Del voto electrónico al telemático: El proyecto VOTESCRIPT

From Electronic to Telematic Vote: The VOTESCRIPT Project

A. Gómez, J. Moreno y E. Pérez

Resumen

Este artículo presenta los aspectos más relevantes del trabajo realizado por los autores dentro del proyecto VOTESCRIPT (TIC2000-1630-C02). El objetivo principal de este proyecto fue el análisis, definición e implementación de un sistema que abarcara todas las fases y elementos existentes en un proceso de votación electrónica sobre redes de ordenadores. El artículo incluye las soluciones propuestas dentro del proyecto.

Palabras clave: Voto electrónico, voto telemático, privacidad, protección de datos personales.

Summary

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. The paper includes the proposed solutions of the project to solve these problems.

Keywords: Electronic vote, Telematic vote, privacy, personal data protection.

El objetivo principal del proyecto VOTESCRIPT fue el análisis, definición e implementación de un sistema que abarcara todas las fases y elementos existentes en un proceso de votación electrónica sobre redes de ordenadores

1.- Introducción

Existe un uso generalizado del término *voto electrónico* para referirse a cualquier sistema novedoso de votación que automatice alguno de los procesos implícitos en un proceso electoral: autenticación de los votantes, emisión y recuento de los votos, y publicación de los resultados. Dentro de estos sistemas novedosos hay que distinguir aquellos que hacen uso de las redes telemáticas para comunicar a los votantes con una Mesa Electoral remota. Estos sistemas, también denominados de voto a través de Internet o *voto telemático*, permitirán votar desde casa o desde cualquier punto destinado al efecto, sin necesidad de estar ligado a un determinado Colegio Electoral.

El voto telemático plantea grandes 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, ya que el sistema diseñado debe gozar de la misma confianza que la votación tradicional.

Existen escasas experiencias de votación con validez oficial que hayan empleado el voto telemático, destacando que en la mayoría de ellas no se han reproducido 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, auspiciado por el ministerio español de Ciencia y Tecnología (TIC2000-1630-C02), finalizado oficialmente en diciembre de 2002, 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 telemática, abarcando desde el proceso de emisión del voto hasta el de recuento y posterior verificación de los resultados.

Para llevar a cabo el diseño global de la arquitectura del sistema, se ha trabajado en dos ámbitos distintos y complementarios: la seguridad de todo el sistema de votación y la eliminación de las barreras culturales (y los temores políticos) que dificultasen la aceptación del mismo por los

Pocos esquemas abordan la nueva problemática inherente a la votación a través de las redes telemáticas como la necesidad de potentes herramientas de verificación

ciudadanos, de manera que, al mismo tiempo que se realizaban los trabajos de ingeniería correspondientes, se han efectuado los análisis sociológicos, politológicos y jurídicos necesarios para determinar la viabilidad del sistema que se desarrollaba.

Este artículo describe, de forma somera, las principales características del sistema desarrollado y su comportamiento global.

2.- Algunos requisitos de los sistemas de votación

Hasta la fecha existen numerosas propuestas o *esquemas de votación* que definen los agentes, procedimientos y protocolos de seguridad necesarios para llevar a cabo el proceso de votación. En la mayoría de estos esquemas, la determinación de los requisitos de seguridad que debe reunir el sistema de votación se ha realizado reproduciendo las garantías proporcionadas por el voto tradicional, por lo que fundamentalmente se han centrado en garantizar el anonimato del votante, en evitar la votación por parte de votantes no autorizados o que ya lo hayan hecho y en el recuento correcto de los votos. Sin embargo, pocos esquemas abordan la nueva problemática que lleva inherente la votación a través de las redes telemáticas como son la necesidad de potentes herramientas de verificación para garantizar la corrección de los resultados ante posibles confabulaciones entre los agentes del sistema o la existencia de interventores, que a la manera tradicional, supervisen el correcto desarrollo de todo el proceso de votación.

En el proyecto VOTESCRIPT hemos tenido en cuenta ambos tipos de requisitos.

3.- Descripción del sistema VOTESCRIPT

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 miembros de la elección.

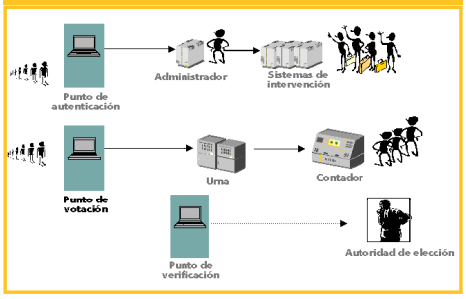
La tarjeta inteligente, diseñada especialmente para este proyecto, es capaz tanto de generar claves como de realizar gran parte de los procesos criptográficos necesarios para la seguridad del sistema. Implementa diversos algoritmos adicionales, además de los ya habituales en las tarjetas criptográficas.

