Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 1 / ISSUE 2 / AUGUST 2006 / 58 – 71

This paper is Available online at
www.jtaer.com

Design of an Advanced Platform for Citizen Participation Committed to Ensuring Freedom of Speech

Emilia Pérez[1], Ana Gómez[2], Sergio Sánchez[3], Jose D. Carracedo[4], Justo Carracedo[5], Carlos González[6] and Jesús Moreno[7]

[1,2,3,5,6,7] Universidad Politécnica de Madrid, Departamento de Ingeniería y arquitecturas Telemáticas,
{belleboni[1], agomez[2], sergio[3], carracedo[5], cgonzalez[6], jmoreno[7]}@diatel.upm.es
[4] Observatorio para la Democracia Digital y los Derechos de la Ciudadanía en Internet, Madrid,
jdcarracedo@democraciadigital.es

Received 06 December 2005; received in revised form 27 April 2006; accepted 20 June 2006

Abstract

The expansion of new platforms of digital democracy does not necessarily entail an increase in citizen participation. The VOTESCRIPT group has made a sociological analysis to determine the causes of this apparent failure, reaching the conclusion that users are demanding capabilities that are not available in present systems.

This paper presents a proposal for an advanced system of debate in an environment of digital democracy which overcomes the limitations of existing systems. We have been especially careful in applying security procedures in telematic systems, for they are to offer citizens the guarantees that society demands. New functional tools have been included to ensure user authentication and to permit anonymous participation where the system is unable to disclose or even to know the identity of system users. The platform prevents participation by non-entitled persons who do not belong to the authorized group from giving their opinion. Furthermore, this proposal allows for verifying the proper function of the system, free of tampering or fraud intended to alter the conclusions or outcomes of participation. All these tools guarantee important aspects of both a social and technical nature, most importantly: freedom of expression, equality and auditability.

Key words: e-democracy, e-government, freedom of speech, security, anonymity, telematic platform

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 1 / ISSUE 2 / AUGUST 2006 / 58 – 71

This paper is Available online at
www.jtaer.com

1 Introduction

Far removed from day-to-day politics, the advent of telematic systems of citizen participation and management has been presented in the abstract as a solution to the present-day crisis of legitimacy, trust and participation broadly affecting institutional democracies (both representative and parliamentary). Teledemocracy, cyberdemocracy, e-administration, e-democracy, e-government, electronic government, digital government, electronic government, electronic democracy, digital democracy are a series of terms that appear ever more frequently in the popular media; they feature in electoral programs, in public statements by politicians and in general plans aiming to further the development of the "information society". Nevertheless, there are significant differences between the meanings given to these terms. This lack of definition directly affects plans for developing the information society, as an initiative can easily bill itself as "an advance towards digital democracy," in the absence of standard parameters for validating it as one. Such projects in public affairs carry an additional risk, for no standards exist for evaluating the results of initiatives undertaken, as they are often proposed, designed and executed by researchers of an exclusively technical background.

The lack of theoretical clarity allows telematic or electronic voting to be presented as experiments in digital democracy; while this is a common tool in democratic systems, it is by no means the only one as is stated -for example- in [20]. It is also true that present democratic systems privilege voting at the expense of processes of information and discussion. It is also believed that computer-mediated communications enables the pursuit of solutions independently of objections, which have made systems of direct democracy unfeasible for over two hundred years (due to scales of territories, sizes of populations and lack of qualified knowledge to responsibly make decisions).

Thus, the problem around digital democracy lies in the fact that it reopens the debate on forms of democratic organizations. This is important to study because it must allow for identifying the functions and characteristics to be developed. The properties and potential of information and communication technologies (ICT) gives rise to imaginative speculation regarding a multitude of models consistent with the political conceptions of each community [11]. We have observed, with particular doubts, how present implementations of ICT often expand the possibilities of social control– even in platforms of telematic participation- and generally deepen the construction of what [18] calls the *surveillance society*. It is obvious that in most democracies there is no exercise of (citizen) democratic control over processes of technological innovation or analysis of its consequences. Faced with this reality, our research group considers itself intellectually committed to a line of investigation that seeks to deepen, develop and implement computer systems that enhance citizen rights and minimize the possible negative effects on these rights by the establishment of the *network society*.

In our view, the plethora of possibilities offered by digital democracy would tend to strengthen processes rooted in classical conceptions of direct democracy. Our VOTESCRIPT multidisciplinary group is committed to the development of telematic systems that would enable free public participation with the aim of promoting both the mutual relationships of citizens to each other and citizens' relationships with authorities in a way that allows them to draw conclusions that facilitate decision-making, based on their own discussions. The method of applying the results of these discussions and whether they are to be binding or not, are issues that are beyond the scope of this group, as those issues fall within the domain of public affairs.

This group's first step in developing a system of citizen participation consisted of compiling a list of the demands of the population. It has thus conducted several sociological and political science projects in Spain, the most important of which was a qualitative investigation with discussion groups throughout the country to study perceptions and images aroused in citizens by the use of Internet in general, and systems of participation through the Internet in particular [22]. The investigation found that the social demands of citizens for a particular electronic service often center on the need to have guarantees that the service operates properly: that is, that fraud could be detected by the managers or administrators of the service. In the case of a citizen participation service, our work also confirmed that fears exist among citizens regarding possible malfunctioning of the system, which could mean that certain messages were not published because they were considered contrary to the opinions of interest, and second, the fact that the emission of opinions could lead to reprisals, particularly in smaller communities. These conclusions meant that the design of the debate platform, the global security of the platform and anonymity are crucial issues to be taken into account. The final part of the sociological work requires testing the social validity of the solutions undertaken; thus, following implementation of the platform, a new sociological study is to be performed with the aim of determining the extent to which the solutions meet citizens' expectations.

