Digital Identity Applied to Telematic Voting Involving European Citizens. Social and Legal Implications

Emilia Pérez Belleboni[1], Sergio Sánchez García[2], Justo Carracedo Gallardo[3] and Ana Gómez Oliva[4]
Departamento de Ingeniería y Arquitecturas Telemáticas. Escuela Universitaria de Ingeniería Técnica de Telecomunicación. Universidad Politécnica de Madrid
Ctra. Valencia km. 7. 28031 Madrid.
Telephone: (+34) 91 336 78 02. Fax: (+34) 91 336 78 17,
{belleboni[1], sergio[2], carracedo[3], agomez[4]}@diatel.upm.es

Abstract

This paper describes the characteristics of systems of electronic voting in which both the vote itself and the authorization to vote circulate through computer networks (telematic voting), with a focus on the problems arising from the need to ensure correct identification of citizens seeking to access the voting system in a Europe-wide environment. The advantages offered by such a system are discussed, as are the major social and legal implications these solutions may entail.

1. Introduction

We are now living through a process in which interpersonal activities or citizens' dealings with other social actors – activities that had been carried out through conventional forms of communication, and usually in person – are now increasingly being undertaken with computer networks, in what might be called the gradual introduction of the so-called Information Society. This transformation of the behavior of social actors unquestionably offers a number of advantages, but it also involves certain risks that must be taken into account in order to ensure that the modernization of communications systems will result in an enhancement of the rights acquired to date and to win the trust of the citizens.

Democratic voting processes in which the citizenry expresses its opinion and makes decisions in public affairs have not been isolated from this process of modernization. Thus, for many years we have seen increasing automation of every phase of the voting process. At first, systems have been developed that use computer-based electronic ballot boxes and, more recently, proposals have been made that rely on the remote communications provided by telematic networks.

Accurate identification of citizens who seek to vote is a crucial element for ensuring the democratic validity of any voting process. In the transition from in-person voting processes to remote voting through computer networks, one of the most sensitive aspects is verification of the identity of the voter by means of robust cryptographic and electronic methods so as to ensure the voter's right to participate in the voting process.

These new forms of identification and behavior involve not only the technological development of complex systems: they also imply social, political and legal changes that must be taken into account as a preliminary step prior to the implementation of a new voting system.

First, this article analyzes different options for automating the voting process and it discusses the differences between electronic voting in ballot boxes in sight of voters, on the one hand, and electronic voting in remote ballot boxes through computer networks (telematic voting) on the other. Next, it provides a summary description of the structure of such a system of telematic voting and the actions to be performed by voters. Then, the article will address the problem of identity and delegation of identity in systems of telematic voting in pan-European environments and specify which elements bear the greatest social and legal implications.

2. Telematic voting involving European citizens

For more than a decade in the European Union (EU), reciprocity agreements have allowed the citizens of certain countries to participate, as either electors or candidates, in elections held in another country of the Union where they are living [1].

Further, as cooperation between countries in the Union grows ever more intense, it will become ever more common for some people to travel to other EU countries for diverse work-related reasons. The number of people traveling in Europe for pleasure or personal reasons is also likely to increase. In all such cases, if remote voting through telematic networks is implemented, citizens will be able to participate in elections being held in their countries of origin.

2.1 Telematic voting: the development of electronic voting in cyberspace

We shall use the term *electronic voting* to refer to an automated process of casting and tallying votes. In such a system, electronic machines in sight of voters are used to cast a vote in an electronic process. These computer systems, called *voting machines* or *voting equipment*, are replacing traditional ballot boxes. In *electronic voting* ballots are inserted, captured and stored in an electronic format and then automatically tally votes once the voting is over.

A more advanced phase in the automation of electoral processes is represented by "telematic voting", in which case voting is effected with the use of telematic networks and specific telematic agents whereby a vote is cast in a remote ballot box which is located out of sight of the voter. In this system, the entire process is automated: from the identification of voters all the way to the tallying of votes, including the casting of votes themselves. Both the authorization to vote and the vote itself "travel" through a network.

Why should it be called telematic voting? Quite often, the literature uses the term electronic voting (eVoting) for what we call herein telematic voting. The answer is that we believe it is more useful to maintain a nomenclature that distinguishes electronic voting and telematic voting because an in-person vote and a vote in a remote ballot box are alternatives with both a technological dimension and socio-political requirements that are radically different, and a failure to clearly differentiate between them will generate confusion among the public.

