

Sistema VOTESCRIPT: Una propuesta innovadora desarrollada para resolver los problemas clásicos de la votación electrónica

Justo Carracedo Gallardo¹, Ana Gómez Oliva¹ y Jose-David Carracedo Verde²

¹Dpto. de Ingeniería y Arquitecturas Telemáticas de la Universidad Politécnica de Madrid.
Ctra. Valencia Km.7. 28031 Madrid. España
{carracedo, [agomez](mailto:agomez@diatel.upm.es)}@diatel.upm.es

²Dpto. de Ciencia Política y de la Administración III. Observatorio para la Democracia Digital y los Derechos de Ciudadanía en Internet. Universidad Complutense de Madrid.
Campus de Somosaguas. 28223 Madrid. España
jdcarracedo@proyectos.diatel.upm.es

Resumen. En este artículo se presenta la descripción global de un sistema de voto telemático basado en criptografía avanzada y en el empleo de tarjetas inteligentes (proyecto VOTESCRIPT), destacando las aportaciones de este nuevo sistema sobre propuestas anteriores. Para enmarcar el trabajo desarrollado se presenta una panorámica general de la votación electrónica y se señalan los condicionantes que estas experiencias comportan. Asimismo, se resumen otras versiones particulares de VOTESCRIPT (proyecto VERA) y se comentan las características de una prueba experimental llevada a cabo para evaluar la viabilidad de la propuesta.

1 Introducción

Desde que a mediados de los 60 comenzaron las primeras experiencias de votación empleando ordenadores, hasta la actualidad en que se emplean urnas electrónicas o se ensaya la votación por Internet, los medios de comunicación han recogido multitud de experiencias de votación en todo el mundo bajo el epígrafe común de *voto electrónico*. Sin embargo, se trata de sistemas de votación muy dispares, en los que encontramos que las garantías de seguridad requeridas en los procedimientos de autenticación, emisión del voto y recuento son proporcionadas de muy diversas formas.

Así, por ejemplo, en algunos sistemas existe personal especializado encargado de realizar el procedimiento de autenticación del votante, mientras que en otros éste se realiza de forma automática. En unos sistemas la emisión del voto se realiza empleando papeleta, con recuento automático y posibilidad de participación de interventores, mientras que en otros la votación se realiza a partir de un panel seleccionando una opción y sin posibilidad de verificación posterior de los resultados. Posteriormente han ido apareciendo otras propuestas basadas en el empleo de criptografía y redes telemáticas.

2 J. Carracedo Gallardo, A. Gómez Oliva, D. Carracedo Verde

Con objeto de analizar debidamente cada experiencia de votación, es conveniente, en primer lugar, establecer una clasificación de los escenarios de votación, de manera que una vez encuadrado un sistema en uno de estos escenarios, los riesgos y amenazas a la seguridad sean conocidos y, por tanto, puedan ser debidamente neutralizados. En [1] se propone una clasificación de los sistemas de votación en varios niveles de complejidad. A partir de ella, podemos distinguir dos grandes grupos relevantes para nuestro trabajo:

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

Desde hace varios años, la casi totalidad de las acciones gubernamentales encaminadas a la automatización de los procesos de votación se encuadran en las actuaciones del primer grupo, 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 la falta de garantías de verificación que ofrece).

En el segundo grupo, voto a través de redes telemáticas, que nosotros hemos dado en llamar **voto telemático**, se han realizado escasas experiencias con validez oficial, destacando que en la mayoría de ellas no se reproducen las mínimas garantías de seguridad que se proporcionan con el sistema de voto tradicional, como son el anonimato, la posibilidad de que existan interventores para supervisar el proceso o que, en caso de discrepancia, exista la posibilidad de verificar los resultados.