2 Conceptual Framework

One of the first tasks of VOTESCRIPT group concerning digital democracy involved analysis of the leading experiences in this topic as practiced to date. Outstanding examples include the projects implemented through the VI European Union Framework Program. The DEMOS [7], [16] project was among the most relevant, as it approached digital democracy from the perspective of the discussion process, analyzing and proposing new methodologies enabling interactive communication between large numbers of people, methodologies capable of aggregating and interrelating the different individual contributions, identifying and promoting the most promising discussion aspects,

profiling different stances and working to achieve convergence between these, all towards the objective of getting a result that could influence the political decision-taking process. The DUNES [8], [12] project is also interesting for its contribution in the field of constructive discussion: enabling citizens to debate the issues that concern them, collaborating amongst themselves and participating in a respectful fashion. Another noteworthy project is the WEBOCRACY [21], [23], whose objective is to provide citizens with an innovative voting, access and communication system in order to achieve increased voter participation in decision processes. We must also mention the EURO-CITI [10], [25] project, through which a shared services architecture has been developed for the public sector, including voting services, electronic form delivery and citizen consulting. Another important digital democracy project orientated towards decision-making is the TED [26] project. This aims to develop new techniques based on Bayesian methodology that facilitate a result to a problem in which it is unavoidably necessary to weigh up multiple sources of uncertainty, where conflicts of interest exist making necessary integration of the opinions and desires of disparate groups.

In Spain a multitude of experiences based on the principle of citizen participation in public affairs are under development, most particularly the promotion of forums created to debate municipal issues. Among these initiatives, for the number of local councils involved, we highlight the Ciudadanos2005 [5] project, organized by Europa Press in collaboration of the Spanish Ministry for Industry, Tourism and Commerce, in which some 80 small and medium sized municipalities are involved in promoting some kind of access to participative Information Society tools for everyone. Other initiatives are also underway in local, national and European elections aiming to bring politicians closer to voters, and enabling public communication between them [9].

An analysis of the aforesaid experiences, as well as our sociological fieldwork, enables a series of conclusions to be reached concerning the characteristics which all citizen participation systems should hold to achieve strong acceptance:

1. First, the problem of digital stratification must be confronted. Though there are fresh government initiatives daily backing the introduction of computers across demographics, there still exists a high percentage of the population which is information technology (IT) illiterate. Particularly for these people, it is essential that citizen participation systems are simple and easy to use.

2. The issues under discussion must be close to the participants' concerns. On this point, participation systems orientated to local issues have proved very attractive for local communities.

3. There must be a commitment by the relevant authorities that the conclusions arising from a debate are taken into account in a final decision. It has been found that one of the most negative aspects affecting the success of a given forum is that opinions offered hold merely testimonial value, or that mechanisms have not been clearly defined to transmit these opinions to the pertinent bodies. The promises and expectations generated by the process must be respected and fulfilled if citizen participation is intended to grow.

4. The discussion process must be clearly structured into well-defined phases: selection of subjects of interest, expression of participants' opinions and the drawing of conclusions. The last phase can be undertaken through an automatic or semi-automatic procedure that extracts knowledge from the messages emitted, which can be followed by dynamics of conciliating postures and consensus building or even voting processes.
5. The system must guarantee certain aspects relating to the identity of participants, or their anonymity, if desired, secure storage of information and its freedom from tampering.

2.1 The Issue of Security

The issue of security would appear to suffer from the most neglect in systems of digital democracy. It has been seen that most of the open forums in municipalities do not perform any type of access control over the participants, or this control is incomplete, in such a way that systems can be flooded with messages from participants who are not entitled to respond on the matter under discussion. Often, this lack of security results in messages that are insulting, or in breach of protocols of participation, or even in conscious practices of sabotage of the discussion process as is stated in [24]. In contrast to this model, and to avert chaos, we have found other systems in which participants are clearly identified by the system but also subject to possible monitoring. This also constitutes an impediment to free participation, as participants may feel that their involvement is under surveillance, and such sentiment may have serious consequences, particularly in smaller communities. In our sociological work, one of the main concerns regarding cyberspace is the lack of anonymity, the sensation of lack of privacy in daily activities. In systems of participation, to ensure freedom of speech, we believe it is crucial for participants to have mechanisms that can ensure their anonymity in certain conversations. Thus, the capacity for anonymity included in the systems analyzed is far from providing the required functionality. Systems that enable the emission of anonymous opinions do so through an alias that is provided to the user beforehand. However, the process of obtaining these aliases involves two additional problems that are not addressed by any of the projects mentioned: either the alias is provided indiscriminately, without verifying the user's authorization to access the system, or the user's identity is verified prior to assigning an alias, at the cost of the allowing the system to know the identity of the user associated to the alias.

Bearing in mind these security considerations, a series of good operating principles have been identified that should be guaranteed by any platform of digital democracy, independently of the honesty and professional abilities of the persons responsible for operating the system:

- Freedom of speech, whereby all users of the platform can express themselves with no fear of reprisals in the present or in the future.

- Equality, whereby the opinions of all citizens carry the same importance.

- Mutual respect. Opinions expressed publicly must observe certain rules that have been defined and accepted by the participants in the forum themselves.

- Determinate duration of discussions. Subjects for discussion shall have a lifetime that is agreed and known by users when the debate commences.

- Citizens should have robust probes in order to verify that the system is functioning properly. That means the system must be auditable.

- Validation of conclusions either by consensus or through a vote. In the latter case, the system must ensure a clean voting process.

2.2 PARTICIPA System

The authors of this paper have designed a system (PARTICIPA) which overcomes the limitations of existing systems. As a result, we have obtained a telematic and protocol communication architecture which easily adjusts to the needs of different human groups and which may be configured and extended according to management needs.

We have been especially careful in applying security procedures in telematic systems, for they are to offer citizens the guarantees that society demands. New functional tools have been included to ensure user authentication and to permit anonymous participation while preventing participation by non-entitled persons who do not belong to the authorized group from giving their opinion. Citizens are provided with tools that will allow them to verify proper system operation against tampering or fraud intended to modify the conclusions or the results of the participation. All these tools guarantee important aspects of both a social and technical nature, most importantly: freedom of expression, equality and auditability. This work is part of the research activities being performed by this group in the project “Development of a secure telematic platform bearing digital democracy scenarios” (Project TIC 2003-2141), under subsidy of the Spanish Ministry of Industry, Tourism and Commerce. The project aims to develop a platform for digital democracy that would include the security services discussed herein [13].

3 Behavior of PARTICIPA System

To meet the demands of society, the system must be equipped with robust security systems. The proposal herein involves the use of cryptographic algorithms with symmetrical and asymmetrical keys, opaque and blind signatures together with the use of smart cards [4].

