Comments on the Council of Europe's Draft Recommendation on Standards for e-Voting

Enhancing the technical requirements to improve trustworthiness and public confidence on e-voting in Europe

August 30, 2004

Andreu Riera Jorba, PhD

Chairman & founder
Scytl Online World Security, S.A.
Barcelona, Spain

andreu.riera@scytl.com

Introduction

A number of European states are currently analyzing the possibilities offered by information and communication technologies to improve their democratic practices. The use of electronic methods of voting, or e-voting, is viewed as a promising field that however poses a set of new challenges that have to be carefully addressed.

The Council of Europe, through a Multidisciplinary Ad Hoc Group of Specialists on Legal, Operational and Technical standards for e-enabled voting (IP1-S-EE), has been studying during the last two years the topic of e-voting in public elections and referendums, under the auspices of the Integrated Project "Making Democratic Institutions Work". On July 6, 2004, the IP1-S-EE Group adopted a final Draft[1] of the "Recommendation of the Committee of Ministers to member states on legal, operational and technical standards for e-voting".

The IP1-S-EE Group enumerates in the Draft Recommendation a number of factors that clearly justify the advancement on the study, experimentation and adoption of e-voting throughout Europe in public elections and referendums:

> *"Recognising that as new information and communication technologies are increasingly being used in day to day life, member states need to take account of these developments in their democratic practice;*
>
> *Noting that participation in elections and referendums at local, regional and national levels in some member states is characterised by low, and in some cases steadily decreasing, turnouts;*
>
> *Noting that some member states are already using, or are considering using e-voting for a number of purposes, including:*
>
> *- enabling voters to cast their vote from a place other than the polling station in their voting district;*
>
> *- facilitating the casting of the vote by the voter;*
>
> *- facilitating the participation in elections and referendums of all those who are entitled to vote, and particularly of citizens residing or staying abroad;*

[1] The definitive Recommendation document will be available before the end of 2004 at http://www.coe.int/democracy

- widening access to the voting process for voters with disabilities or those having other difficulties in being physically present at a polling station and using the devices available there;

- increasing voter turnout by providing additional voting channels;

- bringing voting in line with new developments in society and the increasing use of new technologies as a medium for communication and civic engagement in pursuit of democracy;

- reducing, over time, the overall cost to the electoral authorities of conducting an election or referendum;

- delivering voting results reliably and more quickly; and

- providing the electorate with a better service, by offering a variety of voting channels."

The Draft Recommendation therefore promotes the adoption of e-voting by member states. Still, the IP1-S-EE Group is fully aware of the potential risks that would arise from a careless introduction of e-voting. As a consequence, the Draft Recommendation sets out elevate prerequisite objectives to ensure public confidence and an accurate and sound introduction of e-voting:

"Aware of concerns about certain security and reliability problems possibly inherent in specific e-voting systems;

Conscious, therefore, that only those e-voting systems which are secure, reliable, efficient, technically robust, open to independent verification and easily accessible to voters will build the public confidence which is a pre-requisite for holding e-voting;"

The Council of Europe's Draft Recommendation is the result of a comprehensive and thorough study conducted by the IP1-S-EE Group that sets a series of standards and requirements on the legal, operational and technical aspects of e-voting. The objective of the present document is to further develop some of those standards and requirements by leveraging our expertise on technical aspects related to the security and trustworthiness of e-voting systems. As e-voting security experts with a long experience in the field, we provide in this document our comments on the Draft Recommendation, in particular on sections D (Security) and E (Audit) of its Appendix III (Technical Requirements).

We believe that there is room for strengthening the technical requirements related to privacy, security and verifiability, to better accommodate the principle that states that "*e-voting shall be as reliable and secure as democratic elections and referendums which do not involve the use of electronic means*".

General overview of our comments

Our comments on the Draft Recommendation refer exclusively to the technical standards set out in Appendix III (Technical Requirements), and specifically to sections D (Security) and E (Audit). Still, the proposed comments and additions could also affect the Legal Standards –specifically the section on Verifiability and Accountability– with regard to the provision of mechanisms to enable voter verifiability.

