

GI, the Gesellschaft für Informatik, publishes this series in order

- to make available to a broad public recent findings in informatics (i.e. computer science and information systems)
- to document conferences that are organized in cooperation with GI and
- to publish the annual GI Award dissertation.

Broken down into the fields of "Seminars", "Proceedings", "Monographs" and "Dissertation Award", current topics are dealt with from the fields of research and development, teaching and further training in theory and practice. The Editorial Committee uses an intensive review process in order to ensure the high level of the contributions.

The volumes are published in German or English

Information: <http://www.gi-ev.de/service/publikationen/lni/>

The 2006 conference on Electronic Voting took place in Castle Hofen near Bregenz at the wonderful Lake Constance from 2nd to 4th of August. This volume contains the twenty papers selected for the presentation at the conference out of more than forty submissions. To assure scientific quality, the selection was based on a strict and anonymous review process. The papers cover the following subjects: e-voting experiences, social, legal, political, democratic and security issues of e-voting, as well as solutions on how to (re)design election workflows, and finally how to implement and observe electronic voting systems.



Robert Krimmer (Ed.): Electronic Voting 2006

P-86

GI-Edition

Lecture Notes in Informatics

Robert Krimmer (Ed.)

Electronic Voting 2006

2nd International Workshop
Co-organized by Council of Europe,
ESF TED, IFIP WG 8.5 and E-Voting.CC

August, 2nd – 4th, 2006
in Castle Hofen, Bregenz, Austria

Proceedings



The Voting Challenges in e-Cognocracy

Joan Josep Piles¹, José Luis Salazar¹, José Ruíz¹, José María Moreno-Jiménez²

¹Grupo de Tecnología de las Comunicaciones
Universidad de Zaragoza
María de Luna, 1
50018, Zaragoza, España
{jpiles | jsalazar | jruiz}@unizar.es

²Grupo Decisión Multicriterio Zaragoza
Universidad de Zaragoza
Doctor Cerrada, 1-3
50005, Zaragoza, España
moreno@unizar.es

Abstract: e-Cognocracy[MP03, MP05, Ker03] is a new democratic system that focuses on the creation and social diffusion of the knowledge related with the scientific resolution of high complexity problems associated with public decision making. Using multicriteria decision making techniques as the methodological aid, the democratic system as a catalyst for the learning that guides the cognitive process distinctive of living beings, and the Internet as a communication support, e-cognocracy resolves some of the limitations of traditional democracy and provides room for greater involvement of the citizenry in their own government. In this sense, e-voting is not limited to the choice of a given political party, but to the extraction of the relevant knowledge.

Even though e-voting systems have already been widely studied, there are still some situations not covered yet by classical bibliography, and then it becomes necessary to introduce interesting variations to the main schema. In this paper, we will present one of such occurrences (that associated with e-cognocracy), and will study the modifications needed in the traditional e-voting processes as well as the implications they have.

1 Introduction

The degree of implication of citizens in their own government has traditionally been the issue which has led to most political changes throughout history. It has been traditionally agreed that it is desirable to achieve as much involvement as possible. This involvement should be only limited by what is practical for the smooth operation of the institutions.

This has been usually limited by the access of the citizenry to the relevant information, due to the lack of both education and readily access to the critical information. However, in the last years, with the advent of computers, the information flow between people has been steadily increasing. Internet is responsible for a great deal of this new communication, and it is being widely used by the very same citizens who will elect their leaders.

It is only natural, then, that technology has evolved to assimilate this new method of exchanging information into the classical structure. Thus, electronic voting, or e-voting, was born. However, there have been no shifts in the paradigm of the decision making process, although various different proposals have been made.

One of the obstacles these methods have is the lack of technologic means to allow their implementation. We introduce here one tool to allow one of these novel ideas, e-cognocracy, to be taken to reality.

In section 2 we will introduce e-cognocracy and its main differences with other e-voting schemes. Section 3 provides a description of our proposed voting system, as well as a proof that it satisfies the requirements for its use in e-cognocracy. We offer in section 4 the details of our implementation and actual deployment of the system. Finally, in section 5 we provide the final considerations and future job within this project.