Below are definitions of the entities of this platform, followed by an outline description of the global performance of the debate system. A detailed description of the information flow between them is beyond the scope of this article, though it is fully explored in [14].

3.1 Participating Entities

The scenario proposed involves a set of automatic systems. Figure 1 shows the relationship between these systems described below:

- Participation Points. These would be computers with an Internet connection equipped with a reader of smart cards, through which users can interact with the system. Computers could be located in the user’s home, workplace, in public places like a library or an Internet cafe, and so on.

- Registry. This entity would be responsible for authenticating users and providing them with an alias should they wish their participation in the debates to be anonymous. In addition, when a decision is made to submit to the conclusions of the debate to a vote, the Registry will deliver authorization to legitimate voters.

- Registry Intervention Systems. These complement and supervise the operations of the Registry by performing the same processes in a parallel manner.

- Alias Manager. This entity would ensure that no repeated aliases exist in the system. It will maintain a public list of the aliases being used in each forum.

- Forum. As its very name would indicate, this system would support the debates taking place in the system, receiving and publishing opinions of authorized users and storing all data received so as to enable operational audits if necessary.

- Conclusion Extractor. Through a semantic analysis of the information received in the forum during a discussion, this system would extract useful knowledge. It would basically extract the main lines of argument with the aim of ultimately submitting them to a vote.

- Voting System. This system will gather the votes cast by the users of the system during the voting processes on the conclusions. It will count the votes when the period for their reception is over and publish the results.

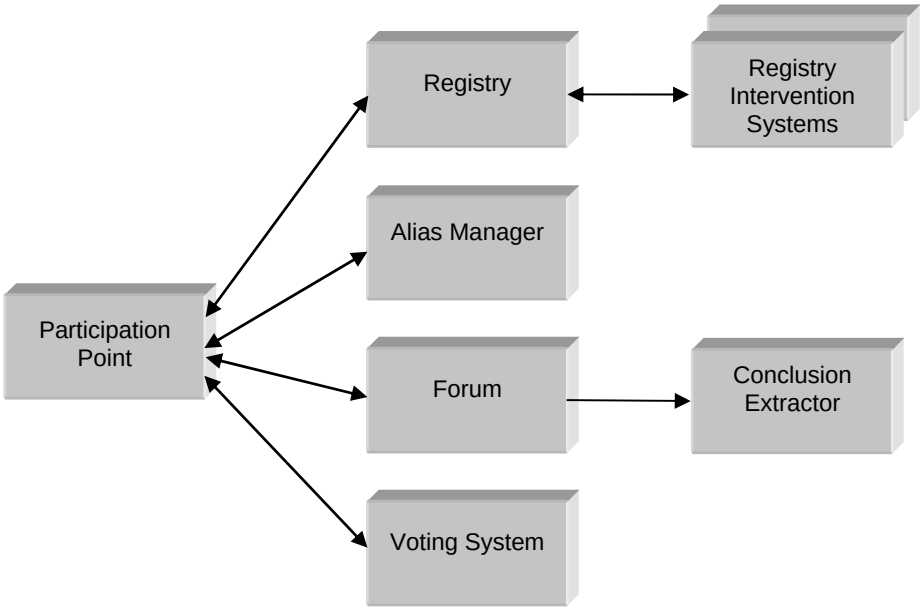

Figure 1: System agents

In addition to the above entities or automatic systems, the following persons participate in the system:

- Users. Every person registered in the census of participants can interact with the system as a user, both through observing the progress of a discussion and expressing opinions in the forum. All users can also participate in votes regarding the conclusions drawn following a debate. Every user will be the bearer of a Participating Card, a smart card that is manipulation-resistant and which enables the performance of multiple cryptographic operations.

- Managers responsible for the operations of the Registry and for each of the Registry Intervention Systems.

- Moderator. Will ensure that debates do not digress from the subject for which they were created. Messages sent to the discussion forum by the moderator will not be taken into account by the Conclusion Extractor.

- Guests. These are users who are allowed to participate –fully identified- in different phases of the discussion process even though they are not on the census of participants. Their number shall be limited and a census of guests will be created. Their opinion will not be taken into account by the Conclusion Extractor.

3.2 Overall Function

Each debate forum has a census of individuals that are allowed to participate. It is beyond the scope of this article to determine which citizens are entitled to participate in a given forum; rather, we begin from the premise that some legitimate authority has created the proper census. The system envisages two forms of participation in issuing their opinions in a forum of discussion: anonymous participation through use of an alias and identified participation, that is, with use of one's real identity with a name and surname. Participation in voting is anonymous in all cases.

Authorized citizens shall therefore have a Participating Card, which shall consist of a tamper-proof smart card that will serve to identify users and to support critical cryptographic processes. This will prevent fingerprints from previously used computers from being incorporated into subsequent attacks. Moreover, this card would store receipts of the operations performed, which would be useful in case of detection or suspicion of system malfunction.

When a citizen wishes to give an opinion in a forum for which he or she is authorized, they must report with their Participating Card to one of the Participation Points, where they can provide their opinions and participate in voting.

If a user wishes to participate in a forum anonymously, the user must first complete a dialogue with the Registry entity to obtain authorization that would allow the user to negotiate an alias with the Alias Manager as explained in 5.4.2 paragraph. The process of obtaining an alias offers the apparently contradictory guarantees of authenticity– only authorized members can participate in the debate– and of privacy, for the system ensures users' anonymity, so that nobody, neither the system itself can link the alias to the user. Furthermore, the system prevents use of the same alias by more than one participant in the forum.

The operations of the Registry are supervised and monitored in parallel fashion by the Registry Intervention Systems, so that the Registry is deterred from any temptation to issue more than one alias authorization to a single member, the issuance of authorizations to false members or in the name of those who have not requested it, or arbitrary denial of said authorization. In order to ensure that opinions have not been altered, messages generated are signed in either anonymous or identified status, as relevant.

After verifying the source of the message, the Forum signs and returns a receipt that is stored in the Participating Card. The purpose of the receipt is to dissuade system managers of the temptation to modify messages or to feign non-reception. After confirming that the content accords with the publication policy, the Forum publishes the message or stores it in a protected place, wherein it notifies the author of the reasons for which the message has not been published.

Once the discussion forum is closed, the conclusion phase begins, in which the Conclusion Extractor generates, through a semantic analysis of the message published by users, the diverse conclusions or lines of argument followed in the debate.

