Aportaciones del proyecto VOTESCRIPT a los esquemas tradicionales de voto electrónico

Ana Gómez Oliva[1], Jesús Moreno Blázquez[1] y Sergio Sánchez García[2]
[1]Departamento de Ingeniería y Arquitecturas Telemáticas. Universidad Politécnica de Madrid
Ctra. Valencia km. 7. 28031 Madrid.
Teléfono: 913 36 78 20. Fax: 913 36 78 17
E-mail[1]: {agomez,jmoreno}@diatel.upm.es
E-mail[2]: ssanche@proyectos.diatel.upm.es

Abstract. *This paper hallmarks the most relevant contributions carried out by the authors in the VOTESCRIPT project (TIC2000-1630-C02). The main goal of this project was the analysis, definition and implementation of a system which copes with every phases and elements existing in a process of electronic voting using computer networks. A summary of the main criticisms of electronic voting is presented to disclose that the most relevant voting schemes only take into account a technological perspective, just trying to imitate the conventional voting schemes. Nevertheless in these proposals important aspects such individual and global verification are not properly undertaken. The paper includes the proposed solutions of the project to solve these mentioned problems.*

1. El voto electrónico ¿una realidad inmediata?

Continuamente los medios de comunicación nos ofrecen noticias sobre el éxito de nuevas experiencias de voto electrónico que se llevan a cabo en todo el mundo. Ante esta profusión de acontecimientos cabe preguntarse si realmente la votación electrónica ha alcanzado ya la madurez y, en breve, podrá sustituir a la votación tradicional.

Sin embargo, un primer análisis de estas experiencias nos lleva a comprobar que el término de *votación electrónica* es un término muy amplio que engloba numerosas actuaciones que pueden ser clasificadas en dos grandes apartados:

- El que sustituye alguno de los elementos físicos del procedimiento de votación clásico por algún tipo de proceso electrónico y
- El que emplea redes telemáticas para comunicar a los votantes con una Mesa Electoral remota.

La casi totalidad de las acciones gubernamentales encaminadas a la automatización de los procesos de votación se encuadran en las actuaciones del primer apartado, siendo la urna electrónica, con o sin papeleta, el dispositivo más comúnmente empleado en todos los casos (la reciente experiencia de Brasil con 135 millones de personas empleando este sistema avalan la validez oficial de este método, a pesar de las nulas garantías de verificación que ofrecía, por tratarse de un sistema de urna sin papeleta).

El segundo apartado, voto a través de Internet, que nosotros hemos dado en llamar **voto telemático**, es el que, a priori, resulta más atractivo desde el punto de vista del ciudadano, ya que le permitiría votar desde casa o desde cualquier punto destinado al efecto, sin necesidad de estar ligado a un determinado Colegio Electoral. Sin embargo, es aquí donde se plantean los mayores retos, no sólo desde el punto de vista técnico, ya que es preciso dotar al sistema de las adecuadas medidas de seguridad, sino también desde el punto de vista social, puesto que el sistema no debe fomentar un desequilibrio en la participación, y por tanto, en la toma de decisiones, en función del nivel de formación informática del ciudadano.

En este apartado, voto telemático, se han realizado escasas experiencias con validez oficial, destacando que en la mayoría de ellas no se reproducen las mismas garantías de seguridad que se proporcionan con el sistema de voto tradicional, como son la posibilidad de que existan interventores para supervisar el proceso o que, en caso de discrepancia, exista la posibilidad de verificar los resultados.

El proyecto VOTESCRIPT[1], finalizado oficialmente en diciembre de 2002, ha abordado la problemática de los sistemas de votación telemática, teniendo como objetivos la modelización y el desarrollo de un prototipo de votación electrónica para realizar votaciones seguras mediante redes de ordenadores públicas y, por tanto, no seguras. Este trabajo ha incluido la realización del análisis, la definición y la implementación de un sistema capaz de soportar los diferentes pasos y elementos existentes en un proceso de votación electrónica, abarcando desde el proceso de emisión del voto hasta el proceso de recuento.