2 From e-democracy to e-cognocracy

Although Western societies have mainly opted for the "democracy" in their governance systems, in recent years there has been increasing discussion of a certain democratic fallacy, because this form of representation no longer meets its initial end, which is of course the participation of the citizens in their own government. Thus, many voices have been raised demanding greater involvement of the citizenry in the governance of society[Rob04]. One of the proposals suggested to improve this participation of citizens is e-cognocracy[MP03, MP05, Mor06]. It is a new democratic system employed to create a new, more open, transparent, civilized and free society that is at the same time more cohesive and connected, and more participative, equal and caring.

e-Cognocracy not only provides room for greater involvement of the citizenry in their own government and resolves some of the limitations of traditional democracy, but it also focuses on the process by which knowledge related with the scientific solution of problems is created and socialised. To this end, it uses multicriteria decision making techniques as the methodological aid, the democratic system as a catalyst for the learning that guides the cognitive process distinctive of living beings, and the Internet as a communication support.

Among the many tools needed to fully develop e-cognocracy, we will focus in e-voting, as it is the first needed to gather the information supplied by the citizens. Most known e-voting processes are limited to the technological aspects associated with the choice of a given party. However, e-cognocracy is focused on the extraction of the relevant knowledge, including the analysis of the individual and social learning derived from the scientific resolution of the problem, and this new orientation requires new technological features[Lot03, RH03].

From the point of view of the voting process, the key element introduced by e-cognocracy is the linkability of votes. In a traditional voting system, whenever the citizenry is asked to be part of a decision making process, a voting process begins.

This process starts with an information gathering phase. In it, each citizen is given the maximum amount possible of information from each of the interested parties (typically, political parties). This usually lasts for several weeks, in order to let every citizen get as much information as possible.

During that period there is very little feedback (if any) from the citizens who will partake in the votation. There are polls designed to get an idea of the actual tendencies, but they affects a very small percentage of the electorate. This, in turn, leads to a lost of interest, as the only really important moment is the voting itself.

In order to get the knowledge seeking process, we divide each votation in several rounds. Each voter can cast his vote in as many rounds as the voting process determines (but only once each round). After each round partial results are published, and more information is provided to the citizens.

For the actual results of the votation, only the last vote cast by a citizen is taken into account. However, all the history of different votations is preserved associated to the vote but not to the voter. This way, there is some information available about the trail each person followed until he arrived to his final decision.

Individual trails are never published, as they could compromise the secrecy of the voter. For instance one could be paid to vote first A, then B, then C and finally D. As the amount of rounds increases, the number of possible combinations becomes big enough to be relatively sure that only one person followed one given track. However, those trails give very valuable information which can help to detect the causes of the changes in opinion (e.g. not only that people switched from A to B, but also that most people switched after a certain event).

Also, people are encouraged to discuss their views in open forums, either anonymously or with an identity, and the effect of those discussions can be linked to the swings in the opinion of the voters.

2.1 Characteristics of our e-voting system

Our e-voting system is born as a tool for e-cognocracy and it has the following properties, sharing some of them with classic e-voting systems[BT94, CC96]:

Precision

- It shall not be able for a non authorized person to modify any votes (that is, only each voter can cast its vote).
- It shall not be possible to remove a valid vote from the final counting.
- It shall not be possible to include a non-valid vote in the final counting.

Democracy

- Only voters in the census shall be able to vote.
- Each voter shall be able to vote only once in each round.

Privacy

- A voter shall not be linked to its vote.
- A voter shall not be able to prove its vote.
- Verifiability
- Voters shall be able to verify that their vote has been correctly accounted.

Linkability

- Two votes from the same voter in different rounds of the voting shall be linked together, but not to the voter who cast them.

3 Our e-voting system

3.1 Actors in the voting process

Voter (V): Each voter must show its preferences in a multi-choice question, and rank them numerically. For each round of the voting the census shall be constant.

Certification Authority (CA): The Certification Authority shall issue the public/private keys and certificates for each actor involved in the process, and will serve as Trusted Third Party with regard to the validation of certificates.

Database server for the Electoral Authority (DBEA): The data shall be kept in a database in a secured location, without public access.

Recount server (R): The Recount server is the only entity allowed to decrypt the votes. The Electoral Authority shall provide information enough to link the votes from the same voter, but not to track them to the actual person who casted them.