For the purpose of validating the conclusions extracted and determining the most suitable one, they may be submitted to vote. The process affords the guarantees of security and anonymity required for a system of telematic voting [15] and all system users registered in the census may participate. The security requirements demanded of this type of system will depend on the interests to be protected in each voting process. In cases where users believe that the importance of the subject should require strong security, use of a complete system of telematic voting, which meets all the security requirements of telematic voting at the highest level, is suggested. Nevertheless, it is reasonable to assume that subjects with lesser interests at stake and where the benefits of possible fraud are lower, a reduced version of the system might be advisable.

After the voting process and achievement of results, these are transferred to the Forum, which makes them public.

4 Platform Architecture

Figure 2 shows the proposed architecture for the platform. If we analyze from the bottom up we distinguish four layers or levels. The lowest level has been termed *Digital Democracy Service Integration Platform*. This can be considered the base supporting the whole system, on which all the services necessary in the different application scenarios are placed. It is in charge of canalizing and managing all interaction between users and services. The group of services we have named intrinsic are included inside the Digital Democracy Service Integration Platform, as can be seen in the right of this figure. The other services, scenario-specific services, interact with the platform through the second level of the chart, called the *Operations and Communications Interface*. We have contemplated the possibility that these services are provided by entities outside the system, so an Operations and Communications Interface is needed to make access to all of them uniform. From what we have said up to now it can be deduced that these specific services are understood as modules which can be placed in the platform depending on the specific needs of the application scenario. This guarantees that the platform, in accordance with basic requirements, is sufficiently flexible to bear the different application scenarios. By way of example, in Figure 2 we have placed some of the services that could be applied in a citizen participation scenario in a small town.

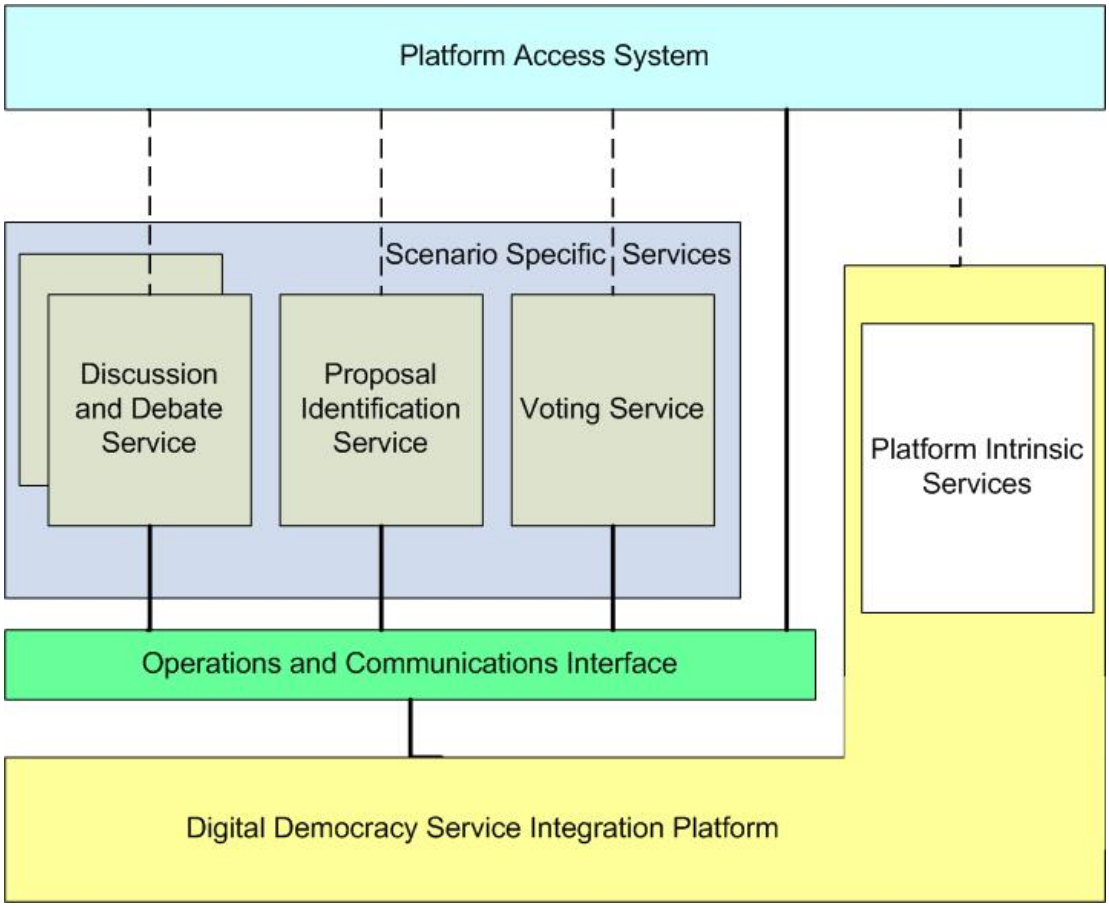

Figure 2: Platform architecture

At the highest architectural level we find the Platform Access System; that is, the application through which users interact with the platform to access the different services and facilities it offers.

Figure 2 shows the interaction both between the access system and services as well as between the access system and the platform. The dotted lines represent a logical access process, while unbroken lines represent physical access. The access system can interact with services, whether intrinsic or specific, only making use of the Operations and Communications Interface. This architecture aims to give the platform capacity to manage the use made of the different services offered.

4.1 Use of the Platform and Vision for Implementation

In Figure 3 we can see the implementation model proposed for constructing the digital democracy platform. The aim of this model is to adequately bear the requirements described in the earlier sections and the architecture defined.

As [19] did, we have chosen an architectural model for third generation Web services making use of standard protocols for the following reasons:

1. The programming environments are extendable, enabling the addition of new elements with very minor impact, thus offering more efficient implementation.

2. The technology is independent of the platform or program languages, making it very flexible and adaptable to different implementation needs, and hence allowing the use of non proprietary environments.

3. Placement of the servers in different protection zones enables the security mechanisms to be implemented efficiently in both applications and the services utilized through them.