[1] El proyecto VOTESCRIPT (TIC2000-1630-C02) ha sido subvencionado por el Ministerio de Ciencia y Tecnología dentro del Plan Nacional de I+D+I (2000-2003)

Este proyecto ha sido abordado desde una perspectiva integradora que tuviera presente tanto los aspectos técnicos como los sociales, esto es, la solución técnica propuesta debería incluir los mecanismos necesarios para resolver todos los aspectos de seguridad exigibles a un sistema de votación telemática pero, a la vez, esta solución debería ser diseñada de manera que gozara de una amplia aceptación por parte de los ciudadanos.

Este papel destaca las principales aportaciones de este proyecto a la votación electrónica, comparando las soluciones propuestas con las recogidas en los principales esquemas de votación que hoy día sirven de referencia en esta área.

Cabe destacar que durante la realización de este proyecto ha existido una colaboración con la Casa de la Moneda, de manera que parte de las soluciones aquí propuestas han sido trasladas al sistema de votación desarrollado por la Casa de la Moneda, del que se realizó una experiencia piloto en El Hoyo de Pinares (Avila) el pasado mes de marzo.

2. Puntos débiles de los sistemas de votación electrónica

Las principales críticas que se hacen a los sistemas de votación electrónica fueron recogidas por Mercuri[1] en su intervención en la Cámara de Representantes del Comité de Ciencia de EEUU. Pueden resumirse en:

a) Que es imposible superar aspectos tan críticos como son el riesgo de venta de votos, coacción, monitorización clandestina y denegación del derecho a voto.

b) Que no hay forma de ofrecer al votante la seguridad de que el voto se ha registrado tal cual ha sido emitido, o que el recuento es el correcto.

c) Que no ofrece control por parte de los partidos políticos.

d) Que los defectos del sistema pueden ser conocidos años después de la elección y que no hay elementos de auditoría.

e) Que los mecanismos criptográficos se pueden romper tarde o temprano.

f) Y que desde cualquier lugar del mundo se pueden atacar los sistemas telemáticos.

La primera tarea del proyecto fue analizar las soluciones que diversos autores han propuesto para solventar los problemas mencionados. Estas soluciones o *esquemas de votación* definen los agentes, procedimientos y protocolos de seguridad necesarios para llevar a cabo el proceso de votación.

En los esquemas de votación analizados (de los que son una muestra [2] [3] [4] [5] y [6]), la determinación de los requisitos de seguridad que debía reunir el sistema se realizaba reproduciendo las garantías proporcionadas por el voto tradicional, por lo que estos esquemas se centran en garantizar el anonimato del votante.

En este proyecto se ha abordado el desarrollo del sistema desde un punto de vista interdisciplinar, tanto sociológico como telemático, lo que ha propiciado que el sistema de votación se haya diseñado en base a los nuevos requisitos demandados por los ciudadanos y determinados por la investigación sociológica. Entre estos requisitos demandados por los votantes cabe destacar la necesidad de disponer de herramientas para poder verificar el correcto funcionamiento del sistema, no sólo a nivel global, sino también a nivel particular.

En los esquemas citados se observó que, en la mayoría de ellos, no existía la posibilidad de verificar que el sistema operaba correctamente, es decir, que como consecuencia del comportamiento malicioso de algún agente telemático del sistema (Mesa Electoral, Urna o Contador) o la confabulación de varios agentes dentro del sistema, no se estaba produciendo una alteración de los resultados de la votación.

Por tanto, las tareas de este grupo se centraron en el desarrollo de un esquema de votación que ofreciera a los votantes, al menos, las mismas garantías de seguridad que la votación tradicional, poniendo especial énfasis en que además ofreciera pruebas robustas (mediante el empleo de algoritmos criptográficos) del correcto funcionamiento del sistema.

3. Características del sistema definido en el proyecto VOTESCRIPT y resumen de la arquitectura

En el desarrollo del proyecto VOTESCRIPT se decidió emplear tarjetas inteligentes para garantizar la identidad del votante, mediante un certificado personal incluido en la tarjeta. En este punto, se vio la conveniencia de emplear tarjetas criptográficas que permitieran, además, la realización de determinadas funciones de cifrado/descifrado o comprobación de firmas dentro de la propia tarjeta, con objeto de impedir el ataque al sistema. Asimismo, se detectó la necesidad de almacenar cierta información asociada al proceso de emisión del voto, con vistas a una posible verificación posterior.

Respecto a las **críticas a)** y **f)** del apartado anterior se constató que la votación desde casa a través de Internet, aunque puede ofrecerse con las garantías de seguridad adecuadas, hoy día presenta riesgos derivados principalmente de la dificultad de determinar la libertad de acción de la persona que

está utilizando la tarjeta de identificación y por las serias amenazas al sistema que pudieran derivarse de un ataque de denegación de servicio originado por *hackers* que impidieran la celebración de la votación. Por tanto, se consideró que el sistema con más expectativas de éxito a medio plazo era aquel en el que se empleasen puntos de votación que se comunicaran con una urna central mediante una red privada virtual.

En este diseño, se optó por un sistema en el que el votante debe emplear una cabina de votación para emitir su voto, desplazándose a un Colegio Electoral, en lugar de hacerlo desde casa por Internet. De esta forma, se ha pretendido satisfacer de forma más adecuada los requisitos de seguridad necesarios, así como evitar la problemática de la compra de votos, la coacción en el momento de la emisión del voto y la posibilidad de ligar el voto con la ubicación física del votante.

El sistema diseñado se compone de un conjunto de agentes telemáticos (véase Fig. 1), que resumidos brevemente son:

Las Cabinas de Votación, un Sistema Administrador o Autoridad de Identificación encargada de validar al votante como persona autorizada a votar por estar en el censo, un Sistema de Intervención por cada una de las distintas candidaturas que se determine deban participar en la fase de votación, una Urna, un proceso Contador y un conjunto de Puntos de Verificación. El sistema contempla, además, la existencia de una persona jurídica, la Autoridad de Elección, encargada del control general, que se ocupa de atender todas aquellas posibles reclamaciones con respecto al funcionamiento del sistema.

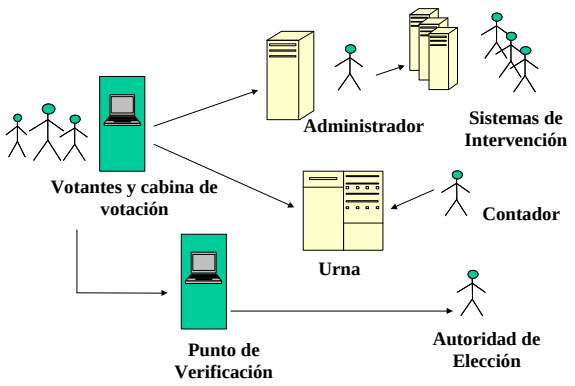

Fig. 1 Agentes telemáticos definidos en el sistema VOTESCRIPT

Como paso previo al comienzo de la votación, se habrá hecho llegar a los votantes una tarjeta inteligente y un identificador de votante que deberá ser conocido por todos los agentes del sistema VOTESCRIPT. La tarjeta inteligente, diseñada especialmente para este proyecto, es capaz tanto de generar claves como de realizar gran parte de los procesos criptográficos necesarios para la seguridad del sistema.

Una vez publicados los resultados de la votación y durante un tiempo limitado, es posible una verificación individual que podrá ser realizada por los votantes a través de los Puntos de Verificación. Asimismo, las distintas candidaturas podrán llevar a cabo una verificación global de los resultados apoyándose en las pruebas criptográficas acumuladas en los Sistemas de Intervención durante el proceso de votación.

4. Aportaciones arquitecturales

En este apartado se comentan las medidas novedosas que han sido incorporadas en la arquitectura del sistema para superar los problemas y críticas mencionados anteriormente.

- Existen unos Sistemas de Intervención para las candidaturas. Cada uno de los Sistemas de Intervención está controlado por un interventor. Estos sistemas, que forman parte del sistema global, serán proporcionados por la Administración Pública y no serán elementos propiedad de las candidaturas. Se prevé que estén ubicados en el mismo entorno que el Administrador y que sus programas estén homologados y sean resistentes ante ataques. Asimismo, se prevé que puedan ser auditados por peritos de confianza de las candidaturas antes del proceso de votación.