Electoral Authority server (EA): The Electoral Authority shall keep track of the census, validate the users in the voting process, and sign their votes as a proof of voting. It shall also keep enough data about the votes to know the hash of the last vote from a voter (in order to link them for the Recount server) but without actually being able to decrypt them.

In this schema it is assumed that both the Electoral Authority and the Recount server do not work together to break the system and are trusted by each other and by the users. However, this is a reasonable assumption for most cases.

3.2 Initialization

The first part of the voting process is the initialization of the actors involved. In order to keep security, both the recount server and the electoral authority shall get a new key pair and certificate each voting. If desired, the keys for the voters can also be reset, though that's not necessary.

CA Initialization. The CA shall initialize only once before the start of any voting process. It shall do so by self-signing a certificate for itself and distributing it to the involved parties so that successive certificates may be trusted referring them to it.

R's private key initialization. The Recount server must decrypt all the casted votes with its private key. To avoid possible power abuses from a single owner of this key, it is possible to split it in different shares, so that a single person has not access to the voting data without coordination and acceptance.

EA's private key initialization. The Electoral Authority shall get a certificate and a key pair in order to do the blind signatures of each vote, which shall be kept by each voter as a proof of voting. It shall generate a census with the public keys of the persons allowed to vote.

Voters' registry. The Certificate Authority shall issue a new certificate and key pair to each voter who didn't have one yet, in order to be included in the census.

3.3 Voting

1. Voter makes his choices and saves the possible vote as a "voting intention" (this intention has no value as witness at all, as one could save as many of these "intentions" as desired without actually voting).
2. Voter encrypts the vote with R's public key.
3. Voter identifies himself to EA and sends it a hash of his vote for EA to issue a blind signature of it, and a ticket made from a mix of his identity and a random value that will be signed by EA as well.

4. EA verifies the voter's identity, checking it against the census and validating the client's certificate, and checks that the voter has not already cast its vote in this round.
5. EA issues a blind signature of the vote, and a signature of the ticket, and stores them linked to the voter for future rounds.
6. Voter sends to EA the vote and the blinding factor for the blind signature ciphered for R.
7. EA sends to R the ciphered vote and secret with the blind signature of it and the signature of the ticket via a secure channel.
8. If the voter had previously voted (in other rounds), EA sends to R a copy of the blind signature of the latest vote, which will be then used by R to link them.
9. EA sends to V the signature of the ticket to prove that his vote has been stored.

3.4 Recount

1. R makes public the signatures of the tickets, and starts a claims period before the publication of the results.
2. R decrypts the original votes, and uses the secret included with it to get a valid signature from the blind signature.
3. R checks the vote with the signature obtained and verifies that it is correct.
4. R links all the votes from the same voter.
5. R publishes the results of the round/voting.

3.5 Proof of fitness for e-cognocracy

In order to be used within the frame of e-cognocracy, our voting system must satisfy all the conditions previously imposed.

Precision

- As each voter authenticates himself to EA, this implies he must have a knowledge of the private key that is impossible to fake provided we use an adequate key length.
- As each voter gets a signature of the ticket he sent to EA, and a list of those tickets is published prior to the recount, even if R is compromised, the votes cannot be erased from the ballot, as such an action would be challenged by the voters with their tickets, which would be shown to exist in EA.

- Each vote is stored with a signature from EA. A vote cannot be inserted even if R is compromised because it would be necessary to get a valid signature, and that is not possible without the private key of EA.

Democracy

- As the votes are not sent directly to R by the users, it is EA's job to get sure that the voter is properly included in the census.
- Analogously, EA will store which voters have already voted in each round, to avoid duplicates.

Privacy

- All the information provided to R is a ciphered vote, its blind signature, and a signed ticket. None of these includes anything that could lead to track the individual who casted the vote.
- The only item a voter receives is its signed ticket. That ticket is generated randomly, and has no relation whatsoever with the actual content of the vote.

Verifiability

- Each time a vote is received, EA sends back to the voter a signed ticket. Later, when the recount starts, the list of the tickets from the votes casted is published. If a voter had a ticket not included in the list, he could use it to challenge EA and see whether it has a copy of it. If EA has a copy, then the vote should be cast again.

