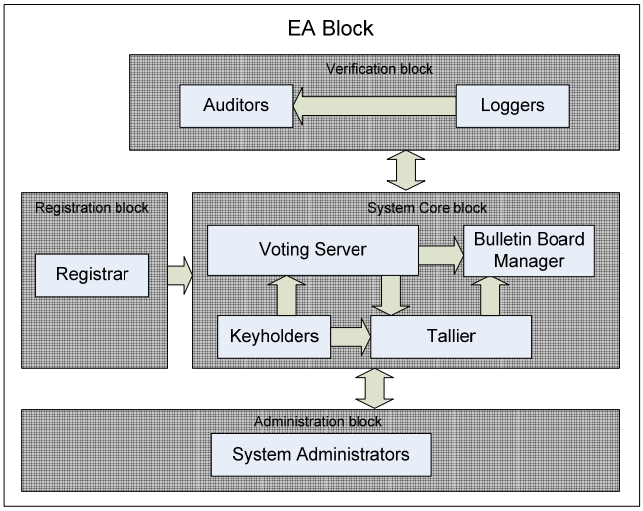

Figure 3. EA block modules

System design and implementation was based on a "trust engineering" methodology as the one described in [3]. This approach combined semi-formal methods (e.g. UML-based design [8]) with risk assessment techniques ([12]), with an aim to provide extensive documentation and to prove system sound operation.

(ii) *Use of open source.* The system used was solely based on open source tools (java programming language - www.java.com, postgre sql database - www.postgresql.org, bouncycastle

cryptographic library - www.bouncycastle.org, etc.) that can be open to scrutiny by experts. Third party tools that were used to complement system functionality were also open source (openCA PKI software, openVPN).

(iii) *User assessment.* The voting procedure was followed by an assessment stage by the users/voters, through the completion of an online questionnaire.

The questionnaire was structured in three thematic parts. The first part was relative to the system and his functionality. Second part was relative to more general subjects of electronic voting (i.e. security issues) and aimed at the investigation of voters' attitude towards the electronic voting. The final part was relative to institutional issues for the wide use of electronic voting. Results of questionnaire answers processing are presented in the "Results" paragraph.

(iv) *Information campaign.* An organized effort was made to involve all relevant stakeholders both before and after the execution of the eVoting pilot. Before the pilot, these efforts included publication of advertisements of the system in the engineers' weekly bulletin, distribution of leaflets and brochures explaining the project, the system and the pilot, explanatory e-mails with detailed instructions and an analytical user manual. Throughout the pilot a help desk service was available to solve any problems. After the pilot, an event was organized to discuss results. All different stakeholders were present, including system designers and developers, voters' community, legal and social experts, relevant researchers, etc. The discussion revealed several interesting issues, including the need for a more user-friendly interface (necessary even for the "expert" engineers!), the need to better convince the voter for the soundness of the process, issues regarding digital divide and e-inclusion, etc.

4. PRACTICAL ASPECTS OF THE PILOT

4.1 Procedure

The total procedure lasted from Monday 3 December 2008, when began the submission of applications for certificate acquisition, until Friday 7 December 2008, when expired the deadline of vote submission.

1) Registration and receipt of an electronic certificate, as means of authentication

The voters could submit certificate application from Monday 3 to Wednesday 5 December, by accessing the website of Certification Authority. Voters completed a form with their personal data and sent this form to Certification Authority. During the time remaining up to the beginning of vote submission, the administrator of Certification Authority checked the data of submitted applications and created the digital certificates for all the legal voters.

At 6 December before submitting their vote, the voters installed their certificate on the browser of their computer, accessing again the website of Certification Authority.

2) Vote Submission

From 10:00 up to 22:00 of December 6 the voters submitted their votes. In the initial page of system they gave their credentials (username and password). These credentials were automatically produced before the beginning of voting by the system and sent to voters via e-mail.

Voters could vote as many times as they want, but only their most recent vote was counted at tallying phase. Voters could see their most recent encrypted vote on the Bulletin Board, a web page actually where were published the public data of voting.

Figure 4. Vote submission page

After voting period expired, the administrator of the system performed the tallying of the votes and published the results.

Figure 5. Voting Administrator page

Support was provided throughout the process by a help desk.

4.2 System configuration

The system is highly modular and customizable in respect to 4 different aspects: scale, security, performance and verifiability.

For the aims of the pilot one central and two local EAs were used. The EAs were three different server machines with exactly the same tools installed and exactly the same configuration. On each local EA a database was installed where the encrypted votes of this EA were stored. On central EA a central database was installed where encrypted votes from all local EAs were stored (see Figure 6).