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 1 / ISSUE 2 / AUGUST 2006 / 58 – 71

This paper is Available online at
www.jtaer.com

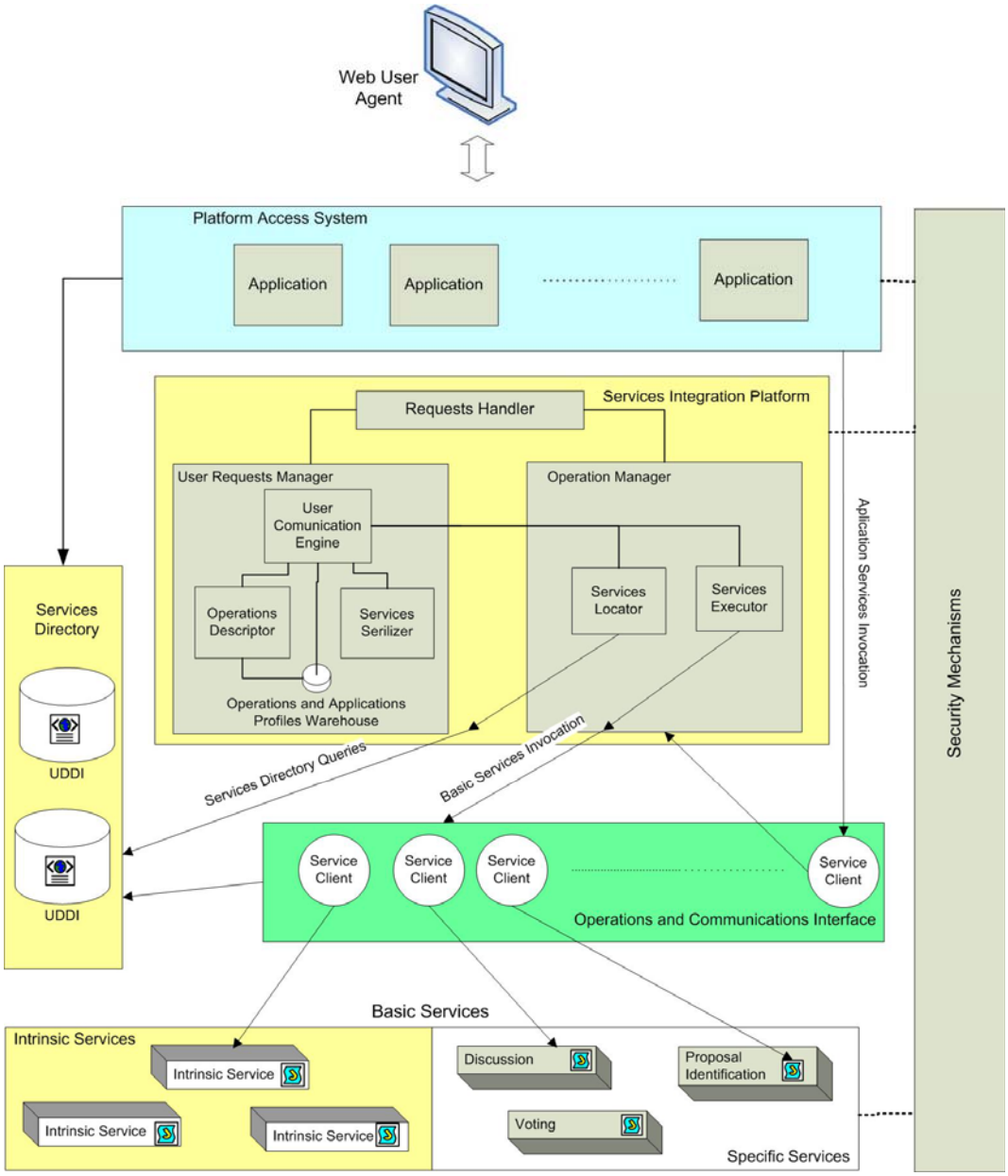

Figure 3: Implementation of the platform

1. It does not require installation of special applications on the part of the user and adapts well to use of different types of interface.

2. It uses transport and packeting mechanisms based on the Internet standards (TCP/IP, HTTP, SOAP, etc.).

Users will connect to the applications using any of the commercial devices enabling access to web applications on the Internet (Web browsers, WAP technology phones, etc.). These devices must be admitted by the servers of the organization installing the application.

Once connected, users will send the applications operation requests, together with the data associated to the operations. On receiving operation requests, the applications will connect with the platform service client and, through SOAP messages, will transfer the operations, waiting for a reply. From this moment the Digital Democracy Services Integration Platform will come into action. The platform's structure and behavior is described below.

Both the platform and basic services will be implemented as Java applications. From the Java classes using development tools, the description of the Web services will be automatically obtained in WSDL (*Web Services Description Language*). This description will be stored in a UDDI (*Universal Description, Discovery and Integration*) services registry directory.

For deployment and use of the services an Apache-Tomcat type server will be used, which has the necessary infrastructure for this task, as well as the suitable API to carry out the corresponding services invocations through SOAP.

4.2 Description of the Functional Blocks

Communication between the different components will be through Web service technology, allowing the functional blocks to reside in different servers. The fact of having several servers enables easier definition of restricted access zones. The Digital Democracy platform implementation model proposed here breaks down into the functional blocks described below and it is shown in Figure 3:

a) **Platform Access System**. Enables communication between the user and services offered by the platform. It will comprise a group of web pages and a group of resident programs (that is, HTML, JSP, Servlets files, etc.). The programs will collect user requests and invoke the Service Integration Platform to obtain the results subsequently returned to the user. Each of these applications is a possible implementation of a specific scenario.

b) **Services Integration Platform.** This is the core of the application. It manages the operation requests received from the Platform Access System, breaks down the operations into services, invokes these, receives the results and transfers them to the Platform Access System for the latter to generate replies. It divides into three functional blocks:

   1. The **Request Handler** is the access point to the services integration. It coordinates all operations and controls session holding.

   2. The **User Request Manager** takes care of controlling execution of each user operation. It receives and supervises execution of operation requested by the Platform Access System.

   3. The **Operations Manager** will take care of locating and executing each of the services into which a user operation breaks down, under the supervision of the User Requests Manager.

c) **Operations and Communications Interface**. This contains the stubs of services to be invoked through SOAP by the Services Executor which is inside of Operations Manager.

d) **Block of Basic Services**. This contains the basic services borne by the platform, whose description is found in the Services Directory.

e) **Services Directory**. This stores the WSDL descriptions of the basic services to be used by the platform applications.

f) **Security Mechanisms**. This functional block will control all security policies in a transverse manner. It is necessary to spread security mechanisms through all the elements of the system to guarantee that the platform meets the requirements established.

