Diseño de un sistema avanzado de democracia digital garante de la libertad de expresión

Ana Gómez Oliva, Emilia Pérez Belleboni, Sergio Sánchez García,
Jesús Moreno Blázquez, Carlos González Martínez

Departamento de Ingeniería y Arquitecturas Telemáticas de la Universidad Politécnica de Madrid.
E.U.I.T de Telecomunicación. Ctra. Valencia km.7. 28031 Madrid. España.
{agomez, belleboni, ssanche, jmoreno, cgonzalez}@diatel.upm.es

Resumen. En este artículo se presenta el diseño de un sistema avanzado de democracia digital, con énfasis en la protección a la libertad de expresión de los ciudadanos, ofrecida mediante el empleo de tarjetas inteligentes y mecanismos avanzados de seguridad. Se regulan los procedimientos de obtención de alias para conseguir la participación anónima de quien lo desee, garantizando que con su uso se oculta la identidad real del usuario (incluso al propio sistema), asegurando, en todos los casos, que únicamente las personas autorizadas pueden participar en el foro correspondiente y proporcionando garantía de integridad de la información, tanto en tránsito como almacenada. Asimismo, los ciudadanos disponen de pruebas criptográficas robustas que les permiten evidenciar cualquier funcionamiento anómalo del sistema que pudiera desembocar en la destrucción o modificación de opiniones y en la consiguiente alteración de las conclusiones o resultados de la participación.

1. INTRODUCCIÓN

El desarrollo de la Sociedad de la Información está promoviendo la puesta en marcha de nuevos servicios telemáticos, cuyo objetivo final es mejorar la calidad de vida de los ciudadanos. Uno de los servicios con más repercusión en los medios de comunicación es el de democracia digital (o gobierno electrónico), donde son relativamente frecuentes las noticias recogiendo alguna nueva iniciativa promovida por Gobiernos o Administraciones.

Sin embargo, un rápido análisis de estas noticias advierte de que existe cierta confusión o abuso en el término *democracia digital*. En una gran mayoría de casos este término ha pasado a ser aplicado a cualquier iniciativa gubernamental destinada a acercar la Administración al ciudadano y facilitarle la realización de trámites a través de una *ventanilla única*. Son pocas las noticias que hacen referencia a sistemas digitales de participación ciudadana como tales, esto es, a sistemas puestos a disposición de los ciudadanos para que puedan expresar sus opiniones libremente, con el objetivo de fomentar la relación de los ciudadanos entre sí y de éstos con las Autoridades, y en los que puedan extraerse unas conclusiones que faciliten la toma de decisiones a partir de las opiniones emitidas, todo ello dentro de los límites del respeto mutuo.

También las experiencias sobre voto digital o voto telemático suelen recogerse bajo el título de *democracia digital* y aunque, evidentemente, la participación ciudadana a través del voto es una cualidad intrínseca de la democracia, en este artículo se considera que la votación es una herramienta fundamental que debe formar parte de los sistemas de democracia digital, pero que estos deben tener como requisito básico la participación interactiva y el intercambio de opiniones entre los participantes, previo a la adopción del resultado final.

Con este enfoque, en España se están desarrollando multitud de experiencias basadas en el principio de participación de los ciudadanos en los asuntos públicos, y muy especialmente, se está promoviendo la creación de foros de debate relacionados con temas municipales. Dentro de estas iniciativas cabe destacar por el número de ayuntamientos implicados el proyecto *Ciudadanos2005* [1], organizado por Europa Press con la colaboración del Ministerio de Industria, Turismo y Comercio español en el que participan 80 pequeños y medianos ayuntamientos implicados en programas de fomento de la Sociedad de la Información para todos. También se han puesto en marcha otras iniciativas con la intención de acercar los políticos a los ciudadanos. Dentro de éstas cabe citar el *Parlament Obert* de Catalunya [2], pionero en este tipo de iniciativas y las plataformas *andalucia2004.net* [3], *candidatos2004.net* [4], y *galicia2005.net* [5], desarrolladas por Europa Press para las elecciones al Parlamento de Andalucía, al Parlamento Europeo y a la Xunta de Galicia respectivamente, y que han permitido a los ciudadanos comunicarse con los candidatos, haciéndoles llegar preguntas y sugerencias, susceptibles de ser respondidas públicamente y que podían ser conocidas por el resto de los ciudadanos.

A nivel europeo hay que destacar las iniciativas puestas en marcha por el V y VI Programa Marco de la Unión Europea. Dentro de éstas, el proyecto DEMOS [6] ha sido uno de los más relevantes, ya que ha abordado la democracia digital desde el punto de vista del proceso de discusión, analizando y proponiendo nuevas metodologías que permitan la comunicación interactiva entre gran número de personas, metodologías capaces de agregar e interrelacionar las distintas contribuciones individuales, identificar y promocionar los aspectos más prometedores de la discusión, perfilar diferentes posiciones y esforzarse por conseguir la convergencia entre ellas. Todo ello con el objetivo de alcanzar un resultado, que pueda influir en los procesos de toma de decisiones de los políticos. El proyecto DUNES [7] también resulta interesante por sus aportaciones en el terreno de las discusiones constructivas: conseguir que los ciudadanos sean capaces de debatir sobre los temas que les preocupan, colaborando entre ellos y participando de forma respetuosa. Otro proyecto destacable es el WEBOCRACY [8], cuyo objetivo ha sido dotar a los ciudadanos de un sistema innovador de votación, acceso y comunicación para conseguir un aumento de la participación ciudadana en los procesos de decisión. También hay que mencionar el proyecto EURO-CITI [9], que ha desarrollado una arquitectura de servicios común destinada al sector público, incluyendo los servicios de votación, entrega electrónica de formularios y consulta ciudadana. Otro importante proyecto sobre democracia digital, que está orientado a la toma de decisiones, es el proyecto TED [10]. El objetivo de este proyecto es desarrollar nuevas técnicas, basadas en metodologías bayesianas, que faciliten un resultado a un problema para el que obligatoriamente es preciso sopesar múltiples fuentes de incertidumbre, donde

existe conflicto de intereses y se hace necesaria la integración de opiniones y deseos de grupos dispares.

El análisis de las experiencias citadas, tanto a nivel nacional como a nivel europeo, permite extraer una serie de conclusiones sobre las características que debe reunir todo sistema de participación ciudadana para su buena acogida:

1. En primer lugar es preciso hacer frente al problema de la *estratificación o brecha digital*. Aunque cada día son más las iniciativas gubernamentales apoyando la introducción de los ordenadores en todos los ámbitos de la vida, todavía existe un porcentaje muy elevado de personas que nunca han tomado contacto con un ordenador. Especialmente para ellas, se hace indispensable que los sistemas de participación ciudadana sean fáciles y cómodos de utilizar.
2. Los temas objeto de debate deben ser muy cercanos a los participantes. En esta línea los sistemas de participación ciudadana orientados al debate sobre asuntos municipales se han mostrado muy atractivos para los ciudadanos.
3. Debe existir un compromiso por parte de las Autoridades correspondientes de que las conclusiones del debate serán tenidas en cuenta en la decisión final. Se ha constatado que uno de los aspectos que incide más negativamente en el éxito de un foro es que las opiniones emitidas tengan un valor meramente testimonial, y que no se hayan definido mecanismos claros para transmitir esa opinión a los órganos competentes.
4. El proceso de discusión debe estar claramente estructurado en fases bien definidas: selección de temas de interés, expresión de opiniones de los participantes y extracción de conclusiones. Esta última fase puede realizarse mediante un procedimiento de votación o un procedimiento automático o semiautomático que extraiga conocimiento de los mensajes emitidos.
5. El sistema debe garantizar ciertos aspectos de seguridad relativos a la garantía de identidad de los participantes, almacenamiento seguro de la información y no manipulación de la misma.

Es quizás este último aspecto el más descuidado en los sistemas de democracia digital, ya que muy pocos de los sistemas mencionados incluyen los mecanismos adecuados para garantizar que los mensajes depositados provienen efectivamente de quienes dicen ser o de que éstos no han sido manipulados o eliminados del sistema por contener opiniones contrarias al *interés* perseguido por los organizadores. Incluso muchos de los foros abiertos en municipios no realizan ningún tipo de control de acceso sobre los participantes o éste es incompleto, de manera que los sistemas pueden verse inundados por mensajes de participantes a los que no les corresponde opinar o decidir sobre el objeto de consulta.

Más aún, si se considera que los sistemas de democracia digital implementados hasta la fecha en los municipios son sólo el primer paso hacia nuevos escenarios de participación ciudadana, veremos que se hace necesario proporcionar garantías de seguridad similares a las existentes en los sistemas de votación convencionales.

En efecto, el tema de la seguridad en los sistemas de debate adquiere relevancia especial en determinados entornos que pueden considerarse como muy sensibles. Un ejemplo de ellos puede ser el de una empresa o factoría que desee fomentar la participación de los empleados en las decisiones colectivas, pero donde éstos puedan sentirse coaccionados por los directivos o por otros empleados al emitir sus opiniones.

Casos similares pueden producirse en otros entornos como partidos políticos, sindicatos o distintos tipos de organizaciones sociales. Desde otro punto de vista, los vaivenes históricos hacen conveniente proporcionar vías que permitan preservar la identidad de los ciudadanos frente a posibles cambios políticos, impidiendo que personajes malévolos pudiesen beneficiarse de la existencia de completas bases de datos con información sensible sobre cada uno de los ciudadanos. En estos casos, además de los requisitos anteriormente mencionados, se hace necesario garantizar el anonimato de los participantes (tal y como ocurre en las votaciones), de manera que las opiniones puedan ser vertidas en el foro sin miedo a posibles represalias ahora o en el futuro.

A partir del análisis de los sistemas de democracia digital citado anteriormente y teniendo en cuenta las consideraciones sobre seguridad mencionadas más arriba, se han identificado una serie de aspectos de buen funcionamiento que deberían ser garantizados por cualquier plataforma de democracia digital, con independencia de la honestidad y competencia profesional de las personas a cargo del funcionamiento del sistema:

- Libertad de expresión, de manera que todos los usuarios de la plataforma puedan expresarse libremente, sin temor a represalias en el presente o en el futuro.
- Igualdad, para que las opiniones de todos ciudadanos tengan la misma importancia.
- Respeto mutuo. Las opiniones expresadas públicamente deben respetar unas reglas definidas y aceptadas por los propios participantes del foro (política de uso).
- Duración determinada de las discusiones. Los temas sujetos a discusión tendrán un tiempo de vida convenido y conocido por los usuarios al iniciarse el debate (que puede ser ampliado si las circunstancias lo requieren).
- Auditabilidad, de manera que los ciudadanos participantes dispongan de información veraz para poder verificar el correcto funcionamiento del sistema.
- Validación de las conclusiones obtenidas bien sea por consenso o por medio de una votación. En este último caso, el sistema deberá garantizar la limpieza del proceso de votación (aunque se considera que este proceso pueda ser proporcionado con distintos grados de seguridad según lo requieran los temas tratados y los usuarios participantes en el foro).

Este artículo presenta una propuesta de un sistema seguro de democracia digital que incorpora nuevas funcionalidades requeridas para garantizar la autentificación de los usuarios participantes, permitir la participación anónima de los usuarios que lo deseen y verificar el correcto funcionamiento del sistema frente a la manipulación o fraude encaminado a alterar las conclusiones o resultados de la participación. Esta propuesta se encuadra dentro de las tareas que este grupo de investigación lleva a cabo en el proyecto *Desarrollo de una plataforma telemática segura para el soporte de escenarios de Democracia Digital* (Proyecto TIC 2003-2141), subvencionado por el Ministerio de Industria, Turismo y Comercio español en el que se está desarrollando una plataforma de democracia digital en la que se integran los distintos servicios de seguridad contemplados en este artículo [15].

2. ARQUITECTURA GLOBAL DEL SISTEMA PROPUESTO

Para satisfacer los requisitos de funcionamiento mencionados en el apartado anterior, es necesario dotar al sistema de mecanismos de seguridad robustos. La propuesta recogida en este artículo se basa en el empleo de algoritmos criptográficos de clave simétrica y asimétrica y en el opacado y firma ciega de la información intercambiada entre las distintas entidades que forman parte del sistema [14].

A continuación se definen las distintas entidades, para luego describir esquemáticamente el comportamiento global del sistema de debate. En el siguiente apartado se recoge con detalle el flujo de información intercambiado entre ellas y las garantías de seguridad proporcionadas.

2.1. Entidades participantes

En el escenario que se propone intervienen un conjunto de sistemas automáticos que funcionan bajo un software cuyo código habrá sido previamente publicado, con la consiguiente posibilidad de auditoría por parte de las entidades correspondientes. En la Fig. 1 se representa la relación entre los sistemas que a continuación se describen:

- Puntos de Participación (PP). Se trata de ordenadores con conexión a Internet y equipados con lector de tarjetas inteligentes, a través de los cuales los usuarios podrán interactuar con el sistema. Pueden ser ordenadores situados en el hogar del usuario, en su centro de trabajo, en lugares públicos como por ejemplo una biblioteca o un cibercafé, etc. La emisión de opiniones en un lugar público evitará que una pesquisa exhaustiva permita localizar al autor de un mensaje anónimo a partir de la dirección de red de la máquina desde la cual se emitió.
- Registro (Rg). Se trata de la entidad encargada de autenticar a los usuarios y de proporcionarles un alias en el caso de que deseen que su participación en los debates sea anónima. Será además la encargada de entregar a todos los usuarios la autorización de entrega de voto necesaria para participar en los procesos de votación de los resultados obtenidos durante la discusión.
- Sistemas de Intervención de Registro (SIR). Complementan y supervisan la labor del Registro, realizando los mismos procesos que éste en paralelo. Cada uno de ellos está controlado por un Interventor de Registro.
- Foro (Fo). Como su propio nombre indica es el sistema encargado de dar soporte a los debates que tengan lugar en el sistema, recibiendo y publicando las opiniones de los usuarios autorizados y almacenando todo lo recibido para posibilitar auditorías de funcionamiento en caso de ser requeridas.
- Gestor de Alias (GA). Es la entidad encargada de garantizar que no existen alias repetidos en el sistema. Mantendrá una lista pública de los alias que están siendo utilizados en cada foro.
- Extractor de Conclusiones (EC). Se encargará, mediante análisis semántico de la información publicada en el foro durante una discusión, de la extracción de conocimiento útil. Básicamente extraerá las principales líneas de argumentación con la intención de que, posteriormente, puedan ser sometidas a votación.

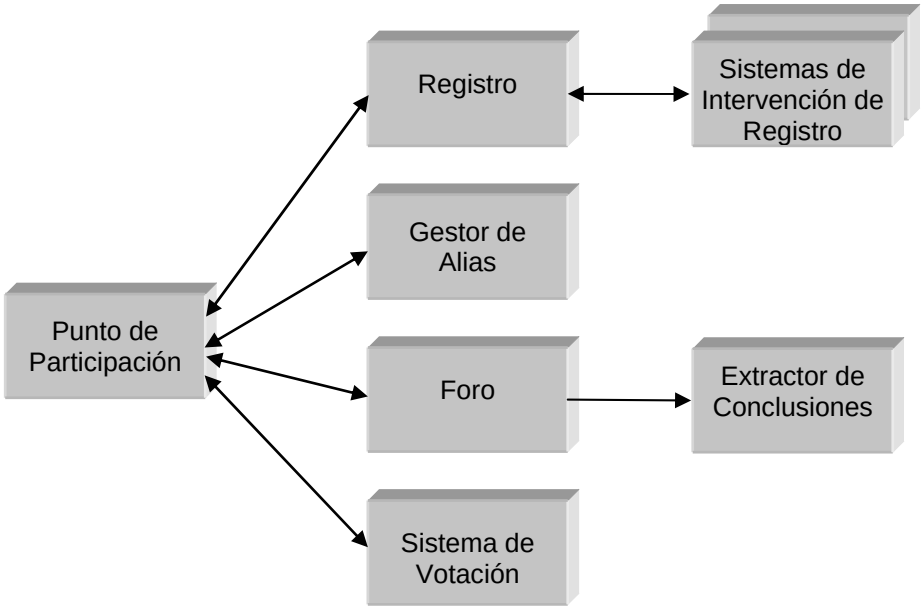

Fig. 1. Agentes del sistema

- Sistema de votación. Será el encargado de recoger los votos emitidos por los distintos usuarios del sistema durante los procesos de votación de las conclusiones. Realizará el recuento de los votos una vez finalizado el período de recepción de los mismos y la publicación de los resultados.

Además de las distintas entidades o sistemas automáticos que se acaban de presentar, participan en el sistema las siguientes personas:

- Usuarios. Cada persona registrada en el censo de participantes puede interactuar con el sistema como usuario, tanto mediante la observación del progreso de la discusión como mediante la emisión de opiniones en el foro. Así mismo todos los usuarios podrán participar en la votación de las conclusiones obtenidas tras el debate. Cada usuario estará en posesión de una Tarjeta de Participación. Se trata de una tarjeta inteligente resistente a manipulaciones que permite llevar a cabo múltiples operaciones criptográficas.
- Un Gestor del Registro responsable del sistema Registro.
- Interventores del Registro responsables de cada uno de los Sistemas de Intervención de Registro.
- Moderador. Será el encargado de controlar que los debates no se desvíen del tema a propósito del que fueron creados. Los mensajes enviados al foro de discusión por el Moderador no serán tenidos en cuenta por el Extractor de Conclusiones.
- Invitados. Serán usuarios que a pesar de no estar en el censo de participantes podrán participar en las distintas fases del proceso de discusión siempre de forma identificada. Su número estará limitado y existirá un censo de invitados. Su opinión no será tenida en consideración por parte del Extractor de Conclusiones.

2.2. Formas de participación

En el sistema se contemplan dos formas de participación para los usuarios a la hora de emitir sus opiniones en un foro o discusión: la participación anónima mediante el uso de un alias y la participación identificada, en la que el usuario emite sus opiniones haciendo uso de su identidad real (su nombre y apellidos reales). La participación en las votaciones es en todos los casos anónima.

2.3. Funcionamiento global

Cada foro de debate creado lleva asociado un censo de individuos a los que les está permitido participar en el mismo (por ejemplo, mayores de edad, residentes en el municipio, trabajadores de la empresa, socios del club deportivo, etc.). Sin embargo, no es objetivo de este artículo determinar el ámbito de ciudadanos que tienen derecho a participar en un foro determinado, sino que se parte del supuesto de que alguna autoridad competente ha confeccionado un censo con los individuos que reúnen los requisitos para participar en ese foro.

Estos ciudadanos autorizados disponen de su Tarjeta de Participación, que les sirve tanto de elemento de identificación, como de soporte para la realización de procesos criptográficos críticos (de manera que no queden huellas en los ordenadores empleados que puedan dar lugar a ataques posteriores). Asimismo, esta tarjeta almacenará resguardos de las operaciones realizadas, útiles en caso de detección de malfuncionamiento del sistema.

Cuando un ciudadano desee emitir su opinión en algún foro en el que se encuentre autorizado a hacerlo, acudirá con su Tarjeta de Participación a alguno de los Puntos de Participación, desde donde podrá verter sus opiniones y participar en las votaciones.

Si el usuario desea participar en el foro de forma anónima deberá haber completado previamente un dialogo con la entidad Registro para obtener una autorización que le permita negociar un identificador (alias) con el Gestor de Alias. En el proceso de obtención del alias se ofrecen las garantías, aparentemente contradictorias, de autenticidad (solo los miembros autorizados pueden participar en el debate) y privacidad (el sistema garantiza el anonimato de los participantes de forma que ni el propio sistema puede relacionar un alias con su propietario). Asimismo, el sistema impide la utilización de un mismo alias por más de un participante en el foro.

La tarea de la entidad Registro se ve supervisada y controlada en paralelo por los Sistemas de Intervención de Registro, de manera que se impida la emisión de más de una autorización de alias a cada miembro que lo solicite, la emisión de autorizaciones a falsos miembros o en nombre de los que no lo han solicitado.

Con objeto de garantizar que las opiniones emitidas no han sido alteradas, los mensajes generados son firmados. Aquellos mensajes emitidos de forma anónima (bajo un alias) se firman con la clave generada para el Foro, mientras que los emitidos bajo la identidad real se firman con la clave privada de su autor.

El Foro, tras verificar la procedencia del mensaje devolverá un comprobante firmado por él, que se almacenará en la Tarjeta de Participación. El objetivo de este

comprobante es disuadir a los responsables del sistema de la tentación de modificar mensajes o de fingir no haberlos recibido. Después de comprobar si el contenido se ajusta a la política de publicación, y según proceda, el Foro publicará el mensaje o lo almacenará en un sitio protegido, notificando en su caso al autor de los motivos por los cuales su mensaje no se publica.

Una vez concluido el plazo de emisión de opiniones, la entidad Extractor de Conclusiones, a partir de los mensajes recogidos en el foro, obtendrá las principales líneas de argumentación, empleando para ello mecanismos automáticos, manuales o mixtos. Asimismo, el sistema propuesto contempla la posibilidad de que las conclusiones obtenidas puedan ser sometidas a votación. La complejidad del sistema de votación podrá ser modulada de acuerdo a los intereses puestos en juego.

3. DESARROLLO DE LA PROPUESTA

A continuación se desarrolla la propuesta presentada en el apartado anterior, describiendo de forma detallada los procesos necesarios para poder participar en los debates y votaciones y la forma en que dicha participación tiene lugar.

3.1. Procedimiento de obtención de alias, debate, extracción y votación de conclusiones

A continuación se detalla la forma en que los usuarios pueden participar en los debates. La notación criptográfica empleada en las distintas expresiones que aparecen a lo largo del texto es la siguiente:

m1, m2	Concatenación de los mensajes *m1* y *m2*.
$A_P\ [m]$	Cifrado del mensaje *m* con la clave pública de *A*.
$A_S\ [m]$	Cifrado del mensaje *m* con la clave privada de *A*.
$A_{sig}\ [m]$	Firma del mensaje *m* por parte de *A* (mensaje *m* en claro y cifrado del hash con la clave privada de A).
$Alias_{sig}\ [m]$	Firma del mensaje *m* por parte de un usuario que hace uso de alias (mensaje *m* en claro y cifrado del hash con la clave k_{cM}).
$O_A\ (m)$	Opacado del mensaje *m* para la entidad *A*.
$A_{bsig}[O_A\ (m)]$	Firma ciega por parte de *A* del mensaje *m* opacado[1].

3.1.1 Obtención de alias

A la hora de debatir en los foros, los usuarios pueden emitir sus opiniones de dos formas distintas, anónima o identificada. En ambos casos hacen uso de su tarjeta inteligente, pero en el caso de la participación anónima es necesario realizar un proceso previo de obtención de alias tal que el alias obtenido se desvincule totalmente

[1] El uso de la notación $A_{bsig}[O_A\ (m)]$ resulta redundante, pues si lo que se está firmando es algo opacado la firma es ciega. No obstante, para mayor claridad se utiliza esta notación a lo largo del documento, siempre teniendo en cuenta que es equivalente y podría ser sustituida por $A_{sig}[O\ (m)]$.

de la identidad real del usuario. Dicho proceso se basa en el uso de la firma ciega (*blind signature*) y puede resumirse en los siguientes pasos:

1. En el Punto de Participación, el usuario introduce su Tarjeta de Participación en un lector de tarjetas y se autentica ante ella mediante un PIN (*Personal Number Identifier*).
2. La Tarjeta de Participación contiene la pareja de claves asimétricas (pública y privada) del usuario. Además, en la tarjeta se generan otro par de claves asimétricas que servirán tanto para la obtención de alias como para la participación en las votaciones de forma anónima. Las claves generadas (k_{dM}, k_{cM}), se almacenan de forma que ni el propio usuario puede leerlas. La tarjeta genera además los factores de opacidad de tal manera que la clave k_{dM} previamente generada se opaca (usando dichos factores de opacidad) para el Registro y para cada uno de los Sistemas de Intervención de Registro, dando lugar a una clave k_{dM} opacada para cada una de las entidades destino del mensaje. Mediante un proceso de diálogo, la tarjeta entrega al Punto de Participación las distintas claves opacadas firmadas por el usuario, con indicación del destinatario de cada una de ellas. Además, le entrega el identificador de usuario firmado. La tarjeta cifra todos estos datos con la clave pública del Registro para que solo éste pueda leerlos. La firma de los datos permite garantizar la integridad de la información transmitida mientras que el cifrado con la clave pública del destino garantiza la confidencialidad. Con los datos referidos en el paso anterior, el Punto de Participación genera una APDU (*Application Protocol Data Unit*) y la envía al Registro.

   $$Rg_P\,[U_{sig}\,(Identificador\_de\_Usuario),\,(U_{sig}\,(O_{Rg}\,(k_{dM})),\,Registro),\,(U_{sig}\,(O_{SIR1}\,(k_{dM})),\,Sistema\ de\ Intervención\ de\ Registro\ 1),\,...,\,(U_{sig}\,(O_{SIRq}\,(k_{dM})),\,Sistema\ de\ Intervención\ de\ Registro\ q)] \quad (1)$$

3. El Registro lee y descifra la APDU, obteniendo lo siguiente:

   $$U_{sig}\,(Identificador\_de\_Usuario),\,(U_{sig}\,(O_{Rg}\,(k_{dM})),\,Registro),\,(U_{sig}\,(O_{SIR1}\,(k_{dM})),\,Sistema\ de\ Intervención\ de\ Registro\ 1),\,...,\,(U_{sig}\,(O_{SIRq}\,(k_{dM})),\,Sistema\ de\ Intervención\ de\ Registro\ q) \quad (2)$$

   A continuación envía todos los datos a todos los Sistemas de Intervención de Registro. Cada uno de los Sistemas de Intervención, al igual que el Registro, deberá comprobar si el identificador de usuario recibido es correcto. Es decir, comprueba que el identificador está dentro de la lista de identificadores válidos, que la firma del usuario que realiza la solicitud es correcta y que no se ha recibido (y por tanto firmado ya) una clave opacada asociada a dicho identificador, es decir, que esa tarjeta no ha realizado previamente la petición. En caso contrario se rechaza lo recibido. Gracias a los Sistemas de Intervención de Registro el Registro no podrá actuar en nombre de los que no lo soliciten ya que desconoce su clave privada imprescindible para solicitar la autorización, tampoco podrá emitir más de una autorización de alias a cada usuario que lo solicite, ni emitir autorizaciones a falsos usuarios ya que los Sistemas de Intervención de Registro detectarían la duplicidad de autorización o su ausencia en el censo. El hecho de que el Registro compruebe en paralelo con los Sistemas de Intervención de Registro que la solicitud realizada es correcta permite que, en caso de producirse una incidencia, todos tengan constancia de ella. Como se puede apreciar, la función fundamental

de los Sistemas de Intervención de Registro es supervisar la actuación del Registro para evitar manipulaciones.

4. Una vez comprobado que el identificador de usuario recibido es válido, los Sistemas de Intervención de Registro se encargarán de firmar de forma ciega la clave k_{dM} opacada que les corresponda, y devolverán el resultado al Registro. Así, por ejemplo, el Sistema de Intervención *q* generará:

$$SIRq_{bsig}\ [O_{SIRq}\ (k_{dM})] \qquad (\mathbf{3})$$

   El Registro hace otro tanto con la clave k_{dM} opacada que le corresponde y la adjunta a las claves opacadas firmadas recibidas de los Sistemas de Intervención de Registro, formando así un *paquete de claves*.

5. Este paquete de claves es firmado por el Registro y cifrado con la clave pública del usuario, tras lo cual es enviado (mediante una APDU) al Punto de Participación. Los datos enviados corresponden a:

$$U_P\ [Rg_{sig}\ [Rg_{bsig}\ (O_{Rg}\ (k_{dM})), SIR1_{bsig}\ (O_{SIR1}\ (k_{dM})), ..., SIRq_{bsig}\ (O_{SIRq}\ (k_{dM}))]] \qquad (\mathbf{4})$$

   De esta forma tan solo la Tarjeta de Participación del usuario podrá leer el paquete de claves (confidencialidad de los datos) y además tiene la garantía de que fue el Registro quien le devolvió el conjunto de claves firmadas que, según se explica más adelante, le servirán como *autorización* para obtener un alias de forma anónima y para poder votar las conclusiones obtenidas al finalizar el debate.

6. El Punto de Participación entrega a la Tarjeta de Participación del usuario los datos contenidos en la APDU que ha recibido del Registro, de tal manera que ésta elimina el cifrado que lo protege y verifica la firma. Una vez leído el paquete de claves opacadas y firmadas a ciegas va eliminando, uno por uno, el factor de opacidad, obteniendo la k_{dM} firmada por el Registro, la k_{dM} firmada por el Sistema de Intervención de Registro 1, la k_{dM} firmada por el Sistema de Intervención de Registro 2 y así sucesivamente. A continuación verifica que las firmas del Registro y de los distintos Sistemas de Intervención de Registro son correctas. Si es así, el usuario dispone de los datos necesarios para iniciar la negociación con el Gestor de Alias y obtener un identificador (alias) sin perder la garantía de que solo los miembros autorizados del colectivo pueden participar en el debate, impidiendo además la utilización de un mismo alias por más de un miembro. El par de claves (k_{dM} y k_{cM}) será para al alias lo que clave pública y secreta es para el nombre del usuario. La clave que servirá para firmar el mensaje o cifrar el voto (k_{cM}) no sale jamás de la tarjeta que la ha generado. La otra parte de la pareja (k_{dM}) que sirve para verificar la firma del mensaje o descifrar el voto es, como hemos visto, previamente opacada dentro de la tarjeta para impedir posteriores relaciones entre las claves y los propietarios de dichas claves.

7. En el caso de que el usuario quiera obtener un alias para participar de forma anónima en los debates, desde el Punto de Participación se iniciará una interacción con el Gestor de Alias. Este último mantiene una lista pública de los alias ya utilizados para el foro, de manera que el usuario elegirá un alias no utilizado. Dentro de la tarjeta se firmará el alias elegido con la clave k_{cM} y el resultado se concatenará con la firma de la clave k_{dM} por parte del Registro y de los Sistemas de Intervención de Registro, dando lugar al siguiente conjunto de datos:

$$Alias_{sig}(alias),\ Rg_{sig}\ (k_{dM}),\ SIR1_{sig}\ (k_{dM}),\ ...,\ SIRq_{sig}\ (k_{dM}) \quad (\mathbf{5})$$

El Punto de Participación formará una APDU con los datos anteriores y la enviará al Gestor de Alias.

8. El Gestor de Alias, al recibir los datos, comprobará que tanto las firmas de la clave k_{dM} por parte del Registro y de los Sistemas de Intervención de Registro como la firma del alias con la clave k_{cM} sean correctas. Si todo es correcto comprueba a continuación que el alias elegido no se encuentre entre los que ya están siendo utilizados y si es así asocia el alias a la clave k_{dM} recibida y publica el alias en la lista de alias ya utilizados para el foro en cuestión. A continuación devolverá al Punto de Participación los datos recibidos firmados, es decir:

$$GA_{sig}[Alias_{sig}(alias),\ Rg_{sig}\ (k_{dM}),\ SIR1_{sig}\ (k_{dM}),\ ...,\ SIRq_{sig}\ (k_{dM})] \quad (\mathbf{6})$$

9. El Punto de Participación entregará lo recibido a la Tarjeta de Participación, donde se comprobará la firma del Gestor de Alias de manera que, si es correcta, se establecerá como alias el elegido por el usuario.

3.1.2. Debate

Como se ha comentado, la participación por parte de los usuarios en el debate puede ser anónima o identificada. En origen, concretamente en el Punto de Participación, se realiza esta distinción con la intención de que, como veremos a continuación, el Foro sea capaz de discernir qué clave utilizar en cada caso para manejar los datos recibidos del usuario. La forma en que tiene lugar la interacción entre el Punto de Participación y el Foro en cada uno de los casos es la siguiente:

3.1.2.1. Participación Identificada

En el caso de la participación identificada todos los mensajes emitidos por el usuario que se publiquen en el foro aparecerán asociados a su nombre real una vez que se verifique su firma.

Durante todo el proceso de debate puede darse el caso de que la discusión se desvíe del tema central. En esos casos entra en juego la figura del Moderador, que se encargará de dar toques de atención e intentar centrar la discusión en el tema concreto para el cual se ha establecido el debate. La participación del Moderador en todos los casos será identificada.

3.1.2.2. Participación Anónima

En el caso de la participación no identificada o anónima todos los mensajes emitidos por el usuario que se publiquen en el foro aparecerán asociados al alias elegido por el usuario para ese debate concreto, tras verificar (con la clave k_{dM}) la firma de dichos mensajes realizada con la clave k_{cM}.

3.1.2.3. Proceso de envío de mensajes al foro

A la hora de publicar un mensaje, tanto en la participación identificada como en la anónima, se dan los siguientes pasos:

1. En el Punto de Participación el usuario genera su mensaje indicando si se trata de una participación anónima o identificada. El mensaje se firma en la Tarjeta de Participación haciendo uso de la clave apropiada (la clave privada en el caso de participación identificada o la clave k_{cM} en el caso de participación anónima).
2. El mensaje firmado y la identidad del usuario (nombre real o alias) se concatenan para dar lugar a una APDU que se enviará al Foro.

$$U_{sig}\ (mensaje),\ Identidad\_de\_Usuario \quad (7)$$
$$\text{o}$$
$$Alias_{sig}\ (mensaje),\ Alias$$

3. El Foro, tras recibir la APDU anterior, verificará que el usuario está autorizado a participar en el debate en curso y, si es así, se le devuelve, a modo de comprobante de recepción, la firma del conjunto de datos recibidos concatenados con el identificador del foro.

$$Fo_{sig}[\ U_{sig}\ (mensaje),\ Identidad\_de\_Usuario,\ Identificador\_Foro] \quad (8)$$
$$\text{o}$$
$$Fo_{sig}[\ Alias_{sig}\ (mensaje),\ Alias,\ Identificador\_Foro]$$

   A continuación se comprueba la firma del mensaje recibido y que el mensaje es adecuado para su publicación. Esto último se traduce en un análisis sintáctico y semántico del mismo con la intención de detectar posibles palabras o expresiones que no estén de acuerdo a la política de buen uso del Foro. Si se detecta cualquier tipo de problema durante el análisis o en la verificación de la firma el mensaje no se publica y se le indica al usuario la razón del rechazo. El mensaje rechazado será almacenado en un sitio protegido accesible por parte de los auditores de manera que la información allí contenida, junto con el comprobante en la Tarjeta de Participación proporcionarán pruebas irrefutables del correcto funcionamiento del sistema. Si todas las comprobaciones son correctas el mensaje se publica en el foro junto con la identidad (real o alias) de su autor.
4. El Punto de Participación entrega el comprobante recibido a la Tarjeta de Participación del usuario que, tras verificar la corrección de la firma, lo almacena durante un determinado periodo de tiempo, previamente establecido, para que sirva como prueba de entrega en caso de una posible reclamación por mal funcionamiento del sistema.

3.1.3. Obtención de conclusiones y votación de resultados

Todos los foros tienen asociado lo que se podría denominar tiempo de vida, de manera que cuando ese tiempo de vida termina el foro se cierra, no permitiéndose la publicación de nuevos mensajes, pasándose a la fase de obtención de conclusiones. Básicamente en esta fase el Extractor de Conclusiones obtiene, mediante análisis semántico de los mensajes publicados por los usuarios en el foro, las distintas conclusiones o líneas de argumentación que se han seguido durante el debate. A la hora de analizar los mensajes para extraer las conclusiones o líneas de argumentación el Extractor de Conclusiones no tendrá en cuenta los enviados por el Moderador ni los de aquellos participantes que bajo la figura de Invitados hayan podido intervenir en el debate, de manera que las conclusiones obtenidas correspondan única y

exclusivamente a aquellas derivadas de la participación de usuarios del sistema propiamente dichos.

Como ya se ha comentado con anterioridad, con la intención de que las conclusiones extraídas sean validadas y se pueda determinar cuál es la más acertada se someten a un proceso de votación. En dicho proceso podrán participar todos los usuarios del sistema inscritos en el censo con las garantías de seguridad y anonimato propias de un sistema de votación telemática [11] [13].

3.1.3.1. Procedimiento de votación y obtención de resultados

A la hora de someter a votación los resultados extraídos de los procesos de debate se empleará un sistema de votación telemática. Los requisitos de seguridad exigidos a este tipo de sistemas para una determinada votación dependerá de los intereses a proteger, es decir, en aquellos casos en los que los usuarios consideren que la trascendencia del tema a votar lo merezca, se sugiere la aplicación de una arquitectura de votación telemática completa, que cumpla con todos los requisitos de seguridad exigibles a las votaciones telemáticas al más alto nivel [12]. Un ejemplo de sistema de voto telemático de este tipo sería el desarrollado por este grupo de investigación dentro del proyecto VOTESCRIPT [11] [13]. Sin embargo es razonable suponer que para aquellos temas donde sean menos los intereses puestos en juego, el interés por la realización de fraude disminuya, en cuyo caso puede ser recomendable una versión reducida de este sistema.

Una vez realizada la votación y obtenidos los resultados, son transferidos al Foro, que se encarga de hacerlos públicos.

4. RESULTADOS

La solución aquí presentada permite garantizar el buen funcionamiento de una plataforma de democracia digital bajo los aspectos recogidos en el apartado de Introducción, con independencia de la honestidad y competencia profesional de las personas a cargo del funcionamiento del sistema. Entre las principales aportaciones de esta propuesta cabe destacar que:

- La plataforma verifica que únicamente los usuarios autorizados pueden participar en el foro correspondiente, garantizando su identidad en caso de que la participación del usuario sea en modo identificado, es decir, cuando haga uso de su identidad real.
- Con objeto de garantizar la libertad de expresión de los participantes, aún bajo posibilidad de coacción, el sistema definido propone que los participantes puedan hacerlo bajo un alias, garantizando que ni el propio sistema pueda desvelar la identidad real de quien se oculta bajo ese alias, pero verificando que se trata de una persona autorizada a participar en ese foro de debate.
- La plataforma garantiza la integridad de la información publicada y almacenada, de manera que todos los mensajes depositados en el sistema son publicados sin modificaciones si cumplen la política de uso asociada y pactada para ese foro. Para evitar que las herramientas de filtrado automático asociadas al foro pudieran ser manipuladas, impidiendo la publicación de las opiniones de determinados usuarios,

la plataforma propuesta ofrece mecanismos de seguridad como el uso del comprobante de entrega y el almacenamiento de la información no publicada para su posterior examen si fuera necesario.