Este grupo de sistemas de votación es el más atractivo, desde un punto de vista tecnológico, debido a los retos técnicos y de seguridad que debe resolver. No obstante, desde un punto de vista sociológico, plantea serios interrogantes, ya que parece que la causa primordial de que estos sistemas de votación electrónica no estén siendo utilizados masivamente radica en el cambio cultural que el nuevo sistema supondrá para los ciudadanos. En efecto, no sólo deberán desarrollar nuevas habilidades para poder utilizar el sistema, sino que habrán de confiar en sistemas informáticos, cuya tecnología conocen vagamente, pero de los que sospechan (no sin razón) que son mucho más susceptibles a la manipulación que los sistemas tradicionales de votación. Los sistemas de voto electrónico que aspiren a sustituir algún día el sistema de voto tradicional deberán incorporar las bondades de estos, a la vez que deberán ofrecer nuevas facilidades que permitan contrarrestar la natural desconfianza de los votantes hacia el proceso de votación electrónica.

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 (de los que son una muestra [2] [3] [4] y [5]), 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.

El proyecto VOTESCRIPT¹ ha abordado la problemática de los sistemas de votación de este segundo grupo, 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 del recuento.

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 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 [6].

Con esta perspectiva metodológica, el desarrollo del proyecto se ha abordado mediante un equipo multidisciplinar, compuesto por investigadores pertenecientes tanto al campo de la ingeniería telemática como al campo sociopolítico: uno de ellos con sede en el Departamento de Ingeniería y Arquitecturas Telemáticas, DIATEL (Universidad Politécnica de Madrid) y el otro en el Departamento de Ciencia Política y de la Administración III (Universidad Complutense de Madrid).

2 Escenario de comunicación

En una primera aproximación, el sistema VOTESCRIPT pretende dar soporte a votaciones telemáticas realizadas en un entorno en el cual todos los votos se recogen en una sola urna, aunque se ha contemplado su adaptación a entornos en los que sea necesario la presencia de múltiples urnas. Este diseño pretende plasmar telemáticamente ciertas garantías del sistema convencional de control descentralizado basado en la existencia de varias mesas con sus respectivos conjuntos de interventores.

2.1. Agentes y sistemas automáticos

En el escenario de comunicación contemplado en VOTESCRIPT intervienen un conjunto de sistemas automáticos que funcionan bajo unos programas que habrán sido previamente publicados, con la consiguiente posibilidad de evaluación y auditoría por parte de todas las entidades implicadas en el proceso de votación. En la Fig. 1 se representa este conjunto de sistemas. Esto son:

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)

4 J. Carracedo Gallardo, A. Gómez Oliva, D. Carracedo Verde

- o Puntos de Autenticación, PAs. Se trata de un tipo de cabinas, dotadas de lector de tarjetas pero sin capacidades criptográficas en las que el Votante inicia el proceso de votación.
- o Puntos de Votación, PVs. Al igual que los PAs no tienen capacidad criptográfica. Se trata de cabinas dotadas de lector de tarjetas que ayudan al Votante a determinar cuál es el voto que desea emitir. En VOTESCRIPT el Votante puede elegir para autenticarse cualquiera de los PAs existentes y podrá emitir el voto en cualquiera de los PVs existentes.
- o Un Administrador de autenticación (que se podría considerar como *oficial*).
- o Varios Sistemas de Intervención (SIs) que complementan la labor del Administrador. Cada uno de ellos está controlado por un Interventor nombrado por cada una de las agrupaciones de electores o candidaturas autorizadas para supervisar la votación.
- o Una Urna que va recogiendo los votos y devuelve comprobantes de votación.
- o Un Contador que realizará el recuento de los votos una vez finalizado el período de recepción de los mismos.
- o Puntos de Verificación que permiten al votante comprobar que su voto ha sido tenido en cuenta y ha sido correctamente contabilizado.