5 Providing Security

Having described the global architecture of the system, this section will present the solutions that have been proposed to incorporate the security necessary in order to meet the requirements demanded by users. These solutions aim at securitizing both the interaction users-web service and the interaction between the web services themselves by analyzing in each of these dialogues what security facilities must be provided. Then, we propose the incorporation of security mechanisms suitable for providing the facilities detected, with a distinction between *basic* facilities, namely those which can be provided directly in the above interactions and *advanced* facilities, which must be provided through additional interactions with the citizen participation application.

5.1 User-Service Interaction

As we have seen in the functional description, users of the platform interact with a set of services that enable performance of all the operations supported by the system. Given that the set of services is implemented as web services, said interaction becomes an exchange of SOAP messages that must be securitized.

As in any exchange of messages between applications, we can establish security at different levels, from the IP using for instance IPSec, to the application level, or at the transport level with SSL, for example, in the case under study herein, security would be included in application level, which would not preclude the use of security measures at lower levels.

When ensuring the security for the exchange of messages between the user and the services, a combination will be made of the demand for different security aspects, as appropriate:

- User authenticity. The service demands that the interaction occur with an authorized user, for which it must verify the authenticity of the messages; making certain that they have been sent by a user authorized in the system. This is usually ensured with the use of a digital signature.

- Data integrity. The exchange of messages must take place without the messages being exposed to modification or, in case they are altered, said alteration can be easily detected. This is normally ensured by using a digital signature or, if not possible, through the functions of digest or hash.

- Data confidentiality. In addition to preventing alteration, it is often indispensable or advisable for data to remain hidden from any entity for which it is not intended. Data confidentiality is normally ensured by cipher algorithms.

- Non-repudiation. Another of the interesting aspects is an exchange of message in which none of the parties involves can deny, at any time, having sent or received messages. We can distinguish here between two types of non-repudiation: non-repudiation at the origin and non-repudiation of delivery. The first ensures that if an entity sends a message it cannot deny having done so, while the second guarantees that if an entity receives a message, it cannot deny having done so.

- Anonymity. One of the outstanding characteristics of user interaction with the platform is the possibility of doing so anonymously, through use of an alias. The obtaining and using of aliases is permitted only to previously authorized users, and linking the alias to the person behind it is impossible at all times.

5.2 Interaction between Web Services

From the perspective of interaction between services, security aspects to be ensured are primarily the same as those mentioned in the preceding section. Nevertheless, there are other specific security problems, the most important of which may be that of guaranteeing that the service being interacted with is worthy of trust; that is, whether the given service's authenticity and correct performance have been verified, and is thus deserving of trust.

Web services add a new dimension to the security challenges already faced by conventional distributed systems. The security of web services is related to knowing when the web service is interacting with the right entity, when communications between elements are confidential, when messages exchanged are maintaining integrity and when entities for which web services are being invoked are known, trusted, authorized to use the service and can be clearly identified by all authorized services. In sum, the security of web services provides a level of XML-based abstraction for already existing security technologies.

Communication with web services takes place through an exchange of SOAP messages. SOAP is a packaging scheme based on XML that allows for transporting XML messages from one application to another. SOAP messages consist mainly of two parts: the header, which contains security information, and the data.

5.3 Enabling Basic Security through Web Service Standards

One form of guaranteeing authenticity in the platform is the through the use of digital signatures. Specifically, given that interactions take place between web services, and thus through the exchange of SOAP messages, which are ultimately based on XML, ensuring the authenticity of the origin entity of messages, that is, guaranteeing that the entity sending a message is in fact who it says it is, is based on the use of the standard XML Signature [2]. In like manner, one of the most important aspects of any secure exchange of data is integrity. In interaction with web services, this means the integrity of SOAP messages, which can be ensured with the use of the same standard signature.

To ensure the confidentiality of an exchange of data, cryptography is used, specifically the ciphering of messages with cryptographic algorithms that allow only the parties involved in the communication to decipher them and access their content. For the platform, the standard to be applied for information ciphering, given that SOAP messages are being exchanged, is XML Encryption [17].

For the platform, the decision was made to use the standard WS-Security [27], which related standards for security in XML and security in the exchange of SOAP messages. WS-Security involves the integration and specific application of security in XML, and thus of XML-Signature and XML-Encryption, to SOAP messages. From the perspective of their application to the platform presented, it enables providing for the integrity, authenticity and confidentiality of messages exchanged in the use of services, whether internal or external to the Digital Democracy platform.

WS-Security provides a simple model for secure messaging that will be used when the number of messages exchanged in an interaction is small. Should a more continuous or intensive exchange of messages prove to be necessary, the standard WS-SecureConversation will be used [1], which enables the establishment of security contexts that facilitate and optimize the exchanges of series of messages between entities.

The description of the platform shows that it can make use not only of its own services but also external ones as well, meaning that they could belong to different environments. This possibility constitutes a significant security challenge, for in addition to having to ensure the integrity and confidentiality of interactions, it must identify users or entities in different domains of trust, create and maintain the digital credentials, and specify the access permits for resources.

To facilitate portability of identities between platforms and thus, between domains of trust, use will be made of the specifications in he XML standard called *Security Assertion Markup Language* (SAML) [3] combined with WS-Security. The latter enables transport of SAML assertions, and thus facilitates identity portability in the use of web services, which is crucial when working with web services that belong to different trust domains.

When specifying the permissions and security conditions for access to services in the platform, we will use the definitions in the WS-SecurityPolicy [6], so as to establish policies that enable agreeing conditions of interaction between web services in terms of security.

5.4 Enabling Advanced Security through Application

The provision of advance non-repudiation and anonymity facilities differs in form from the provision of basic facilities in so far as the user must, in this case, interact with the debate application in order to obtain some information that will enable subsequent user-service interaction. Then, detailed comments are made on the procedures that are to be incorporated to the application and which will require the user to engage in additional interactions with it.

5.4.1 Non-repudiation

Repudiation is the fraudulent denial by an entity that it is the author of a message that it has in fact sent, or that it is the receiver of a message that the system has delivered to it.

