

Contract number: IST-1999-20338

Project Acronym: An Innovative Cyber Voting System for Internet Terminals and Mobile Phones

Project Name: CyberVote

Project Logo:



Project abstract:

CyberVote, "an innovative cyber voting system for internet terminals and mobile phones", is a research and development (RDT) project being funded by the European Commission, with additional funding from the companies and organisations undertaking the work. It is part of the Information Society Technologies (IST) 1999 programme for research, technology development and demonstration under the fifth framework programme (5th PCRD). It is attached to Key Action "Systems and Services for the Citizens".

The goal of CyberVote is to develop and demonstrate the first highly secure cyber-voting prototype using mobile and fixed internet technologies. The project will define and implement a CyberVote prototype embedding an innovative voting protocol relying upon the use of advanced cryptographic tools that will be developed to ensure integrity, privacy and authentication of the voters. The project will also analyse the laws in force in the participating countries. The prototype will be tested during trial elections that will be held in Germany, France and Sweden. Further information can be found on the Web site of the project: <http://www.eucybervote.org>

List of Key Words:

Internet voting, Internet-based voting systems, Internet terminals, mobile phones, cryptographic protocol, security, public election legislation, democratic process, on-line democracy, e-voting, authentication, citizen, e-Government.

1 MAIN OBJECTIVES

The goal of the CyberVote project is to develop and demonstrate an on-line voting system integrating a highly secure and verifiable Internet voting protocol, and designed to be used at local, regional, national or European elections.

The project will analyse the laws in force in the participating countries in order to identify the requirements the system shall meet but also to study possible amendments to allow its use in the legal framework in Europe.

This system will allow voters to cast their vote through the use of Internet terminals such as PCs, handheld devices and mobile phones. It will rely upon an innovative voting protocol, designed within the project, that uses advanced cryptographic tools. This protocol will ensure authentication of the voters, integrity and privacy of their vote when sending it over the Internet and during the vote counting and auditing process.

This system will be tested in 2003 during trial elections that will be held in Germany, France and Sweden. These trials will involve more than 3000 voters and will allow full assessment of the system before any potential product launch.

1.1 SOCIAL OBJECTIVES

This project aims to achieve an improvement of the democratic process by increasing voter participation and thereby increasing the number of votes. On-line voting should lead to an increase of citizens taking part in numerous types of elections.

The project will evaluate to what extent on-line voting influences voter participation. CyberVote should improve the voting process for all voters, but examples of citizens who should particularly benefit from CyberVote include people with limited mobility (the disabled, the ill, hospital patients, the elderly, etc.), people travelling during the election day, and expatriates. The system will satisfy their requirements by allowing them to cast their vote without the need to go to their usual polling station. However, voters will still have the option to vote via the usual paper procedure.

This system relies upon a flexible and innovative approach. It will facilitate an increased and equal participation in democratic processes. It will likely lead to a substantial cost reduction in the electoral process for both the citizens and the affected administrations. It will emphasise the transparency in a convenient and user-friendly approach.

CyberVote will be simple to use, accessible and affordable for all voters and candidates.

1.2 SECURITY

CyberVote will allow the voters to cast their vote in total confidentiality by preserving their privacy during the whole voting procedure.

As this goal cannot be achieved by a simple combination of off-the-shelf cryptographic primitives, special-purpose cryptographic protocols will be used to implement this unique set of security properties. The fundamental problem addressed involves the simultaneous fulfilment of absolute ballot secrecy and full auditing possibility of the voting system.

1.3 TECHNOLOGY

The implemented system will offer on-line voting through different kinds of Internet access. It will allow voters to use commercially available equipment (PCs, handheld devices or mobile phones) or existing public equipment (self-service Internet access terminals, Internet booths, polling station equipment, etc.).

1.4 MEASURABLE RESULTS

In terms of quantifiable and measurable results, the project will deliver the following results:

- a CyberVote prototype of an e-voting system working according to selected user requirements. It is anticipated that:
 - administrations will require a usage cost less than 3 €/ election / voter (e.g. 30 000 €for an election involving 10 000 voters)
 - voters will require a usage cost less than 1 €(e.g. communication costs).
 - administrations will require an equipment cost less than 1 €/ voter (e.g. 10 000 € of equipment for 10 000 voters)
 - voters will require an equipment cost less than 15 € for each voter (e.g. specific equipment to buy for voting).
- a CyberVote prototype performing as advertised (e.g., counting the ballots correctly)
- a CyberVote system verifiable without compromising ballot secrecy providing a basis for certification of the voting system by government bodies.
- A CyberVote system reliable and robust to handling trial election loads (communication, volume, etc.) without losing one vote.
- a CyberVote system architecture allowing voters to cast votes from a wide range (at least one PC, one mobile phone and one other device) of user-friendly platforms and devices.