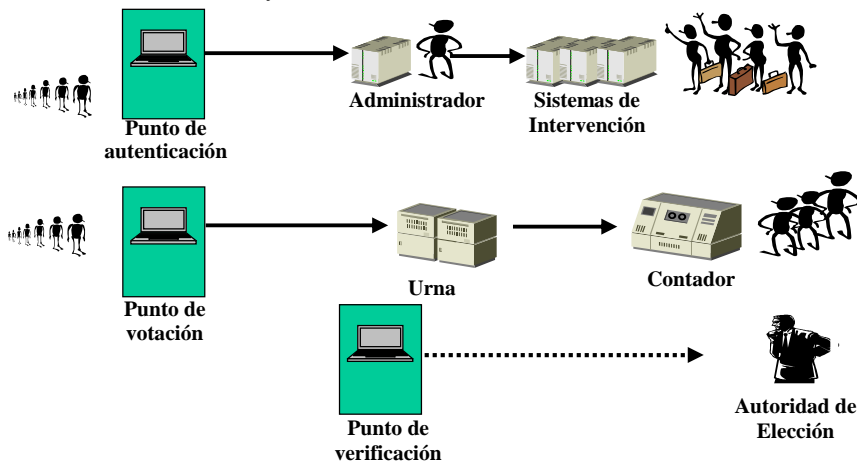


Fig. 1. Arquitectura del Sistema VOTESCRIPT

2.2. Personas que participan en el proceso

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

- o Votantes. Cada Votante está en posesión de una Tarjeta inteligente de Votación, TV. Se trata de una tarjeta inteligente especialmente diseñada para VOTESCRIPT que permite llevar a cabo múltiples operaciones criptográficas.

- o Un Gestor del sistema Administrador.
- o Interventores responsables de cada uno de los Sistemas de Intervención.
- o Autoridad de Elección. Es la persona encargada del control general del sistema y de resolver posibles reclamaciones.

El Administrador y los Sistemas de Intervención junto con el Gestor del sistema Administrador y los Interventores constituyen la plasmación en este sistema telemático de la mesa electoral convencional. Una vez finalizado el proceso de recepción de votos, se procederá a la apertura de la Urna con el fin de llevar a cabo el recuento y se publicarán las listas con los resultados oficiales e información adicional que posibilite la verificación fiable de los resultados.

2.3. Claves e identificadores

Como paso previo al comienzo de la votación, se habrá hecho llegar a cada uno de los votantes una Tarjeta de Votación y un identificador de votante (almacenado dentro de la tarjeta) que deberá ser conocido por todos los miembros que participan en el control de la elección. Todas las personas que deseen ejercer su derecho a votar, acudirán a los sitios especialmente habilitados para la votación (PAs y PVs) provistas de la Tarjeta Inteligente que les permite identificarse y posibilitar la comunicación con los agentes del sistema VOTESCRIPT.

El Administrador, los Sistemas de Intervención, la Urna, el Contador y la Autoridad de Elección poseen un par de claves (pública y privada). Las claves públicas de todos ellos, mediante los correspondientes certificados, son conocidas por todos los agentes telemáticos y todas las personas participantes en el sistema de votación a través de su tarjeta inteligente.

También, todos y cada uno de los votantes poseen un par de claves (pública y privada) almacenadas en su tarjeta. La clave pública (mediante su certificado) es conocida por todos los agentes telemáticos del sistema y por la Autoridad de Elección.

En los trabajos para el desarrollo del proyecto VOTESCRIPT, principalmente con motivo de la implantación piloto del sistema VERA (descrita en el apartado 5), se llevó a cabo todo un estudio del proceso previo de inicialización de tarjetas inteligentes y asignación de claves e identificadores:

- o Asignación de un identificador de votante a cada una de las personas participantes en el proceso. Este identificador se genera en relación con el número de DNI que aparece en el censo oficial de votación.
- o Asignación de un par de claves públicas y privadas a todas las personas y agentes telemáticos participantes, admitiendo la posibilidad de que los votantes puedan cambiar con posterioridad su par de claves y comunicar este cambio a la Autoridad de Elección.
- o Generación de certificados de todas las claves públicas presentes en el proceso. Para ello, existe una Autoridad de Certificación específica que se encargará de generar los certificados que serán utilizados para garantizar la validez de las claves públicas que intervienen en el proceso. Todo ello, constituye una infraestructura de clave pública (PKI) bajo la cual operan los distintos protocolos seguros que gobiernan el sistema.