Telematic voting is also sometimes called remote voting; but voting by mail is also a form of remote voting and thus creates further confusion. As a result, if we call both types of voting electronic voting (eVoting), one would have to say in each case "electronic voting with an in-person voting machine" or "remote electronic voting", but that would involve an unnecessary complication and add further difficulties of public understanding.

In general, two types of scenarios for telematic voting can be distinguished:

type a) Voting requires going to specific voting sites in person. In such a case, the telematic voting process must be supported by its own, functionally independent, telematic components: a terminal for authentication, a terminal for casting a vote, a remote ballot box, systems for managing and tallying votes, etc. Further, it must use its "own" telematic network dedicated solely to the voting process.

type b) The voter can vote from anywhere, even from home. In such an arrangement, voters would use their own connection device to cast the vote and ordinary services of an ISP for authentication and sending the vote to a remote ballot box. This specific type of telematic voting can be called Internet voting.

In reality, when a *type a* scenario speaks of using its "own" telematic network dedicated solely to the voting process, this does not necessarily refer to a complete network, from links and the physical level until transport servers, dedicated exclusively to the voting system. Hence the inverted commas. The most reasonable option would be a virtual network supported on an Internet data transport infrastructure. For example, in the Votescript+ system [2], the virtual voting network is divided into three independent virtual networks in order to preserve voter anonymity by preventing the multiple votes or voting by individuals that are not eligible to do so. These networks are: the Authentication Network, the Voting Network and the Verification Network, as shown in figure 1.

The framework of "type a" telematic voting includes the Votescript proposal, which has been designed and developed by the authors of this article with the participation of a more extensive multidisciplinary team where sociologists and jurists took part.

To reinforce the anonymity of voting, the Votescript+ telematic voting system described in summary fashion in this paper includes use of an infrastructure that supports the electronic Identity Card (eID Card), which is a smart card capable of electronic signatures and reliable identification of its owner and which is starting to be used in a number of EU countries, among them Spain. This card is not used in the voting phase, in order to robustly separate the identification/authorization phase from the secret ballot casting phase. Even though the eID Card is once again used in the verification phase, a complete infrastructure is not required to guarantee citizens' identity. Different phases of the process also make use of another card, the Smart Voting Card (SVC+), which is generic and identical for all voters. Information identifying the user cannot be extracted from this card. The SVC+ contains programs and stores data in a way that no user terminals in any of the networks require cryptographic capacities or data storage capacities. Further, it is useful to emphasize that the possession of a valid identity document does not necessarily mean being eligible to vote, as voting rights may have been lost in a court ruling, or due to residence in a region outside the scope of the given voting process or non-eligibility for reasons of age, etc.

From the point of view of the voter, the voting process can be divided into five phases, which are briefly described as follows:

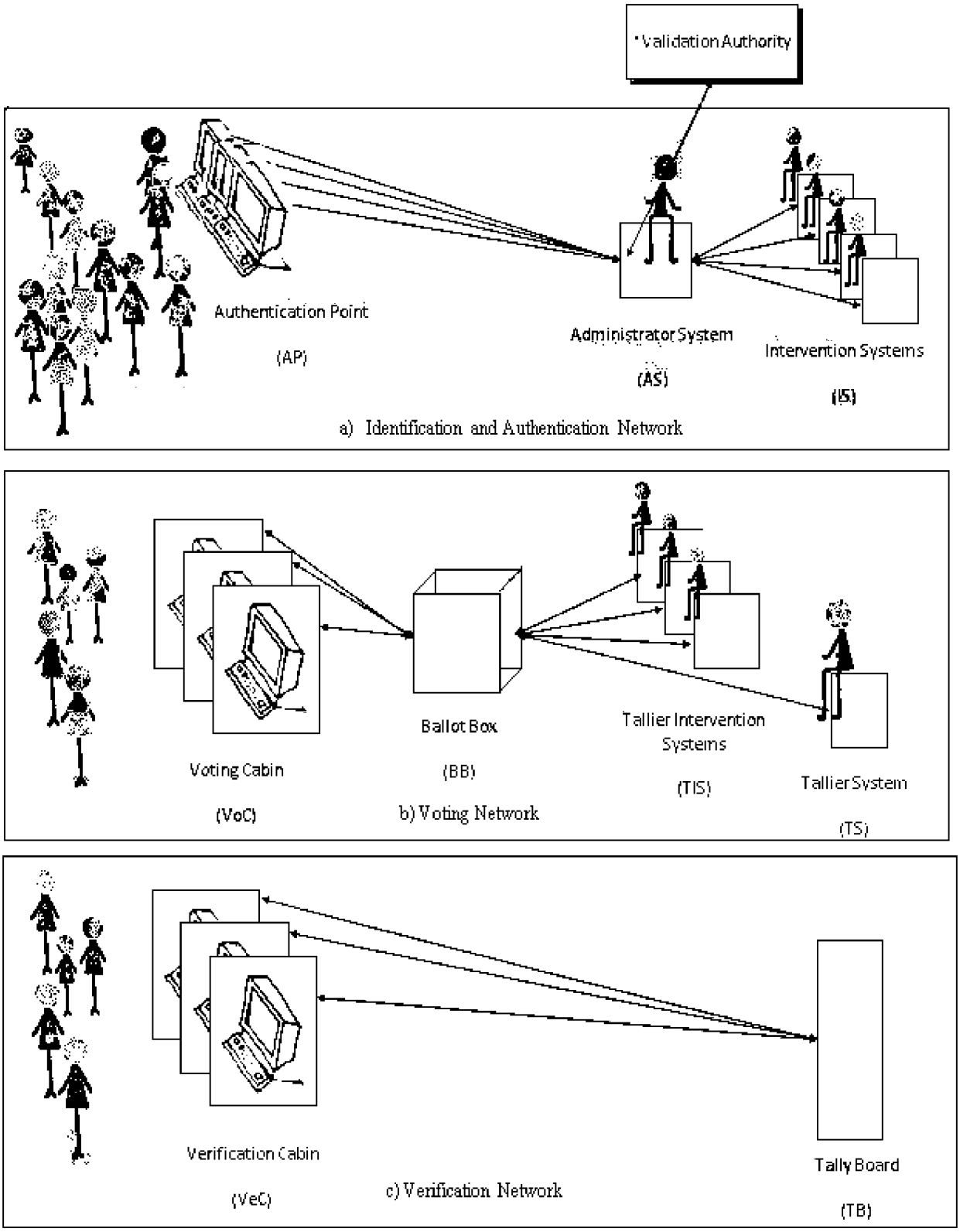

Figure : Global architecture of Votescript+

In phase 1, the voter makes use of both the eID Card and the SVC+ to identify him or herself in any of the system Authentication Points and requests authorization to cast a vote; authorization will be denied if the voter has

already gone through the process previously or if the person is not a part of the electorate. The authorization request issued through the execution of processes specifically designed for this purpose stored in the Smart Voting Card (SVC+) consists of a key (K_{dV}, hidden in the card with an opacity factor to prevent subsequent linkage of the vote with the voter) that will later be used to decipher the vote. The authorization request carries an electronic signature provided by the eID Card. Authentication Intervention Systems and the Administration System decide whether to issue authorization. This authorization key (K_{dV}), which is blindly signed by the Administration System and the Authentication Intervention Systems, will be a guarantee in the next phase that the vote has been cast by a legitimate voter. Validation of the identity of a citizen seeking to vote is performed with the eID Card and with the collaboration of a Validation Center in accordance with the processes and protocols established by the public authorities. That is, Votescript+ delegates to the eID Card scheme the assurance of voter identity. The Validation Center is external to Votescript+, as a resource provided by the eID Card infrastructure. Over time, as this assurance becomes more robust and wins public trust in its incorporation to daily life, Votescript+ will inherit the enhancement because of this delegation.

Therefore, before implementing a telematic voting system using eID Cards for voter authentication, educational campaigns must be carried out on the security offered by these systems and sociological studies made to corroborate public trust in digital methods of identification.

Phase 2 (voting itself) for the voter starts after receiving authorization. To cast a vote, the voter simply reports to any voting cabin with the SVC+ (the eID Card is unnecessary). Inside the cabin and isolated from external interference, the voter will find resources that will enable him or her to cast a vote ciphered with a key known only to the SVC+ that has generated it, (K_{cV}), which is symmetrical to the K_{dV} used recently. The vote is ciphered in a way that the ballot box cannot decipher the bit of information it receives. Finally, the card securely stores the vote receipt it receives from the ballot box.

Phase 3 (tally) will begin once the two prior phases have concluded. Here the ballot box is opened, and it transfers to the Tallier (T) and the Tallier Intervention Systems the votes it has stored while phases 1 and 2 were active. Each receptor of the contents of the ballot box, acting simultaneously, so that all the controllers can corroborate them.