In the PARTICIPA system, special stress is laid on the information flow between the user and the application and vice-versa, with the particular fact that users can act in an identified capacity or anonymously. A communicating entity cannot repudiate authorship of a message when the receiving entity shows a message signed by the author. Although the issuer of the message may decide the remain anonymous, the same algorithms will be applied to the signature, but this time with a secret key that is paired with a public key registered for the alias. Thus, non-repudiation at the origin is ensured in any of these cases.

To expose fraudulent actions in which the system could deny reception of a message (repudiation of delivery) must return a signed receipt to be stored in the user's Participating Card. If this message is not stored, it will be an indication that the operation did not terminate in a satisfactory manner.

5.4.2 Anonymity

The user must interact first with the Register within debate application, which provides an alias for anonymous participation. After obtaining an alias, all interactions become anonymous, since alias received is completely detached from the real identity of the user. The alias acquisition process is based on the use of the blind signature and can be summarized in the following steps:

1) At the Participation Point, the user inserts their Participating Card in a card reader and authenticates it with the PIN (*Personal Identifier Number*).

2) The Participating Card contains the pair of asymmetrical user keys, both public and private that identifies its owner. In addition, the card generates another pair of asymmetrical keys that can be used to obtain an alias and to participate anonymously in votes. The keys generated - k_{dM}, k_{cM} – are stored in such a way that not even the user can read them. The card also generates blinding factors so that the k_{dM} key previously generated is blinded (using the blinding factors) for the Registry and each of the Registry Intervention System, thus yielding a blinded k_{dM} key for each of the message's destination entities.

3) Through a dialogue process, the card delivers to the Participation Point the different blinded keys signed by the user, with an indication of the recipient of each. In addition, it delivers the signed user ID. The card encrypts all this data with the public key of the Registry so that only the Registry can read them; the Participation Point generates an APDU (Application Protocol Data Unit) and sends it to the Registry.

4) The Registry reads and deciphers the APDU. Then it sends all the data to all the Registry Intervention Systems. Each of the Intervention Systems, like the Registry, must verify if the user ID received is correct; if not data are rejected. The fact that the Registry engages in a parallel with the Registry Intervention Systems

the verification that the request made is correct allows all, in the event of an incidence, to have the same probe of it. The main function of the Registry Intervention Systems is to supervise the actions of the Registry so as to prevent manipulation.

5) Following verification that the user ID received is valid; the Registry Intervention Systems will make a blind signature of the corresponding blinded k_{dM} key and return the result to the Registry. The Registry does the same with its blinded k_{dM} key and attaches it to all the signed blinded keys received from the Registry Intervention Systems, thus forming a keys package. This keys package is signed by the Registry and encrypted with the public user key, after which it is sent by means of an APDU to the participation point.

6) The Participation Point delivers to the user's Participating Card the data contained in the APDU which was received from the Registry so that the latter is the only one who can eliminate the encryption protecting it and verify the signature. Then it eliminates one-by-one the blinding factor, thus obtaining a k_{dM} signed by the Registry, the k_{dM} signed by the Registry Intervention System 1, the k_{dM} signed by the Registry Intervention System 2 and so on. It then verifies that the signatures of the Registry and the different Registry Intervention Systems are correct. If so, the user has the information necessary to initiate negotiation with the Alias Manager and obtain an identifier (alias) without losing the guarantee that only authorized members of the collective can participate in the debate, while also preventing use of the same alias by more than one member. The pair of keys (k_{dM} and k_{cM}) will be for the alias what a public key and secret one are for user name. The key for signing the message or encrypting the vote, (k_{cM}); will never leave the card that has generated it. The other member of the pair (k_{dM}), which is used to verify the message signature or decipher the vote has been, as we have seen, previously blinded in the card to prevent subsequent relationships between the keys and its owners.

7) If a user should decide to obtain an alias to be able to participate anonymously in the debates, from the Participation Point will interact with the Alias Manager. The latter has a public list of the aliases already used for the forum, so that the user will choose an unused alias. In the card, a chosen alias with the key k_{cM} will be signed and the result will be concatenated with the k_{dM} key signed by the Registry and the Registry Intervention Systems. The Participation Point will form an APDU with the above data and send it to the Alias Manager.

8) The Alias Manager, when receiving the data, verifies that both the signatures of the k_{dM} key by the Registry and the Registry Intervention Systems and the signature of the alias with the k_{cM} key are correct. If everything is correct, it then verifies that the alias chosen is not among those already in use, and if so, the alias is associated to the k_{dM} key received and is published on the list of used aliases for that forum. Then it will sign the data received and return it to the Participation Point.

9) The Participation Point will deliver what it has received to the Participating Card, where the signature of the Alias Manager will be verified; if it is correct, it will be established as the alias chosen by the user.

6 Conclusions

Systems of digital democracy are still in a period of maturation, both from the technological point of view and from a functional, social one. In this first phase, digital democracy must be brought to the citizens through the design of attractive systems that are easy to use and which arouse their interest. Moreover, public authorities must lose their suspicion of systems of digital democracy– for these constitute the most direct form of control by citizens over decisions affecting them- and instead lend full support to their use in decision-making processes.

After this stage of "making contact" is overcome, systems of citizen participation must increase the services they offer in order to be useful in more critical environments, realms in which there may be a manifest interest on the part of individuals, organizations or authorities to not adequately reflect the participants' opinions, with the aim of reaching certain conclusions. For these circumstances, the system of citizen participation should contain mechanisms for detecting any possible anomalies in the system, such as the loss or alteration of messages.

Moreover, there are numerous scenarios of citizen participation in which users consider possible anonymous involvement to be a requisite for partaking. In these cases, anonymity must be provided with the due guarantees, wherein the obtaining and using of aliases is permitted only to previously authorized users, and linking the alias with the person behind it is impossible at all times.

The platform for citizen participation presented in this article is designed to meet the security requirements demanded by users, not only as regards what we would call *basic aspects,* such as guaranteeing user authenticity, the integrity or confidentiality of data, but also through he provision of *more advanced* aspects that enable ensuring the anonymity of participants and the non-repudiation of messages sent in a forum. At this stage of design, we have analyzed the emerging security standards in web services to verify their applicability in the scenario of participation proposed, and we have found that it is quite feasible to provide the basic services indicated through a standardized secure dialogue between the user and the web service or between web services. However, providing guarantees of

anonymity and non-repudiation – both for the user and for the forum to which a message is sent – demands specific mechanisms in the application, and these are also presented herein.