Regarding the aspects mentioned above, we selected a small-scale configuration of the system, with the following features:

Scale: At the pilot the number of voters amounted to 200, so it was decided to use only two local EAs. Also for this number of voters, it was considered as a suitable way to copy the data from local databases to central database via a synchronous way. That means that during the submission, the encrypted vote was stored in both local and central database. In larger scale elections asynchronous replication is recommended.

Security: The voters were called to answer to a question that concerns the sector of engineers in their country. As the process of voting is not considered extremely critical, it was not necessary to use all the available security measures that system provides: PKI infrastructure, SSL between voters and local EAs and VPN connections between local and central EAs. Moreover voters login in the system giving their username and password.

The selected protocol possesses mechanisms for solving other security issues but their use was judged pleonasm in our case.

Performance: The whole number of voters was divided in the two local EAs. The number of local EAs was considered suitable for the purpose of our pilot, but on a larger scale voting procedure more local EAs must be used in order to obtain better performance.

Verifiability: Limited log files were maintained with voters' identifiers and their encrypted votes. The tallying took place on both locals and central EA in order to verify the final result.

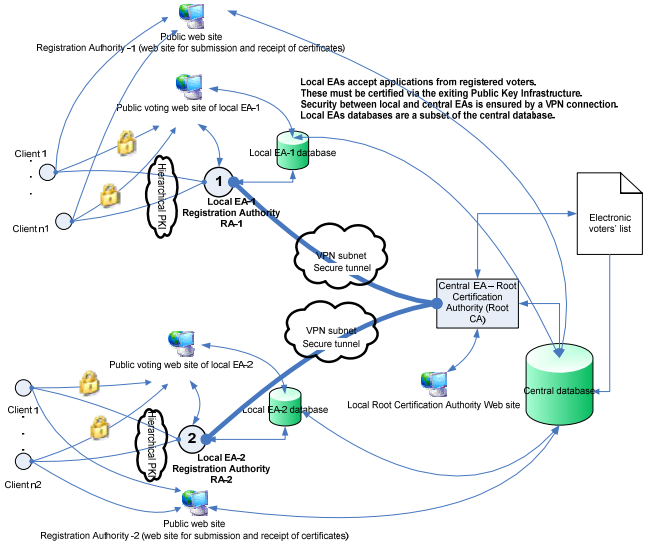

Figure 6. Pilot configuration

5. Results

The pilot was considered successful as a whole, both regarding system operation as well as user acceptance.

Participation: Participation percentages were satisfactory and varied for the two phases of the procedure. 37% of the voting population tried to register electronically, and 31% voted. 20% took part in the assessment phase and completed the questionnaire.

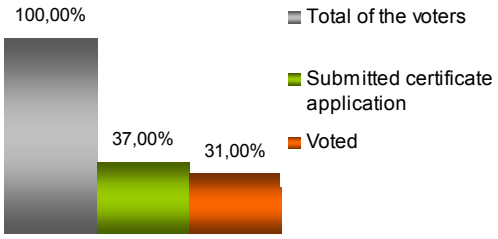

Figure 7. Participation percentages

System operation: System operation during pilot was satisfactory regarding the proposed distributed architecture, the selection and interconnection of the tools (OpenVPN, OpenCA, and other implementation tools) and the implementation of system components.

During voting procedure some minor problems were reported, which were immediately solved by the help desk. These problems were mainly associated with the certificate application submission and more specifically with user browser settings (Active X controls activation). Another problem during this phase was the incompatibility of the certification tool (OpenCA) with Windows Vista (only 1 problematic case). During vote submission no problems were reported.

System assessment results: The system was assessed by 40 users, 32 of whom used the system up to the end of the procedure.

From the answers it resulted that the participation of the majority (78,1%) of the voters was motivated by personal interest for the electronic voting, while only a small percentage (9,4%) participated because of the subject of voting.

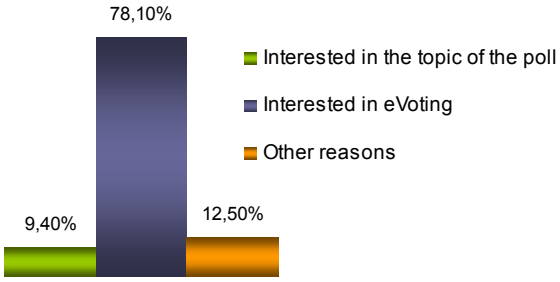

Figure 8. "Which were the reasons for using the particular system?"

With regard to the system, the majority of voters found the system functional enough or very functional (40,6% and 25% respectively). The instructions provided also contributed greatly to this. There was a no negligible percentage that found the system little or by no means functional (percentage 18,8% and 15,6% respectively). This is probably due to the process of application and acquisition of certificate, which the 49,6% considered complicated and the 9,3% excessively complicated. Nevertheless, 43,8% found the process of certification simple.

