Voto y encuestas telemáticos en la Universitat Jaume I

Manuel Mollar (mollar@uji.es), Vicente Andreu (vandreu@uji.es), J. Pascual Gumbau (gumbau@uji.es), Modesto Fabra (fabra@uji.es), Paul Santapau (santapau@uji.es).

Resumen

Este documento ofrece una descripción general del sistema de encuestas y voto telemático de la Universitat Jaume I. El objetivo primero de ambos sistemas es garantizar al usuario el máximo nivel de anonimato sin tener que confiar en los responsables administrativos o en los técnicos administradores del sistema. El anonimato se basa en la arquitectura del sistema construido y en el software que lo implementa, distribuido como código abierto. En el caso de las votaciones el sistema garantiza también la integridad del recuento gracias a su diseño y a la forma en que es operado.

Introducción y objetivos

La Universitat Jaume I se define por su apuesta sobre el uso de las nuevas tecnologías como eje central de su gobierno. Durante estos últimos años se han desarrollado herramientas con el fin de respaldar este hecho.

Esta universidad siempre ha sido consciente del papel que juegan las nuevas tecnologías en la relación con el alumnado, los profesores y el personal de administración y servicios en general, es por eso que ha focalizado esfuerzos en el desarrollo de herramientas que faciliten los diversos trámites y gestiones dentro del ámbito universitario. En este documento presentamos un sistema que acomete dos objetivos distintos pero relacionados.

En primer lugar, la realización de encuestas que reflejen una fidelidad lo suficientemente acorde con la realidad, requiere disponer de una total garantía de anonimato, de forma que el encuestado tenga la seguridad de que sus respuestas no van a ser relacionadas con él en ningún momento y que, así, pueda expresar su opinión real en la misma sin ningún tipo de coacción.

La realización de una campaña tradicional de encuestas, realizada en soporte "papel", inspira confianza a los participantes en tanto que el anonimato parece obvio, deducible a simple vista si se realiza correctamente y necesita escasa auditoría. Frente a ello, el uso de medios

electrónicos el anonimato se presupone por la confianza que el participante deposita en una persona que se supone un profesional intachable, o en una empresa u organización ajena al encuestador y el encuestado que actúa con profesionalidad. Pero al final, detrás de un sistema informático hay una persona, a veces varias, por cuyas manos pasan los datos, con capacidad plena para inspeccionarlos. En resumen, el anonimato se basa en la honradez de una persona, o lo que es peor, de varias “en paralelo”.

El sistema construido provee de anonimato (incluyendo no-trazabilidad) basándose en la profesionalidad de muchas personas “en serie”, es decir que para romper el anonimato sería necesario poner de acuerdo a muchas personas, como tendría que hacerse en el caso del soporte "papel", en el que para romper el anonimato se tendrían que poner de acuerdo al menos el encuestador marcando las hojas y quien las procesa. La ventaja del sistema telemático es que las personas que intervienen están distribuidas geográficamente y ni siquiera se conocen entre ellas, con lo que podemos garantizar que se alcanza un nivel de anonimato igual o superior al del procedimiento “en papel”.

Todo el anonimato se construye a nivel técnico en el cliente, que emplea programas de código abierto los cuales se pueden obtener de forma segura y someter a extensa auditoría. El usuario sólo necesita un navegador de Internet que soporte Javascript.

Este proyecto también engloba los procesos electorales, que son de una importancia clave para nuestra sociedad, como una de las principales herramientas garantes del sistema democrático. Es por esto que continuamente se debe trabajar en pulir y revisar los mecanismos que velan por la integridad y el anonimato de las elecciones, así como tratar de acercarlas más al votante, con el fin de conseguir una mayor participación y facilitar al ciudadano que, por razones médicas, de accesibilidad o de residencia, presenten más dificultades para ejercer su derecho al voto. Esta es la razón de ser de los sistemas de voto telemático.

Adicionalmente, el voto telemático ofrece sustanciales mejoras en aspectos administrativos y logísticos. Un sistema de voto telemático bien diseñado e implantado, nos permitirá minimizar las tareas burocráticas y la generación de documentos, eliminando los costes de producción, distribución y verificación manual de papeletas, actas, sobres y censos, atenuando la probabilidad de error humano en alguna sección del procedimiento. La centralización de la información, entre otras ventajas, permite evitar los problemas derivados de la asignación exclusiva de un censado a un colegio electoral, así como reducir drásticamente el número de oficiales de mesa movilizados y, en aquellos que sigan siendo necesarios, puede reducir el tiempo servicio.