Linkability

- Together with each vote, EA sends to R the blinded signature of the last vote casted by the same person. At the time of the recount, R looks for each vote the one which blind signature matches the included with the vote, and it reconstructs this way all the links which allow to trace the voting history of a voter, without actually revealing his identity.

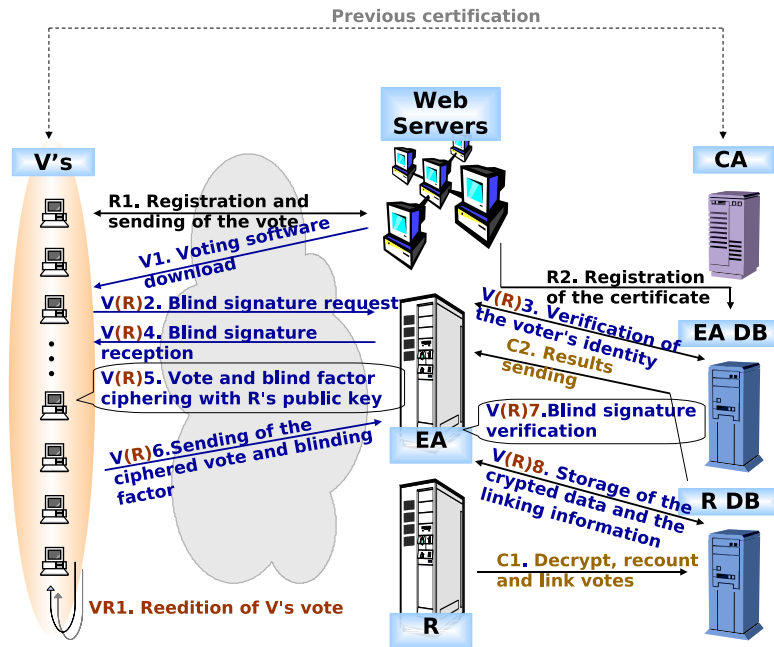


Figure 1: Overview

4 Implementation details

In order to implement the e-voting protocol, it has been chosen to use JAVA technologies, both in the client side and in the server side. This has several advantages:

- Better communication between the different components.
- More code reusability, as we can develop a series of cryptographic libraries which will be used both by the client and by the server software.
- Easy integration with the browsers.

In order to minimize the number of configurations in which the client side had to run, we decided to choose a standard web browser. In this case, it was selected Mozilla Firefox as the reference browser. It has the advantage of being open source, so its source code is readily available, contributing to increase the feeling of transparency in the process.

The browser has been completed with some libraries (JSS), needed to be able to access the client certificates which are stored in it from within the JAVA applet that will be the client software. If those libraries were not available, the user should manually add the client certificate and the CA to the JAVA application.

The application server to use will depend on the available infrastructure at the moment of the deployment. In our tests, we used Tomcat as application server. It is open source as well, and its capacity for this kind of systems is well proven.

It was chosen to use MySQL as a backend to store the data related to the votings (both the actual votes -ciphered and clear-text after the recount- and the information about the votings -question of the voting, number of rounds, period of time for each round...).

As there are two different servers (Electoral Authority server and Recount server), there could be two web and application servers, working with two different database servers. None the less, when doing the actual deployment it might happen that it is advisable to put both applications in the same application and/or web server. Likewise, it could be desirable to use two databases in a single database server. This would not be a problem, but it should be taken into account that should the server machine be compromised, the whole voting and recounting system would be broken.

All the communications between the client and the server will be both authenticated and encrypted. To achieve these goals, it will be necessary to set up an infrastructure allowing SSL and client side certificates.

4.1 Deployment details

Our group carried out a deployment of a test voting system. None the less, any future deployments should take into account that the specific details will depend on the available resources. This will be much more important if, as it usually happens, the servers are shared with other applications. The implications for the security of the system must be studied on a case by case basis.

Regarding the choice of software, we used Apache as the webserver and Tomcat 5 as application server, both of them running in LINUX i386 machines. As this was a proof of concept, the system load was expected to be very low. This allowed us to consolidate both services (the Certificate Authority server and the Recount server) within the same Tomcat instance. Likewise, both databases were stored in a single MYSQL server which was executing in the same machine with Apache and Tomcat.