- 3 trial applications using the CyberVote system involving each time more than 1000 voters;
- an evaluation report of the trial applications showing a 80 % satisfaction rate of both administration project end-users and trial voters.

2 KEY MILESTONES

The CyberVote project officially started on 1 September 2000 and will end in March 2003.

The various milestones of the project are as follows:

- Milestone 1: definition of the overall system architecture (31/07/01).
- Milestone 2: CyberVote prototype version 0 (28/02/02).
- Milestone 3: CyberVote prototype version 1.0 (15/10/02).
- Milestone 4: demonstrations of the trial applications (28/02/03).
- Milestone 5: final report (28/02/03).

3 MAJOR INNOVATIONS

3.1 STRONG AND HIGHLY SECURED CRYPTOGRAPHIC PROTOCOLS

A first goal of the CyberVote project is to design and test a voting system for which the underlying cryptographic protocols fulfill a rich set of security properties. In particular, it is required that the voting system is universally verifiable, which means that any party can verify that the election result actually corresponds to the encrypted votes cast during the election and furthermore that ballot secrecy is controlled by a set of talliers of any size deemed appropriate. That is, ballot secrecy is not necessarily dependent on a small, fixed number of parties but can be scaled to any desirable number of parties. We call scalable distributed trust. Hence, among other things, the underlying cryptographic protocols are designed to satisfy the seemingly conflicting requirements of universal verifiability and ballot secrecy.

The cryptographic strength of the CyberVote system will thus be much higher than of all of the other Internet-based voting initiatives except for the products by VoteHere.net (and the prototype used in the InternetStem project) which target the same set of security properties as the CyberVote project. Clearly, good overall security of the election system is not simply guaranteed by the strength of the underlying protocols, but weaknesses in

these can never be compensated for by additional security measures. Any appropriate state of the art security measures will be applied to achieve good overall security of the CyberVote system.

3.2 USE OF MOBILE PHONES AND MOBILE INTERNET TERMINALS

A second goal of the CyberVote project is to extend the platform for voting clients from PCs to other networked devices such as mobile phones, smartphones and possibly TV set-top boxes. Availability of voting clients on these devices will provide greater convenience to the voters. Some of the challenges are to implement the above mentioned cryptographic protocols, which require large-integer arithmetic, and to find suitable user-interfaces for these constrained devices. An important part of the CyberVote effort will be devoted to these issues.

3.3 ASSISTANCE IN THE DEVELOPMENT OF NEW PUBLIC ELECTIONS LEGISLATION

Finally, a third goal of the CyberVote project is to take legal issues for binding, public elections into account. While private elections allow for considerable freedom, the rules for public elections are generally much more stringent. Also, the goal is to make the CyberVote system compatible with the rules of several countries at the same time, rather than limiting the scope to a single country. For example, compulsory voting may be supported by the CyberVote system, although it is not a requirement in every country. Further, the interaction between the CyberVote project and legislative bodies is supposed to be bidirectional, that is, the CyberVote project tries to match current and emerging requirements for voting systems and, at the same time, the CyberVote project tries to assist the development of new legislation pertaining to Internet-based voting systems.

4 EXPECTED BENEFITS

4.1 CONTRIBUTION TO A EUROPEAN DEMOCRACY

A major obstacle for a common European democracy is the fact that Europe is a grouping of different nations, different cultures and individual communities who are living in a broad common legal and economical framework. To make them feel as “European citizens” with equal European civil rights, electronic democracy is one important mean to bring Europe closer to its citizens. The past has shown that most of the EU citizens feel far away, not concerned or even excluded from European decision making processes. As a result the general rate of participation in European elections is quite low. “Democracy requires that people have the ability to move from discussion to action, from participation to power.” (Steven E. Miller, author of *Civilizing Cyberspace: Policy, Power, and the Information Superhighway*, Addison Wesley, 1996). By bringing the European voting place to the citizens’ homes, the CyberVote system is an important step towards a European Agora where democracy is easy to realize - an aspect which becomes even more important in view of the progressive extension of the European Union.

4.2 EUROPEAN ADDED-VALUE

In an effort to enhance the quality of political debate in Europe, the project aims to promote the use of communications technology by:

- providing assistance to European State Members and their authorities to take up the new communications technologies,
- encouraging the executive arm of local, regional, national governments to publish more material on the Internet and to accelerate the uptake of new communications technologies,
- encouraging individuals and groups (included handicapped people, patients, people with mobility reduced, disadvantaged and elderly people) to use the new technologies to enhance their participation in the democracy process and to claim their civil rights,
- promoting a robust and autonomous civil society in Europe.