It is our opinion that the Draft Recommendation already sets fairly high security levels for e-voting. Our aim in this document is to enhance or develop some aspects that we believe can be further strengthened, with the goal to reach even more secure and trustworthy e-voting systems. We do not propose major changes to the original text, but a number of additions that in some cases are already implicit in the current text.

Broadly speaking, our contribution consists of:

- Introducing the capability of voter verifiability.
- Introducing the requirement of secrecy of intermediate voting results as a Technical Requirement and not just as an Operational Standard.
- Reinforcing the protection of the democratic process from internal attackers (i.e. technical personnel with privileged access to the e-voting system). We believe that not only the communication network used to transport votes, but the voting system used to collect and store those votes has also to be considered as a hostile environment subject to manipulation –in particular by internal attackers–. Malicious actions in the voting system by technical personnel should not threaten the integrity of the results or the privacy of voters.
- Enhancing the auditing capability.

Detailed comments on security and audit in e-voting

Our comments refer to sections D (Security) and E (Audit) of the Appendix III (Technical Requirements) of the Draft Recommendation. Some of the comments introduce a new Requirement, while some other comments develop/enhance an existing Requirement. The comments are presented following the same structure of sections used in the Draft Recommendation. In total there are 9 comments presented in this document, which have been numbered by using Roman numerals to avoid confusion with the numbering of Requirements used in the Draft Recommendation.

Section D: Security

General Requirements

I. We suggest the creation of a new Requirement demanding that "*Technical and organizational measures shall be taken to ensure that neither technical personnel nor any authority, or collusions of them, with privileged access to the e-voting system do not pose any risk to the privacy of individual voters or to the integrity of the voting results*". Although this is somehow already implicit in some of the existing Requirements, we believe that it has to be made explicit given the extraordinary importance of the assertion in the context of e-voting.

II. Following the previous argument, we suggest to enhance the Requirement 18 by adding that "*… confidentiality … shall be maintained, even in the case that technical personnel with privileged access to the e-voting system keep a record of the identities of voters and/or of the source addresses of the voters' connections as these cast their votes*".

Requirements in the Voting Stage

III. Adding to the Requirement 34, we suggest the creation of a new Requirement demanding that "*The fact that a vote has been originated by a voter eligible to vote shall be ascertainable*". The objective of this new Requirement is to allow auditing every single vote with complete confidence at any time, therefore preventing technical personnel with privileged access to the e-voting system from casting bogus votes on behalf of abstaining voters.

IV. We suggest adding to the Requirement 35 that "*… the electronic ballot box. It shall not be possible to eliminate or tamper with sealed votes, even by technical personnel with privileged access to the e-voting system.*" The objective of this addition is clear on its own.

V. We suggest the creation of a new Technical Requirement demanding that "*Intermediate voting results shall be secret to anyone before the proper election authorities have tabulated the votes.*" The objective of this new Requirement is to prevent privileged personnel from leaking information regarding the evolution of the voting with the aim of influencing in some way the behavior of voters who have not voted yet. The Draft Recommendation already sets an Operational Standard (number 18) that suggests this. However, we go further by making it technically impossible, even for privileged personnel and even after the closure of the electronic ballot box, to know intermediate results before the proper election authorities have tabulated the votes.

Section E: Audit

General

VI. We suggest the creation of a new Technical Requirement demanding that "*Audits focused on the accuracy of the voting results shall be based on audit data that cannot be manipulated*". Again, the objective is to prevent privileged technical personnel from being able to tamper with the results.

Monitoring

VII. In line with previous comment II, we suggest adding to Requirement 46 that "… *voter anonymity at all times, even if a record was kept that enables to correlate any single vote in the electronic ballot box with the identity of the originating voter*".

Verifiability

VIII. We suggest strengthening the Requirement 47 by adding that "… *and proving all counted votes are authentic, have not been manipulated, have been cast within the prescribed time limits, and all votes have been counted*".