3.1.- Arquitectura del sistema

El escenario se compone de un conjunto de sistemas automáticos (agentes telemáticos) tales como:

- Cabinas o Puntos de Autenticación a los que acude el votante a identificarse.
- Cabinas o Puntos de Votación, donde el votante emite el voto.
- Un Administrador de autenticación que identifica y autentica al votante.
- Un Sistema de Intervención de autenticación por cada una de las distintas candidaturas que se determine deban participar supervisando la fase de votación.
- Una Urna (que se mantiene cerrada todo el tiempo que se esté recibiendo votos).
- Un Contador que contabilizará los votos una vez finalizado el período de recepción de los mismos y publicará los resultados.
- Puntos de Verificación a los que puede acudir el votante a verificar el tratamiento dado a su voto.

ARQUITECTURA DEL SISTEMA



El sistema contempla, además, la existencia de personas que intervienen de forma directa en el proceso de votación y recuento:

- Votante dotado de una Tarjeta de Votación.
- Autoridad de Elección: máximo responsable del buen funcionamiento de todo el sistema.
- Interventores responsables de cada uno de los Sistemas de Intervención.

En una primera fase, el votante interactúa, con el Administrador y éste con los Sistemas de Intervención para comprobar la identidad del votante y proceder a su autenticación ante el sistema

3.2.- Proceso genérico

A continuación, se resumen los pasos más relevantes del proceso propuesto para llevar a cabo una votación telemática. No se hace una descripción detallada de los protocolos criptográficos y mecanismos de seguridad implementados en cada paso ya que requeriría una explicación más extensa:

- En una primera fase de identificación, el votante interactúa, por medio del Punto de Autenticación, con el Administrador y éste con los Sistemas de Intervención para comprobar la identidad del votante y proceder a su autenticación ante el sistema (comprobar que está autorizado para votar).

  Cabe resaltar que el software de este Punto de Autenticación no posee ningún tipo de capacidad criptográfica y que todas las que se necesitan, tanto en esta fase como en el resto (generación de claves, cifrado y descifrado de datos, firmas y comprobación de firmas,...), las realiza la tarjeta inteligente.

- La segunda fase sería la votación propiamente dicha en la que el votante envía desde la cabina de votación, con todas las garantías de seguridad necesarias, el voto a la Urna, donde se almacena hasta el final del proceso de votación. En esta fase, la Urna devuelve una pieza criptográfica (*comprobante*), que se almacena en la tarjeta del votante y que servirá para que la Autoridad de Elección pueda resolver futuras reclamaciones.

- Una vez terminado el periodo previsto para votar, se inicia la fase de recuento y publicación de los resultados por parte del proceso Contador. Las listas que se publican incluyen las piezas criptográficas necesarias para la verificación del correcto funcionamiento del proceso.

- Con posterioridad a la publicación de los resultados, tanto los votantes como los sistemas de intervención podrán hacer una verificación de la corrección del proceso; es lo que llamaríamos la fase de verificación. Si como consecuencia de esta verificación se produce alguna reclamación, la Autoridad de Elección podrá, con las pruebas criptográficas almacenadas en el sistema y en la tarjeta del votante, comprobar dónde se ha producido el posible fraude.

4.- Aportaciones del proyecto

Entre las medidas novedosas incorporadas en VOTESCRIPT con respecto a otros esquemas de votación, podemos resaltar las siguientes:

Estos sistemas de intervención que forman parte del sistema global serán proporcionados por la Administración Pública, no serán elementos propiedad de las candidaturas

- La existencia de los Sistemas de Intervención para las candidaturas. Cada uno 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. Asimismo, se prevé que sus programas puedan ser auditados por peritos de confianza de las candidaturas antes del proceso de votación.

- La existencia de 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. Están diseñados para reducir al máximo la posibilidad de coacción o de compraventa de votos.

- La existencia de la 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 o los Sistemas de Intervención. En el caso de que se produzca una reclamación por parte de un votante sobre el tratamiento dado a su voto, ésta reunirá 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 tarjeta inteligente será especialmente diseñada para el proyecto y que realiza todas las funciones criptográficas necesarias, dotando al sistema de mayor seguridad.

5.- Pruebas de campo

En cuanto a las pruebas con escenarios reales realizadas, ha existido una colaboración con la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda que ha permitido que parte de las soluciones aquí propuestas hayan sido trasladadas al sistema de votación desarrollado por la Casa de la Moneda. El pasado mes de marzo se realizó una experiencia piloto en Hoyo de Pinares (Ávila), con amplia repercusión en los medios de comunicación al tratarse de la primera experiencia institucional en España de voto telemático.

Este trabajo ha sido parcialmente financiado por el proyecto MCyT TIC2000-1630-C02.

Ana Gómez Oliva, Jesús Moreno Blázquez
(agomez@diatel.upm.es), (jmoreno@diatel.upm.es)
Emilia Pérez Belleboni
(belleboni@diatel.upm.es)
Dpto. de Ingeniería y Arquitecturas Telemáticas - UPM