6 J. Carracedo Gallardo, A. Gómez Oliva, D. Carracedo Verde

- o Inicialización de las tarjetas inteligentes tanto de votantes como de los agentes automáticos incluyendo los identificadores y las claves a los que se ha hecho referencia en los párrafos anteriores.
- o Distribución de tarjetas a los votantes y gestores de los sistemas automáticos en base a un proceso público, previamente definido, supervisado por la Autoridad de Elección.

Por cuestiones de espacio y oportunidad, los procedimientos recogidos en los puntos anteriores no se desarrollan en la presente ponencia, dedicada prioritariamente a explicar, de forma genérica, el comportamiento del sistema y su relación con otros sistemas de votación existentes. Asimismo, dentro de los trabajos en curso del grupo de investigación al que pertenecen los autores de la presente ponencia, se está llevando a cabo un estudio acerca de la posible correspondencia de la PKI bajo la que opera VOTESCRIPT con otras PKIs que en su momento puedan ser implantadas dentro de la Administración Pública para posibilitar la relación ciudadano-Administración y otros procesos de toma de decisiones (Democracia Digital).

3 Comportamiento global del sistema

3.1 Procedimiento de entrega del voto (descripción global)

Relación Votante-Punto de Autenticación

- 1) En el Punto de Autenticación, el Votante introduce su Tarjeta de Votante (TV) en el lector de tarjetas. El Punto de Autenticación reconoce la validez de la tarjeta mediante un identificador genérico que poseen todas las tarjetas participantes en la votación. Por tanto, cualquier tarjeta de otro tipo que se pretenda introducir en el lector será rechazada. El Votante se autentica ante su tarjeta mediante un PIN o un mecanismo de identificación biométrico².
- 2) La Tarjeta de Votante contiene el par de claves (pública y privada) del Votante. Además, en la TV se genera el par de claves asimétricas de votación (k_{dV} , k_{cV}), que se almacenan de forma que ni el propio Votante pueda leerlas. La propia tarjeta genera además un factor de opacidad de tal manera que la clave k_{dV} previamente generada se opaca (usando dicho factor de opacidad) para el Administrador y para cada uno de los Sistemas de Intervención, dando lugar a una clave k_{dV} opacada para cada una de las entidades destino del mensaje. Mediante un proceso de diálogo, la tarjeta entrega al Punto de Autenticación las distintas claves opacadas firmadas cada una de ellas con la clave privada del

² Dentro de esta propuesta la presencia de mecanismos de identificación biométricos se plantea desde un compromiso intelectual y ético que busca explorar y beneficiarse de las ventajas que su uso proporciona, manteniendo muy presente la garantía de los Derechos Humanos y la obligación de **minimizar los problemas de privacidad e intimidad** que su introducción masiva podría llegar a generar. En el marco de nuestra propuesta es la Tarjeta Inteligente la que almacena los datos biométricos, utilizando el Punto de Autenticación como simple intermediario. Este tipo de datos no viaja por la red, ni se encuentra almacenado en el PV en forma alguna, imposibilitando la formación de listas “biométricas”.

Votante, con indicación del destinatario de cada una de ellas. Además, le entrega el identificador de votante firmado con la clave privada del Votante. La tarjeta cifra todos estos datos con la clave pública del Administrador para que solo éste pueda leerlos.

- 3) Con los datos referidos en el paso anterior, el Punto de Autenticación genera una APDU (unidad de datos del protocolo de aplicación) y la envía al Administrador.
- 4) El Administrador lee y descifra la APDU y luego envía todos los datos (ver paso 2) **a todos** los Sistemas de Intervención. Cada uno de los Sistemas de Intervención, al igual que el Administrador, deberá comprobar si el identificador de votante recibido es correcto³. Es decir, comprueba que el identificador está dentro de la lista de identificadores válidos, que la firma del Votante que realiza la solicitud es correcta y que no se ha recibido (y por tanto firmado ya) una clave opacada asociada a dicho identificador (es decir, que esa tarjeta no ha realizado previamente la autenticación). En caso contrario se rechaza lo recibido⁴.
- 5) Una vez comprobado que el identificador de votante recibido es válido, los Sistemas de Intervención se encargarán de ir firmando **de forma ciega** la clave k_{dV} opacada **que les corresponda**, y devolverán el resultado al Administrador. El Administrador hace otro tanto con la clave k_{dV} opacada que le corresponde y la adjunta a las claves opacadas firmadas recibidas de los SI, formando así un “paquete de claves”.
- 6) Este “paquete de claves” es firmado por el Administrador con su clave privada y cifrado con la clave pública del Votante, tras lo cual es enviado (mediante una APDU) al Punto de Autenticación. De esta forma tan solo la TV podrá leer el “paquete de claves” (confidencialidad de los datos) y además tiene la garantía de que fue el Administrador quien le devolvió el conjunto de claves firmadas que, según se explica más adelante, le servirán como “permiso” para poder votar.
- 7) El Punto de Autenticación entrega a la Tarjeta del Votante los datos contenidos en la APDU que ha recibido del Administrador, de tal manera que ésta elimina los cifrados que los protegen (haciendo uso primero de la clave privada del Votante y después de la clave pública del Administrador). Una vez leído el “paquete de claves” opacadas y firmadas a ciegas (paso 5), va eliminando, una por una, el factor de opacidad, obteniendo la k_{dV} firmada por el Administrador, la k_{dV} firmada por el Sistema de Intervención 1, la k_{dV} firmada por el Sistema de Intervención 2 y así sucesivamente. A continuación verifica que las firmas del Administrador y de los distintos Sistemas de Intervención son correctas. Si es así, ha finalizado la interacción del Votante con el Punto de Autenticación, quedándose la Tarjeta de Votante con las firmas de su k_{dV} que posteriormente le servirán como aval durante el proceso de votación.

³ El hecho de que el Administrador compruebe en paralelo con los Sistemas de Intervención que la solicitud realizada es correcta permite que, en caso de producirse una incidencia, todos tengan constancia de ella (al igual que ocurre en la votación convencional por papeleta (conforme al procedimiento aplicado en el Estado Español)). Cabe señalar que la función fundamental de los SI es supervisar la actuación del Administrador para evitar manipulaciones.

⁴ En la presente descripción global no se aborda la actuación del sistema ante incidencias y eventuales problemas en la comunicación PV-Administrador.

Relación Votante-Punto de Votación

- 8) En el Punto de Votación, el Votante introduce su Tarjeta Inteligente en el lector de tarjetas y se autentica ante la Tarjeta mediante un PIN o un mecanismo de autenticación biométrica. El Punto de Votación al igual que el PA es una máquina telemática sin capacidades criptográficas.
- 9) El Punto de Votación solicita al Votante su voto mediante un diálogo interactivo en el que a través de texto e imágenes se facilita al Votante la elección de la opción deseada. En la Tarjeta de Votante se cifra con k_{cV} (*clave de cifrado de voto*) el voto a entregar. (Ello implica que el voto solo podrá ser descifrado usando la clave k_{dV} (*clave de descifrado de voto*) pareja de la anterior).

Mediante un proceso de diálogo entre el PV y la Tarjeta, ésta crea una pieza de información con: el voto cifrado, la clave k_{dV} y la clave k_{dV} firmada por el Administrador y los Sistemas de Intervención. A continuación se “guarda” esta pieza de información en un *Sobre Seguro C* entre la TV y el Contador que solo este último puede abrir⁵. Tras esto, en la Tarjeta del Votante se genera una *clave simétrica* que se junta con el *Sobre Seguro C* y se “guarda” en un nuevo *Sobre Seguro U* que solo la Urna puede abrir. A continuación la Tarjeta le entrega al Punto de Votación este *Sobre Seguro U* para su posterior envío a la Urna.
- 10) Con el *Sobre Seguro U* referido en el paso anterior, el Punto de Votación genera una APDU y la envía a la Urna. Debido a que esos