4.3 IMPROVING THE ACCESSIBILITY, RELEVANCE AND QUALITY OF PUBLIC SERVICES

By giving citizens new forms of voting, the project will enhance the civic involvement in the political process. It should increase the odds of any individual citizen actually making a difference. For example, instead of physically going to the polls, people could vote from their home or from any other places. It will be more convenient and less expensive. Finally, government deliberation will be more accessible to everybody.

4.4 HELPING DISABLED, ELDERLY AND IMMIGRANTS

It is critical that these people with their special needs are able to participate in the political life and democratic processes. One of the major concerns for people with disabilities, elderly citizens and immigrants is their social exclusion and isolation. The impression of being excluded from the social and political life often leads to resignation, and discouraged by the physical efforts they have to undertake to participate in polls and elections, they do not claim their civil rights and do not vote. By overcoming the barriers imposed by time, distance, or disability, the CyberVote system enables these people to connect easily to the outside political world. Furthermore, designing a project keeping in mind disabled and elderly citizens, ensures an increased user friendliness for all citizens.

4.5 DATA SECURITY, DATA PROTECTION AND PRIVACY FOR INDUSTRIAL APPLICATIONS

The project aims to improve democratic processes, namely its related voting processes, by introducing a system which enables citizens to vote electronically in every kind of elections. It is obvious that such a system requires the highest degree of data security, data protection and privacy. In fact, these three aspects are actually of great relevance for the development of many other industrial applications using Internet and new

communications technologies. In this context e-commerce, one of the fastest growing application areas on the web, has to be mentioned. Therefore, when developing practical and reliable solutions for the CyberVote system, these results will be at the same time of highest interest for other applications, where data security and protection is needed.

5 TARGET MARKETS

The primary results expected from the CyberVote project are grouped into five categories:

- **Engine for advanced electronic voting protocols:** The engine is the core implementation of the main security functionality required for highly secure electronic voting systems. The engine will be incorporated into voting clients and servers. The primary mode of exploitation for the engine therefore is to make secure electronic voting protocols accessible to system integrators (both within CyberVote and outside) in a convenient manner. The result will also be disseminated by publishing the CyberVote architecture and protocols in appropriate conferences and journals.
- **Electronic voting client on a mobile phone platform:** The voting client on a mobile phone platform will be built around the client part of the voting engine (see above). The primary mode of exploitation of this result is to enhance the value of a smartphone platform by enabling its use in electronic voting.
- **Electronic voting systems:** This result refers to the voting system as a whole, consisting of servers, as well as clients on various types of platforms. The primary mode of exploitation is the use of these systems in the organisation and management of both public and private sector elections.
- **Academic results:** New proposals for security-critical protocols and systems must be widely disseminated among experts so that they can be publicly scrutinised and evaluated. This is the standard practice in cryptography and security research communities. Electronic voting also breaks new ground in terms of its legal and political aspects.
- **Trials:** A result of planning and conducting the CyberVote trials will be the knowledge and experience on secure electronic voting in a variety of contexts. This result has three potential uses. It will serve as valuable feedback to the designers of electronic voting systems. Trial partners may use it as a basis for future deployment of secure electronic voting in their cities. They will also disseminate the result to members of the CyberVote Special Interest User Group (CSIUG) as well as fellow members in other fora like the Global Cities Dialogue.

Each type of result is addressed to a different market segment. Here we provide only a brief list.

- Organisers of elections constitute the market segment interested in electronic voting systems. Also, they constitute the target group for the dissemination of know-how

acquired during the trials process. This includes governments at various levels, market research organisations, clubs and associations etc.

- Software and hardware developers, and system integrators constitutes the market segment for the electronic voting engine.
- Researchers in the industry and academia constitute the primary market segment for academic results.
- End users who are eligible to vote in one or more elections constitute the market segment for electronic voting clients on different platforms.

6 LIST OF PARTICIPANTS

Industrial partners:

- EADS Matra Systèmes & Information of France, <http://www.matra-msi.com>
- Nokia Research Centre of Finland, <http://www.nokia.com>
- British Telecommunications of the United Kingdom, <http://www.bt.com>

University partners:

- K.U.Leuven Research & Development of Belgium, <http://www.kuleuven.ac.be/kuleuven/>
- Technische Universiteit Eindhoven of The Netherlands, <http://www.tue.nl>

Users partners:

- Freie Hansestadt Bremen of Germany, <http://www.bremen.de/info/statistik>
- Mairie d'Issy-les-Moulineaux of France, <http://www.issy.com>
- Kista Stadsdelsnämnd of Sweden, <http://www.kista.com>

7 CO-ORDINATOR CONTACT DETAILS

Stéphan BRUNESSAUX

EADS Matra Systèmes & Information - BP 613 - F-27106 Val de Reuil Cedex

Phone: +33 2 32 63 40 55 - Telefax: +33 2 32 63 42 00

Email: sbrunessaux@matra-ms2i.fr or contact@eucybervote.org

Web : <http://www.eucybervote.org>