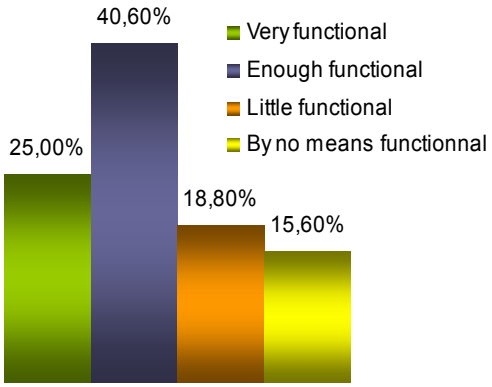

Figure 9. "How much functional did you find the system?"

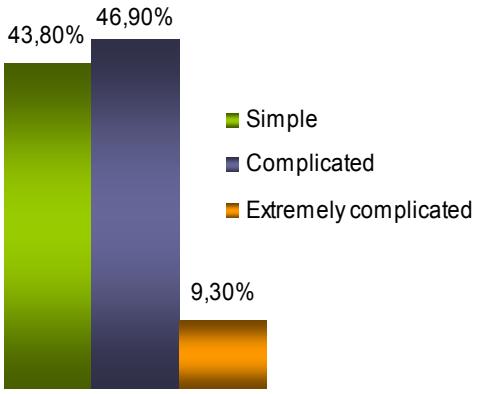

Figure 10. "The certification procedure was …"

This assessment showed that a large percentage of voters found the registration procedure fairly complicated, although they were well familiar with ICT. This is due to the fact that certification was realized with the use of an open source tool simulating a PKI (OpenCA) and not with and existing PKI where the process would be automated. Nevertheless, this remark raises important issues with regard to the target system's user-friendliness, in particular for non-expert users.

Finally, the majority of the voters, taking into consideration the overall experience from the use of the particular system, answered that the electronic voting is easier than the traditional way.

Users were also asked to respond to some questions concerning eVoting in general. It came up that users consider electronic voting easier compared to the traditional way and believe that it will increase the participation in voting procedures. It appears however that there are serious reservations against such systems, since a percentage of 52,5% considers the electronic voting by no means or little secure. This is also confirmed by the answer to the question "Would you vote electronically in national elections?", where the 52,5% answers NO.

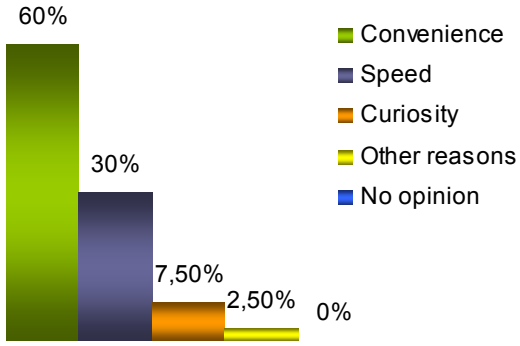

Figure 11. "For which reasons would you choose electronic voting?"

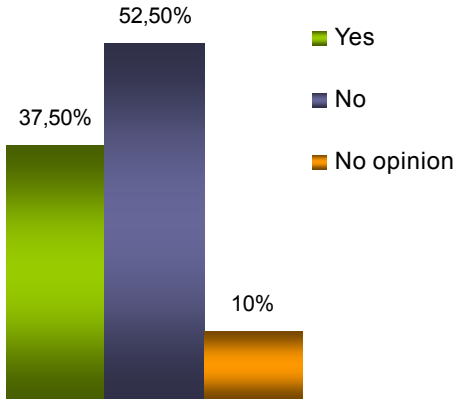

Figure 12. "Would you vote electronically in national elections?"

With regard to legal/institutional aspects of eVoting, the answer to the question "Who institutional intervention you consider more important for the application of electronic voting?" indicates as more important the specification of new roles, as well as the application of measures of protection against phenomena of mass coercion and vote selling. It is also remarkable that only a very small percentage does not have opinion for the subject of question.

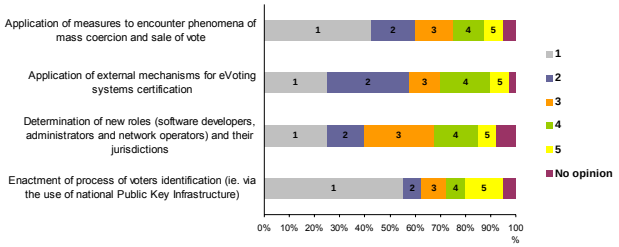

Figure 13. Legal/institutional issues

Also, the sample considers more important practice for the gradual maturation of systems of eVoting the possibility of electronic submission of vote only from fixed points (i.e. kiosks) and not remotely over Internet.

Although examples exist of countries that have enacted the use of Internet-based voting additionally with the traditional voting, the adoption of kiosk-based voting is considered as a milestone for the smooth migration to systems of remote eVoting.