Therefore, we believe that the solution discussed in this article for the development of a platform of digital democracy that ensures freedom of speech will help encourage citizen's confidence in the use of these systems.

At present, the work of the VOTESCRIPT group aims, first, at the implementation of a specific scenario of digital democracy that would reflect the performance of the platform described in this paper. Thus, we have chosen to apply it in a scenario of citizen participation in medium-sized municipality, with a relatively young population where citizens are accustomed to using computers. A new sociological study will determine our successes and challenges for the next steps.

Moreover, this group continues to work on another aspect of the requirements for the platform related to the deployment of applications and their design strategy, so that in the future they can be configured for multiple scenarios and interact with other platforms and thereby enable expansion of the services provided to users of these systems in a systematic and organized manner.

References

[1] S. Anderson et al. (2005). Web Services Secure Conversation Language (WS-SecureConversation). Public Draft. [Online]. Available: [ftp://www6. software.ibm.com/software/developer/library/ws-secureconversation.pdf].
[2] M. Bartel, J. Boyer, B. Fox, B. LaMacchia and E.Simon. (2002). XML-Signature Syntax and Processing. W3C Recommendation. [Online]. Available: [http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/].
[3] C. P. Cahill. (2005). OASIS Standard. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. [Online]. Available: [http://docs.oasis-open.org/security/saml/v2.0/].
[4] J. Carracedo, Seguridad en redes telemáticas. Ed. Madrid:McGraw-Hill. 2004, pp. 458–467 and 522–534.
[5] Ciudadanos2005. (2005). A participative democratic experience. [Online]. Available: [http://www.ciudadanos2005. net].
[6] G. Della-Libera et al. (2005). Web Services Security Policy Language (WS-SecurityPolicy). Public Draft. [Online]. Available: [ftp://www6.software.ibm.com/ software/developer/library/ws-secpol.pdf].
[7] DEMOS. (2003). Delphi Mediation Online System. [Online]. Available: [http://www.demos-project.org]
[8] DUNES. (2005). Dialogic and Argumentative Negotiation Educational Software. [Online]. Available: [http://www. tessera.gr/dunes].
[9] Europa Press. (2005). [Online]. Available: [http://www.europapress.net/default.aspx?opcion=sociedad].
[10] EURO-CITI. (2002). European Cities Platform for On-line Transaction Services. [Online]. Available: [http://www. euro-citi.org/].
[11] C. Gilbert, (2003, September). The changing role of the citizen in the e-Governance & e-Democracy equation, Commonwealth Centre for e-Governance. [Online]. Available: [http://www.electronicgov.net/pubs/research_ papers/cath/index.shtml].
[12] A. Glassner, B. B. Schwarz, The Synchronous Mapping Discussions: The Effects of Floor Control in Turn-Taking and Choice of Argumentative Representations, in Proceedings of the information Visualisation, 8th international Conference on (Iv'04), Washington, DC, July 14-16, 2004, IEEE Computer Society, pp. 899-902.
[13] A. Gómez, C. González, S. Sánchez, E. Pérez and J. Moreno, Architectural design for a Digital Democracy telematic platform, in Proceedings of 2th International CollECTeR LatAm, Talca, Chile, 2005, pp. CDROM.
[14] A. Gómez, E. Pérez, S. Sánchez, J. Moreno and C. González, Diseño de un sistema avanzado de Democracia Digital garante de la libertad de expresión, in Proceedings of 3th Congreso Iberoamericano de Seguridad Informática (CIBSI05), Valparaiso, Chile, 2005, pp. CDROM.
[15] A. Gómez, E. Pérez, S. Sánchez, J. Carracedo, J. Moreno and J.D. Carracedo, VOTESCRIPT: telematic voting system designed to enable final count verification, in Proceedings of 2th International CollECTeR LatAm, Talca, Chile, 2005, pp. CDROM.
[16] T. F, Gordon, G. Richter, Discourse Support Systems for Deliberative Democracy, Lecture Notes in Computer Science, Volume 2456, Jan 2002, pp. 248–255.
[17] T. Imamura B, Dillaway, E. Simon. (2002). XML Encryption Syntax and Processing. W3C Recommendation. [Online]. Available: [http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/].
[18] D. Lyon, Surveillance Society, monitoring every day life. Open University Press. Buckingham: 2001.
[19] B. Medjahed and A. Bouguettaya, Customized Delivery of E-Government Web Services, IEEE Intelligent Systems, vol. 20, no. 6, 2005, pp. 77-84.
[20] J. Padget, E-Government and E-Democracy in Latin America, IEEE Intelligent Systems ,vol. 20, no. 1, 2005, pp. 94-96.
[21] J. Paralic, T. Sabol, M. Mach, First Trials in Webocracy, Lecture Notes in Computer Science, Volume 2739, Jan 2003, pp. 69–74.
[22] Research actions by the Digital Democracy and Citizenry Rights on Internet Ada Byron Observatory, (2001). [Online]. Available: [http://www.democraciadigital.es/rubrique.php3?id_rubrique=2#ar9].
[23] T. Sabol. WEBOCRACY. (2004). Web Technologies Supporting Direct Participation in Democratic Processes. [Online]. Available: [http://europa.eu.int/information_society/activities/policy_link/documents/factsheets/egov_ webocracy.pdf].

[24] O. Saebo, T. Paivarinta, Autopoietic Cybergenres for e-Democracy? Genre Analysis of a Web-Based Discussion Board, in Proceedings of 38th Annual Hawaii International Conference, Hawaii, 2005, pp. 98c, Jan. 2005.
[25] E. Tambouris, S. Gorilas, Evaluation of an e-democracy Platform for European Cities, Lecture Notes in Computer Science, Volume 2739, Jan 2003, pp. 43-48.
[26] TED Project, (2002). Towards Electronic Democracy. [Online]. Available: [http://infodoc.escet.urjc.es/ted/].
[27] G. Thurston et al. (2004). Web Services Security: SOAP Message Security 1.0 (WS-Security 2004). OASIS Standard 200401. [Online]. Available: [http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf].