Un sistema de discusión seguro con participación anónima a través de servicios Web

A secure discussion system with anonymous participation through Web services

Daniel Vásquez[1] Narciso Cerpa[1] Renzo Angles[1]

Recibido 25 de mayo de 2011, aceptado 9 de noviembre de 2012
Received: May 25, 2011 Accepted: November 9, 2012

RESUMEN

Un desafío para la deliberación democrática en un entorno informático es proveer seguridad en el proceso, tanto para el ciudadano individual como para el grupo social. En este sentido, es importante ofrecer garantías de protección a los ciudadanos de forma que no se vea afectada su libertad de expresión y de seguridad en el intercambio de mensajes, de manera que estos sean confiables para todos los participantes. Como parte de este proyecto se ha diseñado y construido un sistema informático de discusión que permite a los usuarios intercambiar opiniones de forma segura, a través de la aplicación de técnicas de criptografía. El sistema permite varios niveles de seguridad e identificación. Se permite la participación identificada a través del uso de firma digital y certificados. Además, se implementa un esquema de participación anónima a través de la firma de mensajes utilizando una credencial obtenida mediante un procedimiento de firma ciega. También se aplican atributos de seguridad para asegurar la integridad, confidencialidad y no repudio de estos. El sistema de discusión se ha construido inmerso en una plataforma de servicios Web orientada a proveer funcionalidades de apoyo a la democracia digital.

Palabras clave: Democracia deliberativa, criptografía, firma digital, firma ciega, anonimato, libertad de expresión.

ABSTRACT

A challenge for democratic deliberation in a computing environment is to provide security in the process, both for the individual citizen and the social group. In this regard, it is important to provide guarantees of protection to the citizens so as not to affect their freedom of expression and security on the exchange of messages, so they are reliable for all participants.
As part of this project a discussion system has been designed and built that allows users to exchange opinions safely, through the application of cryptographic techniques. The system allows multiple levels of security and identification. It allows the participation identified through the use of digital signatures and certificates. Furthermore, it implements a scheme of anonymous participation by signing messages using credentials obtained from a blind signature process. Also security attributes are applied to ensure the integrity, confidentiality and non-repudiation of these. The discussion system was built embedded in a Web services platform designed to provide functionality to support digital democracy.

Keywords: Deliberative democracy, cryptography, digital signature, blind signature, anonymity, freedom of speech.

[1] Facultad de Ingeniería. Universidad de Talca. Merced 437. Curicó, Chile. E-mail: dvasquez@alumnos.utalca.cl; ncerpa@utalca.cl; rangles@utalca.cl

INTRODUCCIÓN

Un aspecto esencial de la democracia es la necesidad de que sus participantes arriben a acuerdos que generen un beneficio común o permitan, al menos, abordar los problemas minimizando los sectores perjudicados. Esta dimensión de la democracia se denomina deliberativa [5].

Por diversas razones, por ejemplo coerción, es deseable que los usuarios puedan proteger su identidad en una discusión deliberativa. Al mismo tiempo, para que todos los participantes puedan confiar en el proceso es necesario proveer características de seguridad que impidan que usuarios maliciosos o no autorizados puedan alterar, intervenir u observar el proceso [11].

El objetivo del presente proyecto es "desarrollar un sistema de discusión deliberativa para la democracia digital a través de servicios Web". Este sistema implementará un modelo de seguridad que contribuya a mejorar la confianza de los usuarios en las conversaciones que se generan, ya sea cuando los usuarios participen en un modo identificado o anónimo. Se aplicarán distintas técnicas de criptografía para proveer un entorno seguro y se utilizará un procedimiento de firma ciega para la obtención de credenciales anónimas.

En la siguiente sección presentamos una revisión de los conceptos de esfera pública, democracia y su visión deliberativa, así como algunos argumentos acerca de la conveniencia del anonimato bajo determinadas circunstancias. En seguida presentamos el trabajo relacionado y un resumen de características que debiera tener un proceso deliberativo en un entorno informático. Luego describimos el modelo del sistema propuesto incluyendo las características de seguridad aplicadas. El punto siguiente presenta la arquitectura y un diseño para la implementación del modelo propuesto. Finalmente presentamos las pruebas funcionales y discutimos las fortalezas y debilidades, así como las posibles aplicaciones del modelo desarrollado.

ESFERA PÚBLICA, DEMOCRACIA Y DELIBERACIÓN

El ser humano para sobrevivir y desarrollarse ha necesitado la cooperación y alianza con otros seres humanos. De organizaciones sociales primitivas como los clanes o las tribus ha evolucionado a la formación del Estado. El Estado se entiende como una agrupación humana con una organización social y económica que posee un territorio y algún tipo de gobierno.

En 1962 Jürgen Habermas [15] reflexiona sobre el concepto de la esfera pública y su evolución. En la obra postula que la práctica de la democracia como un proceso de deliberación es una característica fundamental para alcanzar la legitimidad del sistema de gobierno. Las instituciones del Estado y los grupos de interés organizados se consolidan y se imponen en el proceso político.

En la visión de Habermas, este proceso crea una suerte de nueva feudalización donde la prensa cumple el papel de dotar a la autoridad pública de un "aura exclusiva" al estilo de las autoridades medievales. De este modo, el espacio público se transforma en un espectáculo en el cual los líderes políticos requieren la legitimación a través del voto periódico de una masa de ciudadanos despolitizados. Así los ciudadanos son excluidos de la toma de decisiones y toman un papel de meros ratificadores.

Más recientemente, Habermas indica que las formas de conversación que pueden darse en los medios masivos (*talk shows*, programas de debate) no son comparables al debate crítico racional que constituía, por ejemplo, la esfera pública burguesa del XVIII, sino que "la conversación misma está administrada" y estos no forman un espacio deliberativo [15].

Es en la esfera pública donde los ciudadanos dialogan para tomar decisiones que afectan el devenir del grupo. En escala pequeña, es posible mantener un sistema asambleario en el sentido de que todos o casi todos los que son considerados ciudadanos tienen posibilidad de expresar su opinión. En ese sentido es una democracia directa. Sin embargo, con el crecimiento de las sociedades y la complejidad creciente de los problemas, los sistemas democráticos han devenido en democracias representativas, donde los ciudadanos delegan en representantes el ejercicio de las decisiones democráticas [9].

El modo en que los ciudadanos llegan a una decisión también es un factor importante para definir el tipo de democracia que se ejerce. En un modelo

agregativo los ciudadanos ejercen su voluntad a través del ejercicio del voto. Esto constituye un acto eminentemente privado. En general, el voto se ejerce para elegir a los representantes que tendrán luego la misión de deliberar acerca de los asuntos públicos.

En un modelo de democracia deliberativa el acto político decisivo es "acoplar, en el debate público, la emergencia del consenso" [15, 28]. Por lo tanto se entiende a la deliberación democrática como un proceso dialógico, procedimental y transformativo, llevado a cabo a través de un discurso racional [2]. Donde el modelo agregativo asume como principal un acto privado –la votación–, el modelo deliberativo asume su acto fundamental como un proceso público de entrega, valoración y aceptación o rechazo de razones [9].

La libertad, racionalidad, igualdad y consenso son criterios postulados por Cohen [5] que permitirían juzgar la legitimidad de la deliberación. Por otra parte, Dahl [8] se refiere a criterios para juzgar la legitimidad del proceso deliberativo *per se*; entre ellos la participación efectiva, el voto igualitario, y la ganancia de entendimiento (sobre las materias producto de la interacción).

La democracia deliberativa fundamenta entonces su importancia en los siguientes aspectos [17]: la contribución de diferentes actores mejora la calidad técnica de las decisiones; la mejora de la legitimidad de las decisiones a través de la participación; la promoción del aprendizaje individual y colectivo; la convicción ética de que los ciudadanos tienen el derecho de influenciar directamente las decisiones que les afectan; y la limitación de la influencia de grupos de poder.

Anonimato y libertad de expresión

Habermas [14] plantea que en una discusión o deliberación democrática sólo es pertinente la lógica del discurso en una situación comunicativa en que "el único motivo admisible es la búsqueda de la verdad en cooperación" y en que "la fuerza del argumento es la única compulsión admisible". En esta situación el conocimiento de las características personales de los participantes actúa como elemento perturbador y a veces es un obstáculo para la correcta argumentación. Con el anonimato se evitarían errores o distorsiones en la argumentación como los que se encuentran en algunas falacias, especialmente en las ad hominem. El conocimiento de la identidad del participante, además, condiciona poderosamente la valoración del texto. De este modo, la firma de una persona que tiene un cierto renombre, dentro o fuera del ámbito temático de discusión, puede hacer que los lectores asimilen algún error, mentira o argumento falaz, en este caso de autoridad. Por el contrario, si la firma corresponde a alguien del cual sabemos que ha fracasado en alguna empresa, aunque nada tenga que ver con la cuestión debatida, puede llevar al lector a despreciar la información que proporciona o a no tener en cuenta su opinión a pesar de que esté avalada por una argumentación bien construida.

Otro factor que fundamenta la necesidad de anonimato es el peligro del abuso autoritario [1]. El uso de la capacidad de registro y vigilancia de los sistemas tecnológicos podría atentar contra la seguridad física o cívica de los ciudadanos [25]. En este sentido, es relevante proteger a los participantes de posibles apremios ilegítimos para manipular su participación en un proceso de deliberación.

El problema evidente ante el requerimiento de anonimato de los participantes es el peligro de que la conversación sea desvirtuada por el envío de mensajes en forma irracional, ya sea por su repetición, impertinencia o por usuarios que no pertenecen a un espacio público en particular, por ejemplo, en una discusión de carácter municipal, lo normal es que los participantes sean los habitantes del municipio. Si habitantes de otro municipio participan en una deliberación anónimamente por razones de rivalidad, este comportamiento desvirtuaría la situación de "búsqueda del bien común". Ante ello, surgen mecanismos de moderación, mediación y control de las discusiones [12], lo cual no necesariamente implica una amenaza a la libertad de expresión, sino que puede servir para lograr "una conversación estructurada al servicio de una deliberación inteligente para la toma de decisiones" [24]. Al mismo tiempo, se debería tender a buscar mecanismos que permitan validar a los participantes, a la vez que se protege su identidad, de forma similar a la que se aplica en procesos de votación [25].

Deliberación en la democracia electrónica

El concepto de "democracia electrónica" surge de la aplicación de las Tecnologías de la Información y Comunicación (TIC) a la democracia. Las ventajas potenciales del uso de las TIC son cubrir un espectro

más amplio de la población (al menos desde un punto de vista geográfico), atraer ciertos sectores que usualmente no participan (ejemplo, campesinos, jóvenes), proveer información en todo momento en distintos formatos accesibles para distintas audiencias, facilitar el acceso a información especializada sobre los tópicos, proveer acceso a reportes y resultados de los procesos, así como información actualizada y automatizada, disminución del tiempo en interacción entre gobierno y ciudadanía, trazar el proceso completo que permita ver la progresión y justificación de los resultados y lograr transparencia a través del acceso libre a la información y políticas [13, 32]. Un efecto de esto es una redefinición del espacio-tiempo, en cuanto a que la secuencia "pasado, presente, futuro" se vuelve aleatoria por una parte (análogamente con el hipertexto) y por otra parte se comprime o descomprime en cuanto a la capacidad de inmediatez, a la vez que el alcance se hace global o por lo menos trascendente del espacio jurisdiccional [31].

El reto de la democracia deliberativa en una sociedad informatizada reside en la formación creciente de redes que se articulan más allá del ámbito de decisión de las administraciones, quitando la exclusividad o el protagonismo a las instituciones políticas como espacio público de deliberación [4].

Ante el escenario producido por el alejamiento de los ciudadanos de la esfera de decisiones y tomando las oportunidades que presenta el modelo de democracia deliberativa y las nuevas capacidades tecnológicas, los ciudadanos demandan mayor involucramiento en la esfera pública y al mismo tiempo los gobiernos comienzan a asumir la necesidad de este involucramiento como medio de legitimación ante sus ciudadanos. En forma ideal, la participación ciudadana busca lograr mayor transparencia, confianza y acoplamiento entre las autoridades y los ciudadanos [13], el descubrimiento de asuntos de importancia para la población [13], el descubrimiento de soluciones innovadoras [13], mayor satisfacción o aceptación de las políticas adoptadas, fortalecimiento de las organizaciones sociales, mediación entre visiones divergentes, delegación de poder y mayor control ciudadano [16].

TRABAJO RELACIONADO

Las experiencias relacionadas con democracia deliberativa han sido variadas. Entre ellas podemos identificar las experiencias basadas exclusivamente en el voto electrónico, así como también aquellas orientadas a brindar soporte a la deliberación.

Con respecto a las experiencias sobre el voto electrónico, se pueden encontrar éxitos dispares sobre su aplicación en lugares como Estados Unidos, Venezuela, Brasil o India. Las experiencias relacionadas con consultas ciudadanas son también múltiples. Un ejemplo es Madrid Participa [32] que consistió en consultas ciudadanas sobre asuntos municipales en determinados barrios de Madrid (España).

Con respecto al uso de plataformas de soporte a la deliberación, podemos mencionar varias experiencias. Una de las más relevantes es el proyecto DEMOS [20], el cual fue probado en Hamburgo y Bolonia durante el año 2002, basándose en la técnica Delphi.

En la ciudad alemana de Esslingen se realizó una experiencia de democracia deliberativa usando el software Zeno y la plataforma Dito [27] cuya característica distintiva es la representación gráfica de la argumentación en procesos deliberativos [12]. Las mismas herramientas se usaron en la elección de un parlamento juvenil el año 2001, basándose en el uso de certificados digitales y tarjetas criptográficas para votación electrónica [22].

En el año 2001, el proyecto EDEN se caracterizó por el uso de herramientas basadas en el procesamiento del lenguaje natural para facilitar la participación ciudadana municipal, realizándose pilotos en Holanda, Polonia, Austria, Italia y Alemania [33]. Otra iniciativa relevante es el proyecto DUNES [6], el cual puso énfasis en la colaboración como medio de deliberación, y en la construcción de mapas de argumentación.

El proyecto EURO-CITI [30] ha desarrollado una arquitectura de servicios destinada al sector público, incluyendo: votación, entrega electrónica de formularios y consulta ciudadana. Otro proyecto orientado a la toma de decisiones es el proyecto TED [3], el cual utiliza técnicas bayesianas para ayudar a resolver conflictos con multiplicidad de variables y divergencia de intereses.

El proyecto WEBOCRACY [7] tiene por objetivo dotar a los ciudadanos de un sistema de votación,

acceso y comunicación orientado a la participación en procesos de decisión. El proyecto E-Engagement [13] fue llevado a cabo en el estado de Western Australia como una iniciativa integral de gobierno electrónico con énfasis en los desafíos administrativos y tecnológicos.

Podemos resaltar que los proyectos orientados a la discusión deliberativa no presentan una preocupación técnica dirigida a fortalecer las condiciones de participación segura, esto en comparación con los proyectos orientados al voto electrónico. A su vez, los procesos de votación electrónica podrían ser mejorados si cuentan con sistemas de deliberación previos, con un nivel alto de confianza desde el punto de vista técnico, que legitimen el proceso de definición de los asuntos que llegan a ser sujetos de votación. Para ello es necesario implementar atributos de seguridad avanzados a través de la aplicación de técnicas criptográficas.

REQUISITOS DE UN SISTEMA DE DISCUSIÓN

De acuerdo a los principios planteados por la teoría y la experiencia, se pueden extraer atributos para un sistema de software de apoyo a la deliberación democrática.

Considerando las características propias del entorno electrónico [13], el sistema de discusión debería cumplir los propiedades de accesibilidad, simplicidad, claridad, privacidad, auditabilidad y seguridad. La accesibilidad apunta a cubrir el principio de inclusión e igualdad para las personas cuyas capacidades físicas, intelectuales, de conocimiento o económicas están disminuidas. Esto implica características de usabilidad y simplicidad, con el fin de disminuir la brecha de aprendizaje. Igualmente la claridad y la simplicidad apuntan a la efectividad del proceso [32].

Las políticas de privacidad son necesarias para asegurar a los ciudadanos que no serán perseguidos por sus opiniones y que nadie puede acceder a los datos confidenciales. La auditabilidad implica mecanismos que aseguran que el sistema hace lo que dice que hace y no otra cosa que pueda manipular el proceso público [16].

Un aspecto fundamental en el desarrollo de un sistema de discusión consiste en implementar atributos de seguridad avanzados. En este sentido se deberá poner especial atención a aspectos de seguridad tales como: incluir distintos niveles de identificación y anonimato; uso de firma digital para asegurar el no repudio de mensajes, tanto de origen como en el destino de éstos; aplicación de técnicas criptográficas para asegurar la integridad y confidencialidad de los mensajes; uso de dispositivos seguros para el almacenamiento de claves criptográficas; y entregar soporte para certificados de clave pública.

Complementando las características descritas anteriormente, podemos identificar algunos requerimientos relacionados al proceso de la deliberación democrática, entre ellos [17]: establecer reglas a priori y en forma clara; emplear métodos que aseguren a los participantes que no existe manipulación; estructurar el proceso en forma clara y en fases progresivas; asegurar que el método de decisión final sea validable por los participantes; y acotar los objetivos y duración de los procesos.

Desde el punto de vista de la relación social entre los actores involucrados, el sistema deberá: considerar la necesidad de hacer frente al problema de la brecha digital y de la inclusión de grupos minoritarios; incluir políticas administrativas orientadas al correcto involucramiento de los participantes; crear y mantener el respeto mutuo entre los participantes; crear y mantener la percepción de eficacia del sistema; las autoridades deben comprometerse fuertemente con el proceso y sus resultados; garantizar los aspectos relativos a la seguridad, auditabilidad y libre expresión como medio de aseguramiento de la confianza.

Basándonos en estos requisitos, presentaremos el diseño y desarrollo de un *servicio Web de discusión*. Este consiste en un servicio que permite crear discusiones, acotadas en el tiempo, que cuentan con diferentes clases de participación. Estas clases de participación son relativas a distintos niveles de aseguramiento de la identidad o el anonimato de un usuario. Fundamentalmente, se intenta asegurar que para ciertas discusiones solo participen quienes estén autorizados para ello de un modo fuertemente identificado, mientras que cuando eventualmente sea deseable una participación anónima, los participantes puedan hacerlo sin peligro de ser descubiertos en su identidad y sin perjuicio de que la primera condición se cumpla, es decir, que estén autorizados.

Una idea fundamental en el sistema es implementar atributos de seguridad avanzados a través del uso de una infraestructura de clave pública de modo que los usuarios puedan firmar digitalmente mensajes y de esta manera mejorar la confianza en el sistema. Asimismo, el uso de esquemas de firma ciega es utilizado para que los usuarios puedan participar en servicios de manera anónima si así es requerido. Para este fin, los usuarios son dotados de dispositivos criptográficos (de software o hardware) en el cual almacenarán de forma privada sus claves.

Además se consideran funciones de seguridad como el no repudio de mensajes, confidencialidad en tránsito e integridad que sirven para proteger debidamente que los contenidos que se intercambian en la plataforma son confiables para todos los actores del sistema.

MODELO PROPUESTO

De acuerdo a las características generales presentadas en la sección anterior, proponemos un modelo de deliberación basado en discusiones con diferentes tipos de participación y niveles de seguridad. Para proveer las características que permitan obtener un proceso en que se mejora la confianza y la libertad de expresión de los participantes, utilizamos en los comentarios los tipos de participación y niveles de seguridad propuestos en [25], pero con variaciones en cuanto al modo en que se aplican.

Una discusión se caracteriza por la proposición de un tema y el intercambio de opiniones entre los participantes para arribar a una o varias conclusiones o soluciones. Una discusión puede ofrecer los siguientes atributos de seguridad para los mensajes:

- No repudio: Las discusiones que ofrecen no repudio devuelven la firma de la discusión sobre los mensajes enviados a modo de comprobante para el usuario.
- Integridad y confidencialidad: Los mensajes viajan cifrados y se prueba su integridad al ser recibidos.
- Prueba de origen: Se comprueba que los comentarios firmados provienen de una fuente que cuenta con un certificado de confianza desde el punto de vista del sistema.

Para la interacción con el modelo propuesto, existirán distintos tipos de claves, usuarios, discusiones y mensajes según el tipo de participación que una discusión requiera, los cuales serán descritos a continuación.

Un proceso de deliberación puede ser iniciado por cualquier usuario (identificado o anónimo), el cual será responsable de configurar las opciones disponibles. Un usuario registrado en el sistema poseerá una tarjeta electrónica a través de la cual podrá generar dos pares de claves que le permitirán participar del sistema de discusión

El primer par de claves será un Par de Claves Identificado (PCI), y constará de una Clave Pública Identificada (CPI) y una Clave Privada Identificada (CSI) que serán utilizadas para firmar mensajes de forma identificada en las discusiones. El segundo par de claves será un Par de Claves Anónimo (PCA), y constará de una Clave Pública Anónima (CPA) y una Clave Privada Anónima (CSA), que serán utilizadas para firmar mensajes de modo fuertemente anónimo cuando una discusión lo requiera.

Al generar el PCI el usuario debe generar un certificado autofirmado que contenga la parte pública del par y guardarlo junto a la clave privada. Para que el certificado sea útil ante la plataforma, debe estar firmado por una Autoridad Certificadora (CA) (el modo en que el usuario obtiene la certificación queda fuera del alcance de este artículo). El PCA, por su parte, no requiere un certificado dado que por el carácter anónimo no tiene sentido acreditar su identidad. Por lo tanto, los usuarios que quieran actuar anónimamente registrarán la parte pública ante la plataforma a través de un proceso de obtención de credenciales. En la posesión de la credencial obtenida residirá la garantía de identidad para el usuario. En cualquier caso, las claves son almacenadas en la tarjeta criptográfica y sus partes públicas serán almacenadas en el registro de la plataforma.

Los posibles tipos de usuario, según su identificación en discusiones, serán:

- *Usuario Libre*: No se identifica de forma alguna.
- *Usuario Débilmente Identificado (UDI)*: Cualquier usuario que esté registrado en el sistema. Se identifica a través de un par alias-contraseña.
- *Usuario Débilmente Anónimo (UDA)*: Existirá en el contexto de una discusión anónima y deberá ser registrado previamente.

- *Usuario Fuertemente Identificado (UFI)*: Un usuario del sistema que ha registrado un certificado, y operará con un PCI (generado en su tarjeta criptográfica).
- *Usuario Fuertemente Anónimo (UFA)*: Existirá en el contexto de una discusión fuertemente anónima y debe ser registrado previamente. En el registro solo constará su alias y un CPA (generado en su tarjeta criptográfica).

En base a las formas de participación se tendrán cinco *tipos de discusión*:

- *Discusión Libre*: Cualquier participante del sistema podrá enviar comentarios y leer los contenidos, sin identificarse.
- *Discusión Débilmente Identificada (DDI)*: Permite participar a cualquier usuario registrado, sin embargo los mensajes no irán firmados digitalmente.
- *Discusión Débilmente Anónima (DDA)*: Permitirá al usuario resguardar su identidad ante el resto de los usuarios, pero sin garantía de resguardarla ante los administradores del foro. Los usuarios también podrán participar de forma identificada.
- *Discusión Fuertemente Identificada (DFI)*: Los mensajes serán identificados con el alias y estarán firmados por la CSI de un UFI.
- *Discusión Fuertemente Anónima (DFA)*: Permitirá a los usuarios ocultar su identidad ante los administradores y el resto de los usuarios. Los primeros podrán comprobar a través de una forma anónima que el usuario está facultado para participar. El usuario deberá registrar previamente un UFA, sus mensajes serán identificados con un alias anónimo que haya registrado y estarán firmados con su CSA.

Adicionalmente, se tendrán los siguientes *tipos de comentarios*:

- *Comentario Libre*: No va identificado ni firmado.
- *Comentario Débilmente Identificado*: Identificado a través del alias de un UDI.
- *Comentario Débilmente Anónimo*: Identificado a través del alias de un UDA.
- *Comentario Fuertemente Identificado*: Identificado a través del alias de un UFI y firmado con la CSI del mismo.
- *Comentario Fuertemente Anónimo*: Identificado a través del alias de un UFA y firmado con la CSA del mismo.

De acuerdo con el tipo de participación que se requiera existirán dos tipos de registro adicionales al registro general en el sistema: registro de un usuario débilmente anónimo y registro de un usuario fuertemente anónimo.

Para registrar un usuario débilmente anónimo, un usuario que haya iniciado una sesión deberá enviar un alias anónimo y una contraseña a la DDA en que quiera participar. La plataforma comprobará que la sesión es válida y registrará el usuario anónimo para la discusión en particular.

Para registrar un usuario fuertemente anónimo, es necesario que previamente un usuario fuertemente identificado obtenga una credencial para cada DFA en la que quiera participar. El proceso es el siguiente:

- El usuario enviará $O(A_p)$, donde $O(A_p)$ es una clave pública anónima y opacada y $I_s(O(A_p))$, que es la firma con la clave privada identificada del usuario I_s sobre ella.
- El registro de la discusión comprobará con la clave pública identificada del usuario I_p que la firma $I_s(O(A_p))$ es correcta.
- El servidor retornará $D_s(O(A_p))$ al usuario que representa la firma ciega con la clave privada de la discusión D_s sobre $O(A_p)$.
- El usuario desopacará la firma y obtendrá $D_p(A_p)$ que será la credencial que permitirá a un usuario inscribirse en una DFA.
- Para inscribirse en una DFA el usuario enviará al registro de ésta, la credencial obtenida más un alias y la CPA en claro. El registro de la DFA comprobará que la credencial ha sido firmada con su propia clave privada y registrará un nuevo usuario fuertemente anónimo.

ARQUITECTURA Y DISEÑO

La arquitectura del sistema de discusión propuesto (ver Figura 1) se basa en servicios Web y el uso de tarjetas criptográficas que almacenen claves que permitan firmar los mensajes a través de un cliente de escritorio que actuará como interfaz de usuario. El sistema presenta una arquitectura cliente-servidor donde la comunicación entre ellos se realiza a través

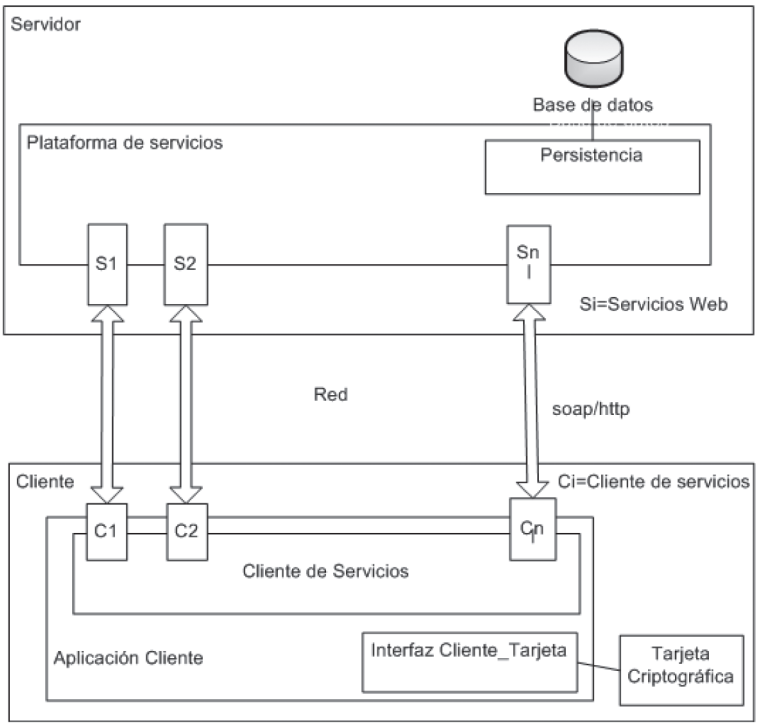

Figura 1. Arquitectura general del sistema de discusión propuesto.

de llamadas a servicios Web usando SOAP sobre HTTP. Del lado del servidor existe una plataforma donde reside el modelo (plataforma de servicios), la capa de datos y la interfaz de servicios Web. El cliente es una aplicación de escritorio que contiene la interfaz de usuario y un componente que actúa como interfaz para invocar los servicios Web. Además existe un componente que permite gestionar las claves criptográficas del usuario a nivel local.

Módulo Servidor

El servidor, compuesto principalmente por la plataforma de servicios, provee la infraestructura necesaria para mantener los repositorios del sistema, ejecutar las interacciones a nivel de dominio y exponer la interfaz de servicios Web que interactúa con la aplicación cliente.

Los repositorios serán implementados típicamente a través de una base de datos relacional. La plataforma se comunica con ésta a través de una interfaz que proyecta el modelo relacional de la base de datos a un modelo basado en objetos que representa el dominio del sistema. Esta proyección objeto-relacional (en inglés, *Object Relational Mapping*) normalmente requiere de un componente o motor de persistencia.

La plataforma de servicios se compone principalmente de un registro de usuarios mantenidos en un censo y un registro de aplicaciones que agrupan servicios específicos ofrecidos a subconjuntos de usuarios que se inscriben en ellas.

En el servidor podemos encontrar servicios intrínsecos y específicos. Los *servicios intrínsecos* se refieren a funcionalidades que sirven de apoyo a la plataforma en sí misma. Entre estos podemos mencionar:

- *Servicio de Identificación*: Se encarga de proporcionar autenticación en forma transversal en la plataforma.
- *Servicio de Censo*: Gestiona el censo de usuarios. Debe proporcionar funciones para añadir, editar, borrar y obtener listas de usuarios.
- *Servicio de Membresía*: Gestiona las relaciones entre usuarios y aplicaciones. Debe proporcionar funciones para añadir, editar, borrar membresías,

además de gestionar solicitudes de membresías que deben esperar aprobación de un usuario con facultades para ello. También debe tener funciones para controlar los roles de los usuarios sobre las aplicaciones.
- *Servicio de Aplicaciones*: Gestiona las aplicaciones. Debe proporcionar funciones para añadir, editar, borrar y obtener listas de aplicaciones.

Los *servicios específicos* son aquellos que entregan funcionalidades orientadas específicamente a la democracia digital, por ejemplo: servicios de encuestas, bitácoras, noticias, documentación, voto, discusión, etc. Uno de ellos, el de discusión, se describe más adelante.

Si bien la interacción de los usuarios con la plataforma se realiza íntegramente a través del cliente, podemos distinguir los siguientes actores funcionales en el sistema:

- *Usuario*: Actor que posee acceso al cliente de la plataforma.
- *Ciudadano*: Es un usuario que ha iniciado una sesión en el sistema como un usuario normal, es decir, no es un administrador de la plataforma. Esto implica que pertenece al censo de usuarios.
- *Administrador de plataforma*: Usuario que tiene poderes sobre la administración de la plataforma. Se encarga fundamentalmente de mantener el censo de usuarios y el registro de aplicaciones. Será nombrado simplemente como Administrador.
- *Administrador de aplicación*: Es un usuario que tiene poderes sobre la gestión de una aplicación en particular. En general está encargado de mantener el registro de los usuarios que pertenecen a la aplicación en particular y puede editar datos generales de ésta. No es una entidad en sí misma, sino que representa un rol de un ciudadano o un administrador de plataforma.
- *Ciudadano anónimo débil*: Es un usuario que participa de forma anónima en alguna parte del sistema, pero que posee credenciales para hacerlo de un modo débil, esto es, cuenta con un password y un alias anónimo, pero tiene pocas garantías de que su identidad está protegida ante el resto de actores.
- *Ciudadano anónimo fuerte*: Es un usuario que participa de forma anónima en alguna parte del sistema, pero que posee credenciales para hacerlo de un modo fuerte, esto es, un alias anónimo y una clave pública obtenida a través de un proceso de firma ciega, por lo que tiene garantías fuertes de que su identidad está protegida ante el resto de actores.

Módulo Cliente

El módulo Cliente es el componente con el cual interactúan en forma directa los usuarios. Consiste de una aplicación para escritorio, con capacidad para comunicarse con el servidor de aplicaciones a través de una interfaz de diversos servicios Web. La interacción Cliente-Servicios Web requiere de un Cliente de Servicios, el cual se encargará de encapsular las llamadas a los servicios Web a través de la red, usando el protocolo SOAP (*Simple Object Access Protocol*) sobre HTTP (*HyperText Transfer Protocol*).

El Cliente es un componente de escritorio debido a la necesidad de acceder directamente a un dispositivo criptográfico (tarjeta criptográfica), la cual se comunica con la aplicación cliente y reside en algún fichero dentro del sistema del usuario. El Cliente y la Tarjeta Criptográfica, a su vez, también requieren de una interfaz de comunicación y de gestión de las claves y operaciones.

Dentro del Cliente se pueden distinguir las siguientes interfaces y componentes:

- *Modelo*: La capa de negocio de la aplicación. Encargado de la coordinación del resto de los componentes.
- *Interfaz con la plataforma*: La comunicación entre el componente y la plataforma se produce a través de una red (normalmente Internet aunque podría ser una red local).
- *Interfaz con la Tarjeta Criptográfica*: Conjunto de componentes de software que permiten interactuar y gestionar un almacén de claves.
- *Interfaz de usuario*: Las ventanas y diálogos con los que interactúa directamente el usuario.
- *Configuración*: Módulos encargados de mantener información general que debe persistir a través de archivos de configuración. Esta información puede ser relativa a idiomas, algoritmos utilizados, ubicación de los servicios, etc.

La Figura 2 presenta una vista general simplificada del componente Cliente. La clase *Model* es la clase

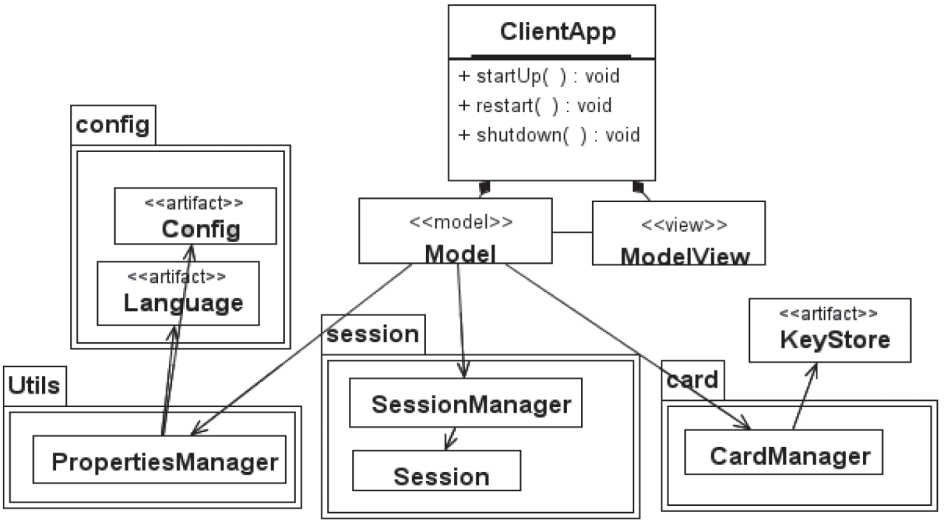

Figura 2. Diseño general de la aplicación Cliente.

principal del sistema ya que mantiene el estado general de la aplicación en todo momento. Por una parte, mantiene el estado de la configuración que es gestionada por un objeto *PropertiesManager* que se comunica con un archivo *Config* que mantiene los datos persistentes. Otro objeto de *PropertiesManager* se encarga de gestionar un archivo que permite seleccionar distintos idiomas para la interfaz de usuario, según disponibilidad y preferencia. A través de *SessionManager* mantiene la información de la sesión concurrente. *CardManager*, en tanto, provee una interfaz entre el almacén de claves y la aplicación.

La clase *ModelView* representa la interfaz de usuario central de la aplicación, mientras que la clase *ClientApp* es la que permite iniciar, reiniciar o parar la aplicación, y es la que inicializa una instancia de *Model* y *ModelView*. Entre las tres configuran una arquitectura clásica Modelo-Vista-Controlador (MVC).

Servicio de Discusión

El Servicio de Discusión, implementado en el sistema propuesto, se describirá a través del diagrama de clases presentado en la Figura 3. El modelo está compuesto de dos clases principales, *Discussion* y *Comment*, las cuales soportan la interacción de los mensajes.

La clase *Discussion* es la clase central del esquema propuesto. Una discusión es propuesta por un objeto *Member* que representa un usuario inscrito válidamente en una aplicación. Una discusión, entonces, pertenece en forma transitiva a una aplicación en particular, a través de su autor. El autor de una discusión, según el contexto en que se implemente la plataforma, podría ser o no un administrador de la aplicación. Una discusión es dueña de varios comentarios, que pertenecerán a la aplicación dueña de la discusión.

Para modelar las características requeridas por el sistema de discusión, de la clase Discussion derivan clases que representan a cada tipo de discusión soportado: discusión libre (*FreeDiscussion*), discusión débilmente identificada (*WIDiscussion*), discusión fuertemente identificada (*SIDiscussion*), discusión débilmente anónima (*WADiscussion*), y discusión fuertemente anónima (*SADiscussion*). Estas clases también se pueden diseñar utilizando un atributo que indique el tipo de discusión de cada instancia de la clase, sin embargo, las diferencias son suficientes como para usar derivación.

Cada tipo de discusión acepta tipos de comentarios diferentes. Además los tipos de discusión anónima y fuertemente anónima requieren manejar registros de usuarios. Por otra parte, los tipos de discusión anónimos además de los tipos de comentarios anónimos, fuertes o débiles según el caso, también aceptan comentarios de tipo identificado, igualmente fuertes o débiles según el caso. Esto hace que sea más atractivo manejar una lista única de comentarios

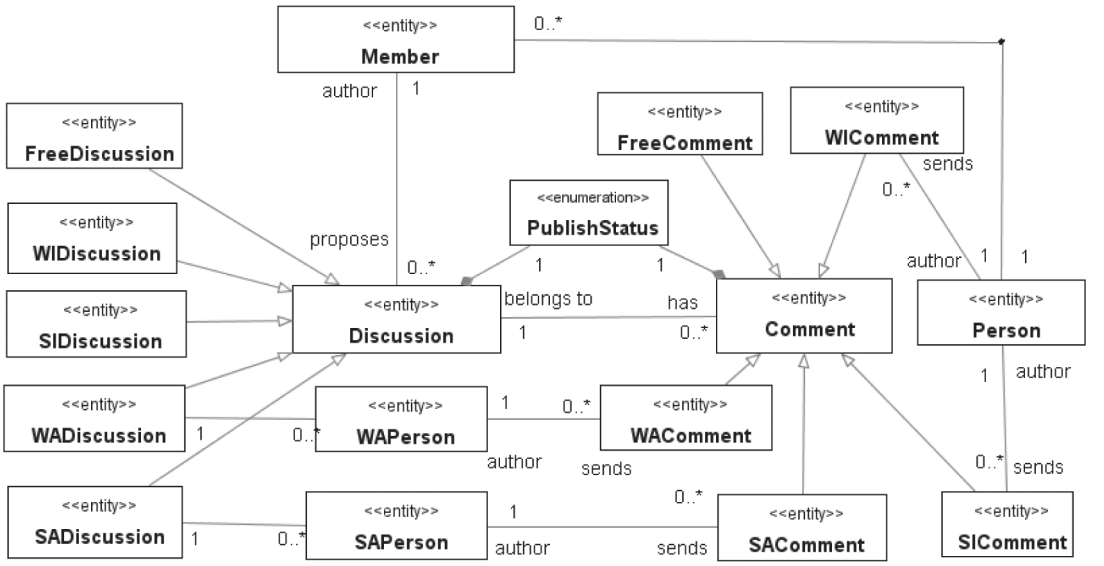

Figura 3. Diagrama de clases para el Modelo de Discusión propuesto.

que provenga de la superclase *Discussion*. De esta manera se introduciría un posible problema de consistencia en el modelo. Aceptándolo como manejable, el esquema propuesto introduce métodos específicos para cada tipo de discusión que solo acepta la agregación de los tipos de comentario que corresponda.

En el modelo se introducen las clases *SAPerson* y *WAPerson*. La primera representa un usuario fuertemente anónimo (UFA) y la segunda un usuario débilmente anónimo (UDA). Ambas clases pertenecen a una sola instancia de *SADiscussion* o *WADiscussion* respectivamente y permanecen durante el ciclo de vida de estas, a diferencia de un usuario que pertenece al censo general y que sobrevive al ciclo de vida de cada discusión.

La clase *Comment* es una clase abstracta que representa los comentarios o mensajes enviados por los usuarios. En el esquema existen cinco tipos de comentarios, siendo la clase *IdentifiedComment* una clase abstracta de conveniencia que permite indicar que los comentarios identificados, fuertes o débiles, tienen un autor proveniente del censo general.

Por su parte, los comentarios fuertemente anónimos representados por la clase *SAComment* tienen como autor un objeto de la clase *SAPerson*, mientras que los comentarios anónimos débiles tienen un autor que se representa como un objeto de la clase *WAPerson*. Los comentarios libres no tienen identificación de ningún tipo. Los comentarios fuertemente anónimos e identificados contienen un atributo *signature* que representa la firma digital de su autor en ellos.

PRUEBA FUNCIONAL

Con el fin de evaluar el cumplimiento de los objetivos del sistema desarrollado hemos realizado un caso de estudio hipotético que ilustra las funcionalidades de éste. Este caso nos permitirá probar el sistema de discusión deliberativa y su seguridad cuando los usuarios participan en modo identificado o anónimo. El escenario es un municipio ficticio llamado Villafeliz.

Escenario

Villafeliz es un municipio de tres mil habitantes que acaba de recibir la llegada de nuevas autoridades luego de la elección municipal. Estas tienen la intención de lograr un mayor involucramiento y compromiso de sus ciudadanos a través de la participación. Sin embargo, estos son apáticos, dado un historial de decisiones arbitrarias y hostigamiento cuando las decisiones de las autoridades van en contra del pensamiento de sus ciudadanos. También se sabe que alguna vez que se requirieron opiniones vía

telefónica, los ciudadanos del municipio vecino y rival, Villatriste, opinaron haciéndose pasar por vecinos de Villafeliz, ante lo cual se tomaron decisiones que en realidad fueron en contra de los deseos del pueblo.

Se asume que Villafeliz cuenta con un padrón municipal donde están los datos de los ciudadanos. También se asume que los ciudadanos tienen medios para acceder a ordenadores conectados por internet. Villafeliz, a su vez, tiene inscritas varias organizaciones sociales o grupos de interés. Existe, por ejemplo, el Grupo de Consumidores o el Grupo de Productores de Vino Enlatado.

Tópicos de Discusión
Villafeliz entonces requiere iniciar una conversación sobre tres tópicos:

- Obtener opiniones sobre el nuevo sitio Web del municipio.
- El Grupo de Productores de Vino Enlatado requiere discutir acerca de la extensión de horarios de cosecha. Los temporeros se oponen, mientras los dueños de la producción quieren presionar a la autoridad.
- Discusión acerca de la autorización para la instalación de un supermercado "HiperMart" en el pueblo. "HiperMart" ha indicado que de no ser autorizados se irán a Villatriste.

Villafeliz recién ha implementado el sistema de discusión ciudadana y quiere probarlo en estos tópicos. Se asume que el Censo de usuarios es completo y cada ciudadano participante es dotado con una copia del programa cliente de la aplicación y acceso a un dispositivo criptográfico. Se identifican los siguientes personajes:

- Guillermo Puertas: Encargado de informática de la Municipalidad, y es quien instaló el sistema y programó las rutinas para adaptar el padrón municipal al censo de usuarios.
- Alcalde Diamante: El recién electo alcalde de Villafeliz quiere aparecer en la prensa nacional a través de la implementación de un sistema de democracia participativa en este pueblo pequeño y aislado. Además, es conocido por sus tendencias favorables al libre mercado y es el principal promotor de la llegada de "HiperMart" al pueblo.
- Alex Torretti: Contendor de Diamante en la pasada elección. Cuenta con un grupo fiel de adherentes y se oponen a la instalación de grandes comercios en el pueblo, para preservar los negocios locales.
- Juan Cuevas: Dirigente de los temporeros que trabajan para los Productores de Vino Enlatado.
- Guillermo Errázuriz: Presidente de los productores.

Pruebas
Guillermo Puertas, instala el sistema y crea una cuenta de administrador para sí mismo. En seguida crea las aplicaciones Villafeliz, Asociación de Consumidores de Villafeliz y Grupo de Productores de Vino Enlatado. Juan Cuevas y Guillermo Errázuriz revisan la lista de aplicaciones y piden unirse a la aplicación "Grupo de Productores de Vino Enlatado". Guillermo Puertas aprueba la solicitud y los transforma a ambos en administradores de la aplicación. Otros miembros de la asociación requieren ser añadidos y ellos aprueban o rechazan las solicitudes. A su vez, Torretti y sus adherentes, entre otros ciudadanos, se unen a la aplicación Asociación de Consumidores de Villafeliz, los cuales son aceptados por Guillermo Puertas.

Puertas crea una discusión, dentro de la aplicación Villafeliz, llamada "Opina sobre el nuevo sitio web del municipio", la cual señala como libre y sin ningún atributo de seguridad. La idea es que todos los miembros del pueblo puedan participar entregando opiniones a modo de "lluvia de ideas".

En la aplicación "Grupo de Productores de Vino Enlatado", Juan Cuevas inicia una discusión débilmente anónima para discutir el asunto de la extensión horaria en conjunto entre los dueños y los trabajadores. Por precaución, indica que la discusión tenga el atributo "no repudio", de modo que los participantes tengan la prueba de que no se han borrado mensajes. En la aplicación del grupo de Consumidores se crea la discusión "¿Debe autorizarse la instalación de HiperMart en el pueblo?", indicando que la discusión es de tipo fuertemente anónima, ya que Torretti se ha quejado ante la prensa nacional de que sus adherentes son perseguidos por las decisiones de Diamante. Además indica que los mensajes irán cifrados en tránsito, para evitar que los habitantes de Villatriste puedan interceptar los mensajes y aprovechar para influir

en la decisión de Villafeliz. También se verificará el no repudio de los mensajes ya que la discusión será traspasada a un acta pública, por lo tanto los ciudadanos han exigido contar con comprobantes de su participación, aun cuando sea anónima.

Torretti y sus adherentes obtienen una credencial para participar en forma anónima y luego inscriben usuarios anónimos para la discusión. Torretti, por ejemplo, inscribió un usuario anónimo con el alias "anónimo1". La discusión se mantiene vigente durante tres semanas, en las cuales Diamante y sus adherentes envían opiniones identificadas a favor, mientras Torretti sigue una estrategia de enviar opiniones identificadas, mientras algunos de sus partidarios opinan anónimamente, incluyendo algunos que trabajan aún en el ayuntamiento. Finalmente, "HiperMart" se instala en el pueblo, sin perjuicio de que en el acta municipal quedaron de manifiesto las oposiciones al proyecto, las cuales en un principio Diamante desconoció, pero luego se vio obligado a reconocer dado que los opinantes tenían las firmas que el sistema de discusión entregó sobre sus opiniones a modo de no repudio. A través de estas discusiones, una libre, otra débilmente anónima y otra fuertemente anónima, se valida el sistema de discusión con sus distintos tipos de participación, dado que en las discusiones anónimas quien lo desea también puede participar de forma identificada.

RESULTADOS

La Tabla 1 muestra las operaciones relacionadas con la creación de discusiones y el envío de comentarios, así como de la obtención de credenciales anónimas.

La función "Verificar Firma" falla en el caso en que un usuario ha firmado un mensaje con un certificado revocado o reemplazado. La falla puede considerarse importante y para su solución requiere la implementación de un sistema que consista de revocación, historial y notificación. Si bien las pruebas fueron en su mayoría exitosas, en cuanto a su efectividad, al momento de su aplicación existen varias consideraciones de orden estético y de usabilidad que se pueden mejorar. Por ejemplo, mejorar los editores de comentarios con el fin de añadir opciones más interesantes de formato o incluir los comentarios en una lista más fácilmente accesible y mostrando a priori el número de ellos o información sobre su actividad dentro del sistema. También la función de obtener credencial debe ser mejorada en cuanto a su presentación, incluso sería deseable la posibilidad de guardar en un archivo el resultado de la operación. La Figura 4 ilustra la adición de la discusión.

La Tabla 2 resume las pruebas realizadas sobre la herramienta de verificación de firma. Las pruebas consistieron en intercambiar distintas combinaciones entre formatos de los tres componentes necesarios para la verificación: Clave pública, firma y texto firmado. Además una prueba consiste en modificar arbitrariamente el texto a verificar para probar que el resultado debe ser incorrecto.

CONCLUSIONES

En cuanto a los objetivos planteados para el servicio de discusión, se ha logrado construir un sistema en que se puede demostrar el uso de atributos de

Tabla 1. Resultados de la prueba funcional del servicio de discusión.

Función	Usuario	Resultado esperado	Resultado
Crear discusión libre	Puertas	Discusión añadida a lista	OK
Crear DDA: NR	Cuevas	Discusión añadida a lista	OK
Crear DFA: NR, Int_Conf.	Diamante	Discusión añadida a lista	OK
Obtener credencial	Torretti	Número de credencial	OK
Registrar UFA	Torretti	Usuario fuertemente anónimo añadido	OK
Enviar comentario Libre	Cuevas	Comentario añadido en lista	OK
Enviar comentario FI	Torretti	Comentario añadido en lista	OK
Enviar comentario FA	Anónimo 1	Comentario añadido en lista	OK
Verificar firma	Torretti	Mensaje: firma válida	Parcial
Verificar firma NR	Torretti	Mensaje: firma válida	OK

Figura 4. Prueba de discusión fuertemente anónima.

Tabla 2. Resultados de la prueba funcional del Verificador de Firma.

Función: Verificar firma	Usuario	Resultado esperado	Resultado
Usando firma PEM	Torretti	Mensaje: Firma válida	OK
Usando firma DER	Torretti	Mensaje: Firma válida	OK
Usando certificado CER	Torretti	Mensaje: Firma válida	OK
Usando clave DER	Torretti	Mensaje: Firma válida	OK
Usando clave PEM incorrecta	Torretti	Mensaje: Firma válida	OK
Modificando el texto firmado	Torretti	Mensaje: Firma válida	OK

seguridad y de los esquemas de identificación y firma. En este sentido se implementó con éxito un sistema que provee funciones de confidencialidad, integridad y no repudio de mensajes. También se pudo implementar un esquema de firma ciega para la obtención de credenciales anónimas y se probó su aplicación para el intercambio de mensajes firmados, tanto anónima como identificadamente.

El sistema da garantías fuertes de que el usuario anónimo no puede ser vinculado con el usuario identificado de origen. Sin embargo, existe una dificultad ante el uso malicioso o para el reemplazo de credenciales anónimas en caso de que un usuario pierda la credencial. El sistema considera el uso de credenciales de largo plazo, a diferencia de lo que ocurre, por ejemplo, en un sistema de votación en que el ejercicio del anonimato es necesario en un período corto. En el sistema que hemos propuesto la solución para el caso en que un usuario pierda sus credenciales y a la vez sus claves es que este descubra su identidad para que se le permita un nuevo proceso de obtención de credencial.

Existen otros esquemas que permiten la revocación y renovación de credenciales, por ejemplo, esquemas de firma grupal. Sin embargo, estos sistemas consideran una entidad con el poder de develar la identidad de un usuario en caso de uso malicioso. En el sistema que proponemos este poder no es aceptable y el uso malicioso debe ser controlado a través de la moderación.

Las pruebas unitarias y funcionales realizadas mostraron éxito en la mayor parte de las funcionalidades críticas implementadas, deficiencias menores y algunas atribuibles al diseño y a la arquitectura que requerirían mayor atención. Esto,

sin perjuicio de lo ya mencionado en cuanto a que se detectó que varias funcionalidades y cambios a nivel de usabilidad son necesarios para lograr una experiencia de usuario más completa.

El sistema propuesto, dado su carácter genérico, tiene múltiples escenarios de aplicación. Sin embargo, deben considerarse necesarias mejoras y adaptaciones para funcionar en escenarios reales. Teniendo esto en cuenta, es posible pensar en aplicaciones para toda clase de organizaciones donde la comunicación entre miembros de base y directivos sea necesaria. Por ejemplo, universidades, clubes deportivos, organizaciones sociales, gremios. Una aplicación del concepto más ambiciosa podría considerar unidades territoriales como ayuntamientos o provincias, utilizando padrones electorales reales e infraestructuras de certificación oficiales. Bajo las condiciones actuales, el escenario más recomendable de aplicación o futuro desarrollo sería en un entorno universitario con un desarrollo medio-alto de competencias informáticas.

La contribución principal del sistema desarrollado es proveer una plataforma con un modelo de seguridad que ayuda a mejorar la confianza de los usuarios en las conversaciones generadas ya sea cuando se identifican o participan anónimamente. Esto ayudará a tener una mayor participación dentro de las organizaciones, logrando consensos o decisiones de mayor calidad.

Trabajo futuro

En primer lugar, se podría implementar este sistema con el uso efectivo de tarjetas inteligentes. JavaCard[2] es una alternativa que va en sintonía con lo ya implementado. Un desarrollo evidente es la agregación de nuevos servicios a la plataforma. Entre los más básicos se puede mencionar un servicio de encuestas, de noticias, de gestión de documentación, de bitácoras personales o de votación electrónica.

En cuanto al proceso mismo de deliberación se pueden agregar funciones de trazabilidad. La idea es poder analizar y hacer seguimiento a los resultados con el fin de poder evaluar su efectividad. Otro componente que se podría agregar al sistema es la implementación de una autoridad certificadora ad hoc. Eventualmente, en un país este rol podría ser tomado por el Registro Civil. Otro campo de trabajo interesante a partir del sistema propuesto es la implementación de esquemas más avanzados de credenciales anónimas [21].

Una característica deseable para la aplicación cliente sería una arquitectura extensible basada en *plugins*. Otra arquitectura a explorar puede utilizar *applets* firmados de java que permitan combinar una interfaz Web con la plataforma.

Finalmente, para validar la herramienta, una vez implementado un sistema de moderación básico se debería diseñar una prueba de campo que considere como variable a medir la confianza de los usuarios al participar en un sistema con posibilidades fuertes de anonimato contra la participación en un entorno común.

[2] http://www.oracle.com/technetwork/java/javacard/

REFERENCIAS

[1] S. Airworth, C. Hardy and B. Harley. “Online consultation: E-Democracy and E-Resistance in the Case of the Development Gateway”, Management Communication Quarterly. Vol. 19, Issue 1, pp. 120-145. August, 2005.

[2] S. Benhabib. “Democracy and Difference: Changing Boundaries of the Political”. Princeton University Press. 1996.

[3] M. Bohlen, W. Gamper, J. and Polasek and M. Wimmer, Eds. “E-Government: Towards Electronic Democracy”. Vol. 3416. 2005.

[4] M. Castells. “Materials for an exploratory theory of the network society”. British Journal of Sociology. Vol. 51, Issue 1, pp. 5-24. January-March, 2000.

[5] J. Cohen. “Deliberation and Democratic Legitimacy”. A. Hamlin and P. Petit, Eds.. Stanford Law School. 1989.

[6] D. Consortium. “Dunes-Dialogic and argumentative negotiation educational software”. 2003. URL: http://www.dunes.gr

[7] W3C Consortium. “Web technologies supporting direct participation in democratic processes (WEBOCRACY)”. URL: http://www.webocrat.sk/webocrat/

[8] R.A. Dahl. “Democratic Dilemma: System Effectiveness versus Citizen Participation”. Political Science Quarterly. Vol. 109, Issue 1, pp. 23-34. 1994.

[9] C. Farrelly. "Deliberative Democracy". Sage publications. 2004.

[10] W. Friedman. "Deliberative Democracy and the Problem of Scope". Journal of Public Deliberation. Vol. 2, Issue 1, pp. 1-29. 2006.

[11] A. Gómez, S. Sánchez, C. González, E. Pérez, J. Moreno and J. Carracedo. "Architectural design for a Digital Democracy telematic platform". Proceedings of the CollECTeR Latam Conference. Talca, Chile. 2005.

[12] T. Gordon Thomas and G. Richter. "Discourse Support Systems for deliberative Democracy". Technical Report, Fraunhofer Institute. 2002.

[13] C. Grillgreen and J. Bryson. "E-engagement: Guidelines for community engagement using ICT". Government of Western Australia Report. 2005.

[14] J. Habermas. "Legitimationsprobleme im Spatkapitalismus". Traducción de Thomas McCarthy. Beacon Press. Boston. 1975.

[15] J. Habermas. "The Structural Transformation of the Public Sphere: An Inquiry Into a Category of Bourgois Society". MIT Press. Cambridge, USA. 1962.

[16] B. Hohberg and R. Lührs. "Offline Online Inline: Zur Strukturierung internetvermittelter Diskurse". Fecha de consulta: 20 Abril de 2008. URL: http://www.demosproject.org/files/HohbergLuehrs.pdf.

[17] M. Lehtonen. "Deliberative Democracy, Participation, and OECD Peer Reviews of Environmental Policies". American Journal of Evaluation. Vol. 27, Issue 2, pp. 185-200. 2006.

[18] J. Lofton. "C Structuring the G2C Component of E-Government Systems: Uncloaking the Clandestine Relationships among Governance and E-Government". Anales del Primer Congreso Iberoamericano en Gobierno Electrónico. Santiago, Chile. 2006.

[19] R. Lührs, T. Malsch and K. Voss. "Internet Discourses and Democracy". Lecture Notes in Computer Science. Vol. 2253, pp. 67-74. 2001.

[20] R. Lührs, J. Pavn and M. Schneider-Fontn. "Demos tools for online discussion and decision making". Proc. of the International Conference on Web Engineering. pp. 167-180. 2003.

[21] A. Lysyanskaya and J. Camenisch. "An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation, Advances in Cryptology". Lecture Notes in Computer Science. Vol. 2045, pp. 93-118. 2001.

[22] J. Mansbridge. M. Amengual, J. Gastil and J. Hartz-Karp. "Norms of Deliberation: An inductive study". Journal of Public Deliberation. Vol. 2, Issue 1. 2006.

[23] M. Meier. "Youth parliament esslingen, living e-democracy first binding election to public office over the internet worldwide". Esslinger Innovationspartner, Steinbeis-Transferzentrum Mediakomm. Technical report. 2001.

[24] A. Meiklejohn. "Free Speech and Its Relation to Self-Government". Harper Brothers Publishers. New York. 1948.

[25] E. Pérez, A. Gómez, S. Sánchez, J.D. Carracedo, J. Carracedo, C. González and J. Moreno. "Design of an advanced platform for citizen participation committed to ensuring freedom of speech". Journal of Theoretical and Applied Electronic Commerce Research. Vol. 1, Issue 2, pp. 58-71. 2006.

[26] J. Rawls. "A Theory of Justice". Harvard University Press. Boston. 1971.

[27] S. Salz and O. Marker. "Anforderungen an e-diskurs-plattformen illustriert am beispiel dito". Innovative Informatikanwendungen. 2003.

[28] F.E. Scott. "Participative democracy and the transformation of the citizen: Some intersections of Feminist, Posmodernist and Critical tought". American Review of Public Administration. Vol. 30, Issue 3, pp. 252-270. 2000.

[29] K. Silveira, R Shaffer and C.A. Behr. "A summary of citizen participations methods for the waterfront development project in Oconto". University of Wisconsin-Madison, Report. 1993.

[30] E. Tambouris, E. Spanos, S. Gorilas, D. Hoholis and M. Sintichakis. "EURO-CITI Tele-Voting: An Application for Realizing Opinion Poll Petitions". 15th Bled Electronic Commerce Conference eReality: Constructing the eEconomy. 2002.

[31] J.B. Thompson. "La teoría de la esfera pública". Voces y Culturas. Vol. 10. Barcelona, 1996.

[32] G. von der Walde and G. Cervelló. “Madrid Participa: e-Participation initiatives in the City of Madrid”. Anales del Primer Congreso Iberoamericano en Gobierno Electrónico. Santiago, Chile. 2006.

[33] A. White and A. Mackintosh. “Electronic democracy european network (eden)”. International Teledemocracy Center. Technical report. 2001.