There are several options available to link Apache and Tomcat. The simplest way is running two independent servers listening in different ports (in fact, it would even be possible to have them running in different machines, should the need arise). Notwithstanding this, we chose to use a tighter integration between them using the JK Connector. This technology allows to redirect queries that would normally be answered by the Apache server towards the Tomcat application server, in a way that is transparent for the user.

However, this choice makes the Tomcat application server unaware of the underlying SSL layer, because the web server forwards the request to the application server, but not the environment and security layer data. Even though the voting system cannot obtain the client certificate from the SSL layer, our protocol allows for the certificate to be sent by the client in case the server is not able to directly retrieve it.

In order to generate the certificates needed, we also set up a Certificate Authority using OpenSSL.

5 Conclusions

We have studied the novel challenges that e-cognocracy imposes upon traditional voting. We have built an e-voting system which provides the means to gather the information needed towards a more participative democracy.

As we have seen, the key to get the linkability of the votes is the separation between the Electoral Authority, who can link the chain of votes to the user but can't know the contents of each vote, and the Recount server, who can link the votes between themselves and decrypt them, but is isolated from the information about each voter.

This isn't a concern as long as both of them are trusted entities who will not work together to cheat the system.

We have also built and tested such a voting system, showing that it is feasible and that its ease of use allows for it to be widely used without any special kind of technical background.

Our future work includes developing other technological tools needed by e-cognocracy. As e-voting provides the raw data, there is still the need for a set of tools which can link the information obtained to the actual social phenomena that helps to form the results obtained in the votation. These tools includes online forum where people can exchange ideas in a controlled way, and the tools needed to extract the relevant or prevalent opinions and match them against the shifts in the voters' opinion.

6 Acknowledgements

This work has been partially funded under the research projects "Electronic Government. Internet-based Complex Decision Making: e-democracy and e-cognocracy" (Ref. PM2004-052) and "Internet-based Complex Decision Making. Decisional Tools for e-cognocracy" (Ref. TSI2005-02511).

References

- [BT94] Benaloh, J. and Tuinstra, D. Receipt-free secret-ballot elections (extended abstract). In STOC '94: Proceedings of the twenty-sixth annual ACM symposium on Theory of computing, pp. 544–553. ACM Press, 1994.
- [CC96] Cranor, L. F. and Cytron, R. K. Design and implementation of a practical security-conscious electronic polling system. Technical Report WUCS-96-02, Washington University, 1996.
- [Ker03] Gregory E. Kersten, G.E. e-Democracy and participatory decision processes: lessons from e-negotiation experiments. *Journal Multi-criteria Decision Analysis* 12(2-3), 127-143, 2003.
- [Lot03] Lotov, A. Internet tools for supporting of lay stakeholders in the framework of the democratic paradigm of environmental decision making. *Journal Multi-criteria Decision Analysis* 12(2-3), 145-162, 2003.
- [MP03] Moreno-Jiménez, J. M. and Polasek, J. M. e-Democracy and knowledge. a multicriteria framework for the new democratic era. *Journal of Multicriteria Decision Analysis*, 12:pp. 163–176, 2003.
- [MP05] Moreno-Jiménez, J. M. and Polasek, J. M. e-Cognocracy and the participation of immigrants in e-governance. In TED Conference on e-government 2005. *Electronic democracy: The challenge ahead*, volume 13 of *Schriftenreihe Informatik*, pp. 18–26. University Rudolf Trauner-Verlag, 2005.
- [Mor06] Moreno-Jiménez, J.M. E-cognocracia: Nueva Sociedad, Nueva Democracia. *Estudios de Economía Aplicada* 24(1), 559-581, 2006
- [RH03] Ríos Insúa, D., Holgado, J. and Moreno, R. Multicriteria e-Negotiation Systems for e-Democracy. *Journal Multi-criteria Decision Analysis* 12(2-3), 213-218, 2003.
- [Rob04] Roberts, N. Public Deliberation in an Age of Direct Citizen Participation. *The American Review of Public Administration*, 34(4):pp. 315–353, 2004.