  La existencia de los Sistemas de Intervención es una de las principales aportaciones de este sistema, puesto que permite el control, por parte de los partidos políticos, de todo el proceso electoral, a la vez que les dota de la posibilidad de realizar de forma sencilla una auditoría no sólo del resultado final sino de todo el proceso. Esta característica permite contrarrestar la **crítica c)** del apartado 2.

- Existe un conjunto de Puntos de Verificación. Los puntos de verificación son elementos cuya funcionalidad es la de proporcionar a los votantes un lugar en el que llevar a cabo la verificación individual del tratamiento dado a su voto por parte del sistema. Mediante la verificación individual cada votante podrá comprobar, de forma independiente, si su voto se ha tenido en cuenta y ha sido correctamente contabilizado.

  Estos puntos de verificación pueden ser las mismas cabinas de votación u otros sistemas adicionales. El principal requisito de seguridad que se les exige es que no den publicidad a la clave con que se ha emitido el voto para evitar así la compra de votos.

- Existe una Autoridad de Elección encargada del control general del sistema, de velar por su correcto funcionamiento, ocupándose de atender todas las posibles reclamaciones que realicen los votantes. En el caso de que se produzca una reclamación por parte de un votante sobre el tratamiento dado a su voto, ésta descubrirá y comparará todas las pruebas criptográficas presentes en el sistema para comprobar la validez del recuento. Solicitará al votante la tarjeta utilizada para la votación y, a partir de ella, podrá determinar si el votante tiene o no razón, si ha existido o no una falsificación por parte del sistema, y estará en condiciones de llevar a cabo las acciones necesarias en cada caso.

- La Urna, además de recoger y almacenar el voto, genera y envía a la Cabina un comprobante de su entrega, que ésta guarda en la tarjeta inteligente del votante. Mediante este comprobante el votante podrá verificar su voto y reclamar en el caso de que detecte un tratamiento incorrecto de su voto por parte del sistema.

5. Verificación

En todo este proceso es importante la forma en que se realiza la **verificación de los resultados** de la votación. Los esquemas de votación clásicos analizados suponen que todos los agentes telemáticos del sistema operan honestamente, siendo por tanto relativamente sencillo manipular los resultados de la votación, sin que exista ningún método de detección. El sistema diseñado se ha concebido para permitir la verificación tanto a nivel global como a nivel individual.

La verificación global, puesta a disposición de los interventores, proporciona pruebas criptográficas robustas, que permiten demostrar sin ningún tipo de ambigüedad si el sistema ha operado de forma fraudulenta. La verificación individual es otro mecanismo, puesto a disposición de los votantes, que les permite durante un tiempo determinado y en unos lugares concretos, comprobar qué opción de voto se les ha contabilizado. La novedad respecto a otras soluciones radica en que en ningún momento el votante puede demostrar ante terceros no autorizados qué ha votado, lo que impide la compra de votos o la extorsión.

5.1 Verificación individual

La verificación individual podrá ser realizada por los votantes a través de los Puntos de Verificación, una vez finalizado el proceso de votación y durante un tiempo limitado. El votante que desee verificar su voto acudirá a uno de estos Puntos de Verificación y previa identificación se le permitirá acceder, de forma individual, a un sistema en el que introduciendo la tarjeta inteligente, podrá leer en una pantalla el voto que le ha sido contabilizado por el Contador, no entregándosele ninguna prueba de esta comprobación. Caso de que el votante crea que votó por una opción distinta a aquella que le ha sido mostrada podrá iniciar un proceso de reclamación, entregando su tarjeta inteligente a la Autoridad de Elección, la cual descubrirá y comparará todas las pruebas criptográficas presentes en el sistema para comprobar la validez del recuento. De esta manera se proporciona al votante herramientas que contrarresten la **crítica b)** del apartado 2.

5.2 Verificación global

Una vez publicados los resultados de la votación, y con la intención de que las distintas candidaturas obtengan una prueba del correcto funcionamiento del Contador a la hora de abrir y contar votos, se permite que cada una de ellas verifique el procedimiento. Cada candidatura tiene la posibilidad, mediante una serie de procedimientos concretos que se han diseñado, de comparar la información que posee con la que se ha obtenido como resultado final del proceso de recuento. Caso de que ambas informaciones no se correspondieran, podrían proceder a impugnar la votación, presentando para ello pruebas criptográficas robustas. Mediante estas pruebas criptográficas se introducen elementos de auditoría en el sistema que permiten garantizar la validez de todo el proceso, respondiendo así satisfactoriamente a la **crítica d)** del apartado 2.