Un sistema de voto tradicional también nos presenta el problema de la coacción. La implantación de un sistema de voto telemático, da libertad al votante de ejercer su derecho en cualquier punto del planeta con una conexión a Internet. De este modo, un votante que tema ser coaccionado, puede ejercer su derecho sin abandonar su casa, o ejercerlo antes de que el coactor pueda ejercer su presión.

No obstante, el sistema de voto telemático se encuentra con nuevos retos, pues además del anonimato, deben garantizarse al menos la integridad y unicidad del proceso. Es decir, que sólo votan las personas autorizadas, que los votos depositados en la urna son los emitidos por los votantes (sin posible inyección), y que el recuento final responde a la realidad de los votos emitidos.

Tras evaluar las diferentes soluciones comerciales existentes en el momento, se acordó emprender el desarrollo de un producto totalmente nuevo, que subsanase las carencias presentes en los sistemas analizados previamente. Como consecuencia de este desarrollo se consiguió un producto capaz de ofrecer las máximas garantías de anonimato para el votante, la máxima confidencialidad en el proceso de voto y la máxima integridad de los votos, minimizando el número de personas o entidades sobre las que fundamentar la confianza en el proceso electoral y disolviendo la responsabilidad entre todos los miembros, evitando así posibles filtraciones o accesos ilícitos por parte de disidentes actuando en solitario o en pequeños grupos. Por ejemplo, el sistema, una vez iniciado no necesita (ni permite) la intervención de un técnico informático.

Encuestas telemáticas: eSurvey.

El responsable del anonimato y la no trazabilidad es un sistema al que hemos denominado eSurvey. En propósito de eSurvey es que el anonimato y la no-trazabilidad de una encuesta no dependan del encuestador. Para que una encuesta tenga pleno sentido, el encuestado debe estar identificado (y autenticado) en el sistema de encuestas. Con ello, un administrador de sistemas malicioso puede fácilmente establecer la relación entre encuesta y encuestado, es decir que el anonimato se apoya en la integridad de (o de los) administrador del sistema informático.

Una primera solución sería que las encuestas estuvieran cifradas con una llave que estuviera en manos de un tercero, que abriera la urna de encuestas al final del escrutinio. Este método divide la confianza entre dos personas, pero fuerza a no disponer de resultados parciales de la encuesta. Además supone modificar cualquier software de encuestas existentes.

Frente a ello, eSurvey en primer lugar, alcanza el anonimato empleando la firma ciega de Chaum. El encuestado obtiene un ticket firmado anónimo del encuestador, de modo que no se puede relacionar encuesta y encuestado. No obstante, el sistema sería totalmente trazable, pues el administrador del sistema puede localizar en el tiempo y en el espacio (en la red, a través de la IP) al encuestado, relacionando el proceso de autenticación con el momento de entrega de la encuesta. Para evitarlo, la encuesta no se entrega al destinatario sino (cifrada) a un intermediario que la conserva un tiempo calculado por eSurvey y después la envía al encuestador, al que le llega deslocalizada en el tiempo y el espacio. Basta con poner más intermediarios en serie para repartir la confianza entre más personas. Cada intermediario recibe un bloque de datos cifrado para él y al descifrarlo obtiene la dirección del siguiente y el tiempo que debe retener la encuesta. Por ello sería necesaria la sincronización de todos los intermediarios para poder localizar una encuesta. En la práctica basta con un par de intermediarios para alcanzar el suficiente anonimato. Los intermediarios son entidades con credibilidad probada, independientes y con intereses totalmente dispares. A la red construida la hemos denominado Red de Latencia Controlada (LCN).El algoritmo de envío a través de la LCN también contempla el uso de varios caminos redundantes para proveer de tolerancia a fallos al envío.

Con este diseño, *eSurvey* es una capa de anonimato que puede añadirse a cualquier programa de encuestas web ya construido, en el que basta con reemplazar el botón de envío por una llamada a eSurvey. Actualmente, *eSurvey* ha sido incluido en el CMS *Drupal,* en *software* de encuestas *Opina* extensamente empleado en el ámbito universitario y, obviamente, en el ERP de la Universitat Jaume I.

Para emplear *eSurvey* el encuestado no necesita ningún software adicional a su navegador, pues la parte de cliente de *eSurvey* está construida en Javascript. El software es descargado por el cliente cada vez, pero puede ser pre-instalado en el navegador Firefox para la máxima confianza, para lo que basta con realizar un solo click.

La ventaja de ser código abierto es que puede ser permanentemente auditado sin necesidad de acudir al desarrollador.

Voto telemático.

Para un sistema de voto telemático, el anonimato no es el único requerimiento indispensable. El sistema de voto telemático de la Universitat Jaume I (en adelante VTUJI), establece una serie de roles funcionales, cuyo cometido es la puesta en marcha y mantenimiento del sistema, ser los depositarios de la confianza del votante y ser los encargados de velar por que se cumplan todos los procedimientos administrativos que complementan las medidas lógicas que ofrece el sistema VTUJI.

En primer lugar, el votante no necesita confiar en el desarrollador del software, pues, en su apuesta por el software libre, la Universitat Jaume I ha construido todo el sistema en código abierto, permitiendo así a cualquier elector u órgano interesado revisar y auditar el sistema de forma totalmente transparente.

En segundo lugar, y ya centrados en la operativa del sistema, se ha elegido un esquema de responsabilidad en que toda la confianza está sustentada en una comisión central de voto. La

composición de esta comisión debe ser tal que: o represente los intereses opuestos de todos los votantes, o esté formada por un grupo de miembros de la comunidad notables por su integridad, imparcialidad y compromiso con el sistema electoral. Esta comisión será la depositaria de la llave de cifrado del sistema de voto, habilitándola en exclusiva para iniciar y acceder al sistema. Para evitar acciones individuales o grupusculares que pudiesen comprometer la integridad del sistema de voto, accidentalmente o en nombre de una de las partes interesadas, la llave se repartirá por medios criptográficos entre todos los miembros de la comisión, requiriendo para reconstruirla un número mínimo de miembros que oscilará según la composición de la misma (pero que, al no precisar a todos los miembros, dará un margen de seguridad para salvar la ausencia justificada de alguno de ellos o la pérdida o destrucción accidental de fragmentos de llave).

Cabe destacar que, frente a otros sistemas, el VTUJI elimina la confianza en los roles de técnico especializado o administrador del sistema, negándoles cualquier clase de acceso al sistema, con la que pudiesen adulterar el funcionamiento del mismo, probablemente sin ser detectados y con consecuencias nefastas. Sin embargo, todos los sistemas de voto telemático estudiados son susceptibles ante un acceso físico a la máquina, que le daría poder total al atacante. El VTUJI se fundamenta en que toda la operativa está escrita en una unidad de CD-ROM, que por su naturaleza de sólo lectura y las medidas de seguridad tomadas, no puede ser adulterada. Los datos que deban ser almacenados, son encriptados en un dispositivo de almacenamiento impidiendo su violación.

Durante el proceso electoral, y gracias a la arquitectura del sistema y a los algoritmos criptográficos empleados, el votante posee, entre otras, las siguientes garantías:

1. Que la conexión al servidor de voto es privada, segura y que la identidad del servidor es la esperada.
2. Que la urna no se abrirá hasta el fin de la elección, no pudiendo obtenerse resultados parciales en ningún momento que puedan violar la privacidad del votante.
3. Que no se almacena información que relacione un voto con su votante.
4. Que una vez emitido, su voto no puede ser manipulado ni alterado.
5. Que un votante no podrá emitir múltiples votos ni votar en una elección en cuyo censo no conste.
6. Que las actas de los resultados electorales no pueden ser manipuladas ni alteradas una vez aceptadas por los miembros de la comisión, al ir firmadas electrónicamente
7. Que cada voto va a ser contabilizado.

El organizador del proceso electoral, posee, entre otras, las siguientes garantías:

1. Que los votos recibidos pertenecen a votantes registrados en el censo y se han emitido entre la hora de apertura y cierre de urnas.
2. Que un votante no ha podido emitir más de un voto ni ha participado en una elección en cuyo censo no conste.
3. Que las actas de los resultados electorales no pueden ser manipuladas ni alteradas una vez aceptadas por los miembros de la comisión, al ir firmadas electrónicamente.

Adicionalmente, y aunque el hecho de no emplearlas no supone ningún riesgo para el proceso, el VTUJI ofrece herramientas que permiten alterar ligeramente su funcionamiento, ofreciendo algunas garantías adicionales, para usuarios especialmente preocupados en aspectos como el anonimato o la participación activa de mesas electorales.

En primer lugar el cliente puede activar el uso de eSurvey, de modo que alcanza el anonimato por sus propios medios. Obsérvese que el sistema VTUJI no requiere de eSurvey, pero es una opción de refuerzo que puede decidir el votante.

En segundo lugar, el modelo de confianza empleado en el VTUJI, relega a la tradicional mesa electoral a un papel de mero observador, permitiéndole sólo observar los resultados y firmar las actas. En algunas situaciones, puede ser deseable dotar a la mesa electoral de un mayor control sobre el proceso de recuento, ejecutándolo en un entorno totalmente controlado por ellos y pudiendo auditar cada detalle del software empleado y del procesamiento de votos.

Con esta finalidad , se creó un componente adicional al navegador Mozilla Firefox, que permite

a la mesa electoral, de forma segura y autenticada, descargar las papeletas presentes en el servidor y realizar un recuento en su propio ordenador, proporcionándoles más información y permitiéndoles controlar y auditar por completo el proceso de recuento, prescindiendo de la confianza en el software del servidor.

Implantación.

Nuestra universidad posee un ERP universitario el cual cubre el 90% de los procedimientos que se llevan a cabo dentro de la misma. En el contexto de este ERP se llevan a cabo las encuestas realizadas por las distintas unidades organizativas dentro de la universidad este procedimiento de realización de encuestas ha sido adaptado a eSurvey, permitiendo de una forma totalmente integrada la realización de encuestas anónimas desde el propio ERP.

Por otra parte el sistema de voto telemático se ha empleado para realizar votaciones en las elecciones a miembros no natos de los Consejos de Departamento, un piloto con dos departamentos en mayo de 2009 y seis votaciones en diciembre de 2009, resolviendo el problema de la falta de participación de los miembros no natos y dando la posibilidad de votar de forma sencilla a los miembros que por razones laborales no pueden desplazarse hasta la Universidad el día de las elecciones.

Estos resultados vienen a reforzar el despliegue de la administración electrónica en la Universitat Jaume I, que desde hace años viene resultando en sistemas consolidados cuyo uso trasciende el de la Universidad. Ejemplos serían el *CryptoApplet,* que permite la realización de firma multiformato (*PKCS#1, CMS, XML Signature, XAdES, PDF, ODF*, etc.) ofreciendo un integración simple en cualquier aplicación web que necesite de un proceso de firma, empleado por diversos sectores de la administración pública; o el *Clauer*, que resuelve mediante una memoria USB el problema del transporte de claves y certificados para firma electrónica y que es ampliamente utilizado fuera de la Universidad.

Conclusiones

El sistema de encuestas y voto telemático, aquí presentado, ofrece las máximas garantías de integridad, unicidad, anonimato y auditabilidad, constituyéndose en una herramienta útil en el marco de la administración electrónica.

Todo el desarrollo es código abierto y puede ser utilizado por cualquier entidad interesada.

En general, las herramientas aquí presentadas se utilizan en diferentes procedimientos administrativos. En su conjunto, estas herramientas permiten la correcta implantación de la administración electrónica fomentando la confiabilidad, seguridad, accesibilidad y participación de los miembros de la comunidad universitaria.

Además, cumplen con requisitos más técnicos como pueden ser la multiplataforma y el multilingüismo permitiendo un mayor impacto en el uso de estas herramientas tanto dentro de la Universidad como por cualquier otro organismo o entidad que desee aplicarlas.

Referencias

Sitio Web del proyecto (2010). *Universitat Jaume I – Equipo de desarrollo*. Consultado 4 Marzo, 2010 en: http://esurvey.nisu.org

Sitio Web de desarrollo (2010). *Universitat Jaume I – Proyectos Open Source*. Consultado 4 Marzo, 2010 en: http://forja.uji.es/projects/esurvey

Sitio Web de despliegue de la aplicación (2010). *Universitat Jaume – Proyectos TIC*. Consultado 4 Marzo, 2010 en http://proyectostic.uji.es/pr/vot/

Firma ciega de Chaum. *Wikipedia*. Consultado 4 Marzo, 2010 en http://en.wikipedia.org/wiki/Blind_signature