- Cada foro lleva asociado un tiempo de vida, transcurrido el cual se destruye la información sensible asociada al mismo, de manera que en un futuro no pudiera utilizarse esta información con fines torticeros.
- La plataforma proporciona un sistema fiable de votación que permite validar las conclusiones obtenidas como resultado del debate.
- La fortaleza del sistema se basa en la utilización de software de código abierto como medida para impedir la realización de tareas ocultas que pudieran perjudicar a los usuarios.

5. CONCLUSIONES

Los sistemas democráticos digitales implantados se encuentran aún en un período de maduración, tanto desde el punto de vista tecnológico como funcional y social. En esta fase inicial, es preciso acercar los sistemas de democracia digital a los ciudadanos, diseñando sistemas atractivos y fáciles de usar, a la vez que abordando temas que susciten interés entre los participantes. También, por parte de las Administraciones se hace necesario que desaparezcan los recelos que suscitan los sistemas de democracia digital (puesto que de hecho constituyen una forma más directa de control por parte de los ciudadanos sobre las decisiones que les afectan) y que se apoye decididamente su utilización en el proceso de toma de decisiones.

Una vez superada esta fase de *toma de contacto*, es preciso que los sistemas de participación ciudadana aumenten las prestaciones ofrecidas para poder ser empleados en entornos más críticos, en los que pueda existir manifiesto interés por parte de individuos, organizaciones o Administraciones en no recoger adecuadamente las opiniones vertidas por los participantes, en aras a alcanzar unas conclusiones determinadas. Para este tipo de situaciones se hace preciso que el sistema de participación ciudadana incorpore mecanismos que detecten cualquier situación anómala que pudiera producirse en el sistema, tal como la pérdida o alteración de los mensajes recibidos.

Asimismo, se ha constatado que existen numerosos escenarios de participación ciudadana en los que los usuarios consideran un requisito para participar en el sistema el poder hacerlo de forma anónima, mediante el empleo de un alias. En estos casos, el anonimato debe proporcionarse con las adecuadas garantías, de manera que la obtención y utilización de alias sólo se permita a los usuarios previamente autorizados y que en ningún momento exista la posibilidad de relacionar el alias con la persona que se oculta tras él.

Este artículo ha presentado una solución para hacer frente a estos problemas, proponiendo un sistema avanzado de participación ciudadana que incorpora los mecanismos de seguridad adecuados para garantizar el correcto funcionamiento del sistema en todas sus fases, a la vez que permite la participación anónima si el usuario lo desea. De esta forma, se espera obtener la confianza de los ciudadanos en el sistema y, por tanto, su plena participación en el proceso de toma de decisiones.

Por último, destacar que hace falta tiempo para que los usuarios, las Administraciones y la sociedad en general tomen conciencia de las posibilidades que ofrecen estos sistemas. Una vez conseguido, el avance y el éxito de la democracia electrónica pueden convertirse en una realidad.

REFERENCIAS

1. Una experiencia de democracia participativa. http://www.ciudadanos2005.net
2. Parlament Obert de Catalunya. http://www.uoc.edu/parlamentobert
3. http://www.andalucia2004.net
4. http://www.candidato2004.net
5. http://www.galicia.candidatos2005.net
6. DEMOS (Delphi Mediation Online System). IST-1999-20530. http://www.demos-project.org/
7. Dialogic and Argumentative Negotiation Educational Software (DUNES) IST -2001-34153. http://www.tessera.gr/dunes/index.php
8. Web Technologies Supporting Direct Participation in Democratic Proceses (WEBOCRACY) IST-1999-20364. http://esprit.ekf.tuke.sk/webocracy/index.html
9. European Cities Platform for On-line Transaction Services (EURO-CITI). IST-1999-21088. http://www.euro-citi.org/
10. TED (Towards Electronic Democracy). http://infodoc.escet.urjc.es/ted
11. Sistema VOTESCRIPT: Una propuesta innovadora desarrollada para resolver los problemas clásicos de votación electrónica. J. Carracedo Gallardo, A. Gómez Oliva y J.D. Carracedo Verde. 2º Congreso Iberoamericano de Seguridad Informática (CIBSI'03). México D.F., 27-31 de octubre de 2003. ISBN 970-36-01049 págs. 376-392.
12. Votación electrónica basada en criptografía avanzada (Proyecto VOTESCRIPT). J.Carracedo Gallardo, A. Gómez Oliva, J. Moreno Blázquez, Emilia Pérez Belleboni. J.D. Carracedo Verde. 2º Congreso Iberoamericano de Telemática (CITA 2002), Mérida, (Venezuela), septiembre 2002.
13. VOTESCRIPT: telematic voting system designed to enable final count verification. A. Gómez Olive, E. Pérez Belleboni, S. Sánchez García, J. Carracedo Gallardo, J. Moreno Blázquez, J. D. Carracedo Verde. CollECTeR LatAm 2005, 3-5 de Octubre de 2005. Talca, Chile.
14. Carracedo Gallardo, J. Seguridad en redes telemáticas, Ed. McGraw-Hill, 2004. ISBN 8448141571.
15. Architectural design for a Digital Democracy telematic platform. A. Gómez Oliva, C. González Martínez, S. Sánchez García, E. Pérez Belleboni, J. Moreno Blázquez. CollECTeR LatAm 2005, 3-5 de Octubre de 2005. Talca, Chile.