El sistema diseñado garantiza también que el voto emitido **no podrá ser conocido en el futuro**. Los esquemas de votación clásicos analizados se basan en la presentación del voto debidamente ocultado al Administrador (y Sistemas de Intervención, si los hubiera) del sistema de votación para que verifique que el votante tiene derecho a votar y que no lo ha hecho todavía. El hecho de presentar a los interventores de las candidaturas el voto oculto mediante algoritmos criptográficos garantiza que en la actualidad éstos no puedan conocer su contenido, pero no garantiza que con el avance de las técnicas de criptoanálisis éste no pueda ser conocido en el futuro. El sistema desarrollado en el proyecto VOTESCRIPT aporta como novedad que en la fase de autenticación del votante no se presenta al Administrador o a los Sistemas de Intervención el voto sino la clave que se va a utilizar después para descifrarlo, evitándose que el Administrador lo pueda almacenar para el futuro (el voto únicamente se envía a la urna). Con todo ello se elimina el riesgo mencionado en la **crítica e)** del apartado 2.

6. Conclusiones

Para el diseño del sistema se ha partido de un análisis crítico y exhaustivo de las experiencias y propuestas que habían sido formuladas con anterioridad y se ha optado por una metodología multidisciplinar (tecnológica, sociopolítica y jurídica) tanto para la determinación de los requisitos y condicionantes como para la evaluación del sistema final que se plantea.

Es importante destacar que la fortaleza del sistema se basa en la obtención, por parte de los distintos actores del sistema (entre los que principalmente se encuentran los votantes y los interventores), de piezas de información criptográficamente robustas y seguras que podrán presentar como prueba ante terceros en caso de litigio o disconformidad con los resultados del proceso.

En los apartados precedentes se ha expuesto un resumen de los trabajos desarrollados dentro del proyecto VOTESCRIPT. En la actualidad, y cómo consecuencia de una colaboración con la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, se ha desarrollado un prototipo que se ha utilizado con éxito en una experiencia práctica llevada a cabo el día 16 de marzo pasado en el pueblo abulense de El Hoyo de Pinares y que ha tenido amplia repercusión tanto en la prensa escrita como en televisión y radio por tratarse de la primera experiencia institucional en España de voto electrónico por Internet [7] [8].

Referencias

[1] Mercuri R. *Testimony presented to the U.S. House of Representatives Committee on Science*, Mayo 2001. http://www.house.gov/science/full/may22/mercuri.htm

[2] Fujioka, T. Okamoto, K. Otha. *A Practical Secret Voting Scheme for Large Scale Elections*, Advances in Cryptology, AUSCRYPT´92, Lecture Notes in Computer Science 718. Springer-Verlang, Berlin, pp.244-251 (1993).

[3] Cranor, Lorrie F. y Cytron, Ronald K. *Design and Implementation of a Practical Security-Conscious Electronic Polling System*, WUCS-96-02, Departamento de Informática, Universidad de Washington, St. Louis, Enero 1996.

[4] Herschberg, Mark A. *Secure Electronic Voting Over the World Wide Web*, Tesis doctoral en Ingeniería Eléctrica e Informática, Massachusetts Institute of Technology, 1997.

[5] M.Ohkubo, F. Miura, M. Abe, A. Fujioka, T. Okamoto. *An Improvement on a Practical Secret Voting Scheme*. Lecture Notes in Computer Science 1729, Springer-Verlag, Berlin, pp. 225-234 (1999).

[6] Riera i Jorba, Andreu. *Design of Implementable Solutions for Large Scale Implementable Voting Schemes*, Tesis doctoral Universidad Autónoma de Barcelona, 1999.

[7] http://www.cert.fnmt.es opción Hemeroteca.

[8] Votación en Hoyo de Pinares http://vototelematico.diatel.upm.es