Computer Standards & Interfaces 32 (2010) 256–265

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Security approaches in e-cognocracy

José Luis Salazar [a,*], Joan Josep Piles [a], José Ruiz-Mas [a], José María Moreno-Jiménez [b]

[a] Grupo de Tecnología de las Comunicaciones, Universidad de Zaragoza, María de Luna, 1, 50018, Zaragoza, Spain
[b] Grupo Decisión Multicriterio Zaragoza, Universidad de Zaragoza, Gran Vía, 2, 50005, Zaragoza, Spain

ARTICLE INFO

Article history:
Received 31 January 2008
Received in revised form 23 March 2009
Accepted 23 January 2010
Available online 1 February 2010

Keywords:
e-cognocracy
e-voting
Cryptography primitives
Smart-cards
Trusted third parties

ABSTRACT

E-cognocracy is a democratic model focussed on the joint creation of Social Wisdom through the Internet by means of the extraction and diffusion of knowledge related with the scientific resolution of highly complex problems associated with public decision making. To this end, e-cognocracy allows for the consideration of several rounds during the resolution process. The linkability of votes, the intensity of preferences and the identification of the arguments that support choices, among other matters, require the design of a specific e-voting process the e-cognocracy, e-cognising. This paper presents various implementations of the technology, commencing with an initial proof of concept and going on to the use of smart cards to permit remote use of the system and influence the level of perceived confidence among users, eliminating the role of one of the confidence authorities formerly required to ensure appropriate system security.

1. Introduction

Philosophical, methodological and technological changes arising in what has come to be known as the Knowledge Society over the last twenty years are at the hear the generalised use of the Information and Communication Technologies (ICT) in Public Administration (e-Government). The rapid penetration of Internet in our lives offers wide scope for potential ICT applications of in both the private and public sectors. In the framework of e-Government, these applications range from straightforward e-administration services (information transmission and simple task execution) to complex systems related with e-participation, including in electronic proposals voting (e-voting), the drafting of public policies (e-governance), debate between citizens and political representatives (e-democracy) and, finally, the involvement of citizens in public decision making and the creation of a better society (e-cognocracy).

Where the nature of these services requires anonymity, as in the case of electoral processes, the technology must provide an appropriate answer to the challenges posed by security issues. No less important, institutions must enhance the trust and perceived security of electoral systems [26] if they are to allow effective use of public services by the citizenry and by institutions to reach the goal of a better society.

Our aim is to create a true "Social Wisdom". Then, we cannot ignore the fundamental role of citizen involvement or the need to encourage active participation in the process. This means avoiding the creation of technological barriers that might undermine the citizen's decision to take part. It is therefore not enough to implement a valid e-cognocracy system, and care must be taken to ensure that the application does not ringfence availability and usability. Interfaces and standards play a key role in this area.

On the one hand, then, it is necessary to adapt the communication interface for the system in line with user needs and facilitate secure access without foregoing any of the essential requirements (security, anonymity, confidentiality, etc.) for any electronic voting technology, or more specifically in this case, for an e-cognising consultation. The two key requirements may be resolved using smart cards, which provide portability and the necessary computational resources.

On the other, the cryptographic tools must not represent a barrier for the user. The goal, then, is to ensure that implementation is as far as possible compatible with existing standards and, where necessary, to create new standards that are capable of adaptation as efficiently and transparently as possible.

The linkability of votes, the intensity of preferences and the identification of the arguments that support choices are just some of the characteristics of e-cognising [17]. These features require the design of specific e-voting requirements, which we will address in the following sections [21].

Following this brief Introduction, the paper is structured as follows. Section 2 includes some background material about e-cognocracy and e-voting requirements from the point of view of security. Section 3 presents the initial approach (proof of concept) we have proposed to address requirements of e-cognocracy. Section 4 gives a second approach for the widespread implementation of the service and deployment of the system. Section 5 describes the third approach with a proposal for the security of the e-voting system by means of a new cryptographic operator and details of the implementation. Finally, Section 6 sets out our final considerations and research tasks within this project.

* Corresponding author.
E-mail addresses: jsalazar@unizar.es (J.L. Salazar), jpiles@unizar.es (J.J. Piles), jruiz@unizar.es (J. Ruiz-Mas), moreno@unizar.es (J.M. Moreno-Jiménez).

0920-5489/$ – see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2010.01.004

2. E-cognocracy

2.1. E-government and e-cognocracy

E-cognocracy [16,19] is a new democratic model intended to make more ambitious use of democracy than the mere election of political representatives. This cognitive democracy (e-cognocracy) seeks to convince citizens not defeat them (e-democracy), by aggregating the results obtained from political parties (representative democracy) and citizens (participative democracy), assigning different weights (w_1 and w_2) depending on the context of the problem (local, regional, national or supranational) and the objectives of the system.

The key characteristics of e-cognocracy [19,22] are:

(a) Human beings are considered in a holistic and systemic context.
(b) Citizens may participate in the system either as they have traditionally done (delegation), or by taking part directly in the resolution of problems. It allows for direct involvement of the citizen in decision making processes, thereby fostering participation in the democratic system and the creation of knowledge in society.
(c) Parliament would be distributed in two parts (public and private). The share of seats allocated to each part depends on the type of problem (around 2/3 and 1/3 for national problems and 1/3 and 2/3 for local problems).
(d) In order to avoid saturating citizens with participation in these processes, only some particularly relevant (strategic) problems would be treated in this manner.
(e) We use multicriteria techniques to solve the problem, including the aggregation of the solutions provided by political parties, on the one hand, and citizens on the other.
(f) Using this model, we are able to extract knowledge as this refers to behaviour patterns, preference structures, stylised facts and trends of the decision making process.
(g) Internet is used to incorporate the preference structures of citizens into the decision making process.
(h) It improves control of the political system and reduces dependence on minority political groups, since it would be essential to win a margin of (online) votes for each problem and at any given moment. This would produce wider coalitions between groups, favouring more moderate proposals enjoying democratic support.
(i) All ideas, even minorities' positions, are included, but decisions are taken according to the majority rule.
(j) It improves overall knowledge and understanding of the system, incorporating a wider range of perceptions of reality, deepening debate and strengthening negotiating processes and the search for consensus.
(k) Effort, learning and continuous improvement are favoured, and recognition is given to the skills and abilities of individuals, thereby identifying social leaders.
(l) It facilitates continuous education (learning) of the interested population, in line with the Rawlsian concept of social justice (i.e. equality of social opportunities).
(m) It allows for easy expansion and diffusion of knowledge (socialisation of knowledge), as well as the creation of minimum ethical standards. In this way, ignorance, which is the real poverty suffered by humans beings, can be reduced.

To sum up, the key idea of e-cognocracy is to educate people, promote relations with others, improve society and construct the future in a world of increasing complexity [19]. The key differences between e-cognocracy and e-democracy can be summarised as follows: (i) if e-democracy deals with the participation of citizens in the discussion of public problems with the aim of transferring information, e-cognocracy deals with the involvement of citizens in the resolution of public problems with an educative goal; (ii) if e-democracy is based on the assumptions that each person has a vote and the political parties filter the ideas of citizens, e-cognocracy is based on the assumption that each person has many ideas that are filtered by the citizens themselves through the network; (iii) if e-democracy tries to defeat people taking into account the number of votes, e-cognocracy seeks to convince them taking into account the best arguments; and (iv) if e-democracy is the government of people, e-cognocracy is the government of knowledge, that is to say, the government of Social Wisdom jointly created by means of Internet.

2.2. E-voting requirements for e-cognocracy

Among the many tools needed to fully develop e-cognocracy, we will focus on e-voting, as this is the first step in gathering 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 focuses 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 [21].

The development of algorithms implementing electronic voting has been wide-ranging from the outset [5]. Most of their services have already been studied, and including them therefore requires only an adaptation.

As we have already mentioned, e-cognocracy seeks to involve people in the identification of the critical issues in the decision making process. This is achieved in two ways:

— Multi-criteria framework: In order to establish the state of popular opinion, several key issues are to the vote, but elected representatives are still allowed some weight in the choice (e.g. it could be x % direct participation and $(100-x)$ % indirect participation) in order to prevent demagogy.
— Linkability of votes: Each poll is divided into several rounds (the number of rounds is fixed beforehand), and each voter can cast votes in as many rounds as s/he wants, but only once each round. The last vote cast by each voter (independently of the round in which it was cast) is the one taken into account for the final result. However, all the votes from the same voter are linked together (while ensuring voter anonymity). This allows us to track shifts in opinion very accurately and to link them to external events, identifying what is really driving people's opinions.

To sum up, e-cognocracy requires the following performance properties, most of which are shared with classical e-voting systems [1,6]:

1. Only voters in the census shall be able to vote (authentication).
2. Each voter shall be able to vote only once in each round (democracy).
3. A voter shall not be linked to his/her vote (anonymity).
4. A voter shall not be able to prove his/her vote (no coercion).
5. It shall not be possible to remove a valid vote from the final count (precision)
6. It shall not be possible to include a non-valid vote in the final count (reliability)
7. Only each voter can cast his/her own vote (veracity)
8. Voters shall be able to verify that their vote has been correctly counted (verifiability).
9. For each round the vote shall be secret until the counting phase (neutrality).
10. Two votes from the same voter in different rounds of voting shall be linked together, but not to the voter who cast them (linkability).

Having defined the requirements, let us proceed to implementation, which involves three approximations:

- Proof of concept: We shall build an initial version that meets all requirements.
- Remote access: We will implement access to the e-cognising service from any terminal connected to the net and equipped with