IX. The lack of transparency of e-voting may cause the electorate to feel uncomfortable as they are dealing with a “black box”. Third party audits may not completely solve this. Therefore, we believe that additional mechanisms have to be introduced to allow also verifiability by voters themselves. The Legal Standard number 14 of the Draft Recommendation already requires that “*The e-voting system shall indicate clearly to the voter the fact that the vote has been cast successfully and the fact that the whole voting procedure has been completed*”. Still, we go a step further by suggesting the creation of a new Technical Requirement demanding that “*Technical and organizational measures shall be taken to ensure that every voter can verify that his or her particular vote has been delivered, totally unmodified, to the corresponding electoral board members or election officials, and that the vote has been taken into account by them for the counting process. These measures shall not be usable by the voter to prove what he or she voted for, in order to prevent allowing or easing vote-buying and/or coercion*”.

We believe that the voter has not only to be informed that his or her vote has been successfully submitted to the e-voting system but also has to gain absolute assurance that his or her vote has been delivered by the e-voting system to the corresponding electoral board members or election officials. This assurance can only be gained after the votes have been tabulated by the election officials, and it ensures that e-voting systems will be at least as reliable and secure as current voting methods.

It is very important to note that the suggested new Requirement does not represent a conflict with the Operational Standard number 16, which states that “*A remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast*”. The latter statement of the new Requirement mandates the compatibility of voter verifiability with the lack of proofs that could be used for vote-buying and/or coercion.

Conclusions

The Multidisciplinary Ad Hoc Group of Specialists on Legal, Operational and Technical standards for e-enabled voting, assembled by the Council of Europe, has released a final Draft for its Recommendation of the Committee of Ministers to member states on legal, operational and technical standards for e-voting. The Draft Recommendation sets out a number of legal, operational and technical standards for the correct adoption of e-voting in public elections and referendums in Europe.

We believe that the Draft Recommendation is an excellent work that contains correct and adequate standards. The Draft Recommendation sets fairly high exigency levels to the security of e-voting. Still, we believe that some aspects can be further enhanced, developed or made more explicit. In particular, we suggest the introduction of voter verifiability in the manner presented in this document, with the objective to increase voter confidence in e-voting.

This document has presented a total of 9 comments on the Technical Requirements of the Draft Recommendation, specifically on the Security and Audit sections, with the aim of further strengthening the security, trustworthiness, audit, and privacy levels of e-voting systems. The final objective is to achieve a level of security in e-voting systems fully comparable to the one in conventional voting systems.

About the author

Andreu Riera initiated academic research on e-voting security in 1995, accomplishing an extensive list of publications in international scientific publications and book chapters. His PhD Thesis “Design of Implementable Solutions for Large Scale Electronic Voting Schemes” was published in 1999. He has coauthored six international patent applications, three of which refer to technical models to bring confidence to e-voting systems. He has also carried out numerous communications on security for e-voting in conferences and seminars in several European countries. He also advised the Spanish Senate on the correct implementation of e-voting referring to security aspects.

In 2001, Mr. Riera founded Scytl Online World Security S.A. (Scytl)[2] as a spin-off of his academic research group on e-voting security. The research activity of the group was initially funded by the Spanish Ministry of Science and Technology and over 6 years it generated more than 20 scientific papers that were presented in international conferences and journals. The group also produced the (still today) only two European PhD Thesis on security systems for remote e-voting. Additionally, the leading research group developed a practical prototype that was used in 1997 to conduct the first Internet-based binding elections in Europe (for the presidency of the IEEE IT Spanish Chapter).

Leveraging all this expertise, Scytl’s R&D team has created ground-breaking security software that ensures privacy, integrity and verifiability in e-voting systems. This unique software, which has already been successfully implemented in several official e-voting platforms in Europe, allows fully complying with the security and audit standards set out by the Council of Europe’s Draft Recommendation and including also the additions and comments suggested in this document.

[2] http://www.scytl.com