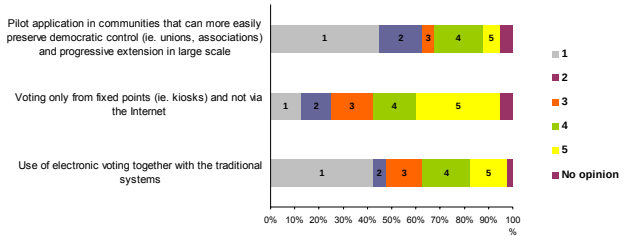

Figure 14. Measures for gradual adoption of eVoting systems

6. CONCLUSIONS

It is unfortunate that with regard to eVoting, there are numerous incidents of misconduct or failures that have had large publicity worldwide. This is not true with other (less complex, admittedly) services such as the submission of income declaration or filling in a job search form at the portal of a municipality. One reason for this is, certainly, the criticality of the eVoting process among all other democratic/governmental processes. However, another equally important, in our opinion, reason is that the system proponents attempted to tackle the eVoting domain in a abrupt, "all-inclusive" approach. Such an approach is very likely to fail (and it failed) because no sufficient time was given to all involved parties, the technologists, the legislators, government officials, and voters to understand each other's needs and constraints. The net result of the "forced" introduction of eVoting was that today people are reluctant even to discuss the adoption of eVoting for participating in electoral processes.

It should be understood that the problem is not about technology. Technology is here to stay and will not cease to enhance and produce more and more innovations. The main issue is whether it will be adopted by people (users) and, if yes, how fast. Our view is that people adoption of IT technology for the implementation of complex and more demanding eGovernment services, such as eVoting, should be a slow, gradual process. This process will provide leaders, managers, and government officials with sufficient time to sense, understand and incorporate into technology, legislation, and service processes, people's feelings and reactions toward eGovernment. Our eVoting findings suggest that complex eVoting services need to be introduced in a step-wise fashion since even a small-scale pilot can generate a disproportionate complexity as well as issues to be further addressed. If these issues are generated and tackled in a step-by-step fashion, using system versions and eVoting procedures of increasing complexity, the generated issues will be easier to handle and address for the next attempt. This is a general remark about the adoption of any new technological innovation. In the beginning, only a few people want to use it. If other people see that these people trust the innovation and adopt it for everyday use benefiting from it, then they will also want to adopt it, leading to an avalanche effect that benefits the acceptance of the innovation among people. Our hope is that this will be the case with eVoting, since its successful incorporation into other successful eGovernment services will be a large step towards the realization of the eGovernment concept in order to cover more complex issues of our Governance and Democracy.

7. REFERENCES

[1] van Acker, B., Remote e-Voting and Coersion: A risk Assessment Model and Solutions, in: Electronic Voting in Europe - Technology, Law, Politics and Society, LNI Proc., 2004, pp. 53 – 62, GI-Editions.

[2] The problems and potentials of voting systems, Communications of the ACM, Special Issue on eVoting, Vol. 47, Iss. 10, October 2004.

[3] Antoniou, A., Korakas, C., Manolopoulos, C., Panagiotaki, A., Sofotassios, D., Spirakis, P. and Stamatiou, Y. C., A Trust-Centered Approach for Building E-Voting Systems, Lecture Notes in Computer Science, Volume 4656, 2007, pp. 366-377, Springer Berlin / Heidelberg.

[4] CapGemini, Online availability of public services: How is Europe progressing? Web based survey on Electronic Public Services. Report of the 6th Measurement. June 2006.

[5] Estonia (National Election Committee), E-Voting System Overview, 2005.

[6] Gritzalis, D., Secure Electronic Voting, Series: Advances in Information Security, Vol. 7, Kluwer Academic Publishers, 2003.

[7] Kiayias, A., Korman, M., Walluck, D., An Internet Voting System Supporting User Privacy, Proc. of the 22nd Annual Computer Security Applications Conference (ACSAC'06), 2006.

[8] Krutchten, P.,The Rational Unified Process, An Introduction, Reading, Addison-Wesley, 1999.

[9] OASIS Standard, EML Process and Data Requirements, ver 4.0, February 2006.

[10] Riedl, R., Rethinking Trust and Confidence in European E-Government, White paper.

[11] Smith, W. D., Cryptography meets voting, living document, version of January 2006.

[12] K. Stølen, F. den Braber, T. Dimitrakos, R. Fredriksen, B.A. Gran, S.-H. Houmb, Y.C. Stamatiou, J.Ø Aagedal, Model-based risk assessment in a component-based software engineering process: the CORAS approach to identify security risks, in: Franck Barbier (ed), Business Component-Based Software Engineering, Kluwer, 2003, pp.189-207.