Phase 4 (verification) is divided into two parts. In the first part, (4.1) clarification is effected of all possible divergences between the results of the official tally and those produced by the Tallier Intervention Systems, for all have received the same data from the ballot box. In the second part (phase 4.2), the voter once again plays a central role, as he or she can now access the Verification Network and review the treatment given their own vote by submitting some of the data stored in the smart card, which will be checked against the information made public by the Tally Board. A voter may present a challenge to the election authority in the event of a discrepancy and provide solid proof, such as the vote receipt issued by the ballot box. The election authority will access the records of different agents and the information released in order to settle any claims presented by controllers; and if the claim has been filed by a voter, it will also access the information stored on the pertinent SVC+.

Why call it telematic voting and not Internet voting? Quite often, what we call herein telematic voting is called Internet voting. From the discussion in the previous paragraphs, one should conclude that this term is inappropriate for a voting scenario like the one we have specified in type a. Even though the transport infrastructure of Internet is used (which need not be the case at all times and in all its scope) this does not mean that Internet is being used, at least from the user point of view. Internet means openness and multiplicity of access, making it much more than a transport infrastructure. Although a road network represents a vehicle transport infrastructure - and little more – the Internet represents a data transport infrastructure and much more.

Only in the case we have classified as type b – where the vote can be cast from any point of access to the Internet, or even from home – would it be appropriate to use the term Internet voting for telematic voting. We believe this method to be unfeasible when sociopolitical environments involve certain risk of masquerade or vote selling. Nevertheless for configuring electoral systems with political validity, for many other voting contexts in which the value at stake is much lower (for example, elections in sport or cultural associations, local processes of political participation, etc.), a system of Internet voting can be an economical and viable option, if it takes into account the security requirements of the given environment. Studies on social acceptance or rejection must be done carefully not to misuse terms.

2.2 The problem of identity verification in pan-European telematic vote processes

As mentioned, the proposal for telematic voting presented herein makes an important delegation of voter authentication to the reliability of the document used to identify voters and thereby reproduces the arrangement used in conventional voting processes with paper ballots in many countries. Possession of a valid identification document is a necessary but not sufficient condition to cast a vote. This is because a European Union citizen with

a document may not have reached the minimum age required to be eligible to vote, or local elections may require that voters reside in a certain geographic area, etc. From this point of view, the existence of "electoral rolls" maintains and even becomes greater in importance. At present, a European Union citizen residing in a country other than his or her country of origin can be entered in the electoral roll of the place of residence to elect members of the European Parliament and must give information on the country, region and municipality in which the person's voting rights were last exercised in order to be removed from that electoral district. In nowadays, it may make little sense to exercise stricter controls than these, which place their trust in citizens' honesty, at least for the moment and given the low public interest shown by high abstention rates. More effective controls should be in place before they have become crucial: that is, when a value that is vital to the public is at stake.

Citizens' new relationship with democratic institutions must be ready to provide a good response to new situations in advance. To achieve this, European authorities must have opened new paths for the exchange of information with each other that, firstly do not give rise to illegal acts of registration in electoral rolls and, secondly, that manage in their entire scope of jurisdiction the temporary suspension for legal reasons or definitive removal (death, change of nationality, etc) of citizens from electoral rolls.

Implementation in European Union countries of a telematic voting system such as the one proposed herein will bring benefits beyond sheer technological modernization. The change of technology will allow for offering greater guarantees of accuracy both in the identification of votes and in the tallying and communicating of results, while enabling control by citizens in a way that is unthinkable or unfeasible in conventional systems: each citizen will have irrefutable proof of how his or her vote was handled in the general tallying of results.

It will also allow for designing system communications interfaces with voters that can adapt to individual circumstances such as disabilities or other peculiarities to facilitate independence in casting a vote. Such circumstances affect both citizens who do not know the local languages and those with difficulties of sight or movement, or those who for any other reason are away from their residence on voting day, provided they are within the jurisdiction of an EU country.

The implementation of these systems carry legal implications, as properly benefiting from the improvements offered by these systems will require addressing the need for a reform of laws in each country and a discussion of the appropriateness of elaborating laws that would affect all European citizens equally.

3. Voters' digital identity

The need has become evident to establish methods that can unify the identification of EU citizens and enable them to exercise, in equal conditions, the different roles that arise in the operation of an electoral system: as voters, candidates, representatives of political parties, etc.

For a number of years, some European countries have had systems for identifying their citizens based on the display of a document issued by the state attesting to a person's identity: these are the national ID Cards. This type of document has evolved over time from a simple sheet of paper with a series of personal details, all the way to documents equipped with strong anti-forgery mechanisms and mechanisms for identifying the bearer, such as a photograph, a handwritten signature and fingerprint. At present, national ID Cards in Europe have similar content in all countries.

Some EU countries have been generating in recent years new identity documents that consist of a forgery-resistant smart card fitted with a chip with cryptographic capacities that can reliably identify the proprietor and digitally sign a document in electronic format using a private key stored inside.

This new form of identification has become more widespread without encountering significant reserves in the public. Nevertheless, the introduction of this new type of digital identification will carry a large number of social implications that, to date, have not been sufficiently well analyzed. Thus, we believe that multidisciplinary studies are needed – with researchers from the fields of technology, politics, sociology and law – to exercise influence with the public authorities to ensure that the implementation of these systems and the legal reforms they imply is done in a manner that protects the rights citizens have acquired and respects their right to decide.

In both countries that have traditional identification systems and those which do not, citizens will have to be given an electronic or digital identity that will enable them to identify themselves in the network with at least the same guarantees provided by their national ID Cards in personal interactions. The telematic voting system will benefit from the deployment an infrastructure that will enable citizens of European Union countries to have their own electronic identification cards. Present national eID Cards, with an external appearance that is similar to traditional identification documents, consist of a smart card that can incorporate biometric identification, are presumably more reliable than traditional documents to identify their proprietor. At the request of the proprietor, cryptographic processes are executed in the chip to authenticate a citizen and, in his or her name, digitally sign a document. This property, along with protection of data stored on the card, lend an electronic signature greater guarantees than those provided in a traditional

handwritten signature, making authenticity verifications more robust than those provided by calligraphy experts. These eID Cards are already being issued in Austria, Belgium, Estonia, Finland, Italy, Portugal, Sweden and Spain.

As mentioned in section 2.1, validation of citizen identification in Votescript+ begins the phase of authentication in the system, is performed with an eID Card with the collaboration of a Validation Center. The Validation Center is a component of the eID Card identification infrastructure that contains information on each and every one of the eID Cards produced in a given country.

Thus, if a telematic voting process is being held in Spain and a citizen seeking to vote accesses the system with an eID Card generated in Spain, the Validation Center will use established communication protocols to notify the Votescript+ of the approval or rejection of the validity of the digital information contained in the eID Card presented by the voter. In contrast, if a Belgian citizen seeks to vote from a voting site in Spain, the Spanish Validation Center cannot approve or reject the validity of the eID Card on its own, but must establish peer-to-peer communication with the Belgian Validation Center and await an affirmative or negative response. This necessary interoperability between the systems controlling the operations of eID Cards in Europe-wide telematic voting environments introduces an added level of complexity, as it requires homogenization not only from a technical point of view, but also in the laws and policies regulating electoral processes in EU countries.

Control over the right to vote in EU countries is becoming extremely complicated. This is due not only to the multiple types of elections, but also the selective right to participate in some elections and not others. For example, an EU citizen who is a foreigner in France can vote in French local elections without losing the right to participate in the same type of local elections in another country; the same is not the case when electing members of the European Parliament, where it is made clear that a citizen can cast a vote only once. This same person cannot participate in the national elections of France. Consequently, registration in the census for one type of elections does not automatically imply registration in another. Proper management of censuses demands quick and truthful communications between the countries involved.

Acquainting citizens with the use of this identification card in different types of telematic transactions will lend telematic voting systems further support and lessen mistrust among the public regarding the honesty of the system. We believe, however, that an in-depth study of legal and social reality is required before adding the new voting system to this new form of identification.

4. Identity delegation

One of the most important issues being addressed in the context of digital identity is delegation of identity. This occurs when a person or organization ask a third party to act on their behalf [3]. Roles for representing others in telematic voting systems include representation by individuals of political parties, candidates, or citizens' groups, or when a voter delegates the casting of a vote to another voter.

4.1 Representation of political groupings

Both in the globalized environment of Europe and internally in each country, citizens organize politically in political parties or other types of groupings. In Votescript+, these organizations play an important role in exercising oversight of the system. The European scene includes everything from the most pan-European parties to the most locally oriented parties, whose very existence and purpose are limited to a specific geographic area. What they have in common is that they will have to appoint representatives before the system, and these must bear dual identification: first, they will have to identify themselves personally with valid credentials and, secondly, they will have to document the organization's decision to delegate them. The nationality of the delegatee and the delegator will no longer be a barrier once Europe has an effective infrastructure to allow for cross-border delegation [4]

4.2 Representation of an absent voter

Apart from the obvious difficulties of managing identifications, another arises in relation to the facilities provided by countries to their citizens to deliver their vote even when they will not be in the vicinity of a voting station on election day. We may be tempted to believe that this will no longer be a problem because telematic networks will provide a solution, as the vote will travel over the network. But this solution will only be valid for citizens traveling within the EU and nowhere else in the world [5].

In Spain, any voter expects to have trouble going to a polling station within the specified time frame can send the vote by post, after having applied for the ballot and supplied identification to a post office civil servant handling the request. In this voting option, the voter implicitly waives several fundamental rights they could otherwise enjoy if the right to vote were exercised in a traditional way: at the post office, there are no representatives of the political parties acting as guarantors of voter identification or access free of coercion, nor are the votes given appropriate custody until the tally is made.

In France, the debate on the weaknesses of voting by post was settled by prohibition of voting (as in many other countries), while proxy voting is allowed, so that a voter can designate a trusted representative, who will also act as a voter in their own right in the election and thus cast both votes: the proxy's own vote and the vote entrusted by the delegator, supposedly fulfilling the will of the latter. If the French approach, or similar versions in effect in the United Kingdom and Holland [5] were to spread in Europe, delegation of electronic identity and its revocation must be sufficiently mature in order to be incorporated in the processes of voter authentication required by telematic voting. Acceptance of any of these methods of identity delegation in different countries will entail changes in the law that we believe must be enacted only after they have been socially and politically accepted.

5. Conclusions

The expansion of computer networks will enable the implementation of voting systems in which both the vote itself and the authorization to vote will circulate on a network (telematic voting), thus noticeably facilitating voters' access to the voting system. The Votescript+ system the authors of this paper have developed shows the technological viability of these alternatives and guarantees voter rights of confidentiality, non-coercion and anonymity.

One of the most significant issues posed by the Internet and other computer networks relates to the need to guarantee users' identity as they access the services available to them. Specifically in regards to telematic voting systems, accurate identification of voters is a decisive factor in the democratic validity of the system. This paper shows that robust and reliable solutions based on eID Cards are available for correctly identifying voters and it discusses the major social and legal implications these systems may entail.

The development of voting systems, with the incorporation of telematic systems, must take into account the fact that electoral processes are closely linked to both the peculiarities and the history of the peoples using them. A multidisciplinary study that encompasses sociology, law, politics and technology must be undertaken prior to instituting any new system so as not to jeopardize either the confidence of electors or the fortitude of democratic institutions.

6. Acknowledgements

This paper is part of the work being conducted by the authors in the projects supported by the Ministry of Education and Science of Spain through the National Plan for R+D+I: ADMISSION (TSI2006-4864), Telematic platform for e-Government based on a choreography of services and SEMPERSec (TIN2009-14406-C05-01), Framework for the provision of accessible security guarantees for personal autonomy.

7. References

[1] Elections to the European Parliament: voting rights and eligibility for citizens of the European Union [On line] http://europa.eu/legislation_summaries/justice_freedom_security/citizenship_of_the_union/l23025_en.htm.

[2] Carracedo Gallardo, Justo and Pérez Belleboni, Emilia. "Use of the New Smart Identity Card to Reinforce Electronic Voting Guarantees" The 4th International Conference for Internet Technology and Secured Transactions. Published by Infonomics Society, UK, November 9-12, 2009, London, pp. 439-444. UK ISB 978-0-9564263-1-4.

[3] Sergio Sánchez García, Ana Gómez Oliva,"Solving Identity Management and Interoperability Problems at pan-European Level", Eds.: Robert Meersman, Pilar Herrero, and Tharam Dillon. On the Move to Meaningful Internet Systems: OTM 2009 Workshops. Lecture Notes in Computer Science, Vol. 5872, Springer, November 2009. pp. 805-809. ISBN # 978-3-642-05289-7.

[3] Improvements of pan-European IDM Architecture to Enable Identity Delegation Based on X.509 Proxy Certificates and SAML. Sergio Sánchez, Ana Gómez. Workshop in Information Security Theory and Practices - WISTP'10. Lecture Notes in Computer Science, Vol. 6033, Springer, April 2010. Passau (Germany)

[5] Voting in France, for Foreigners. [On line] http://france.angloinfo.com/countries/france/vote.asp.

[6] ACE. ACE Electoral Knowledge Network. [On line] http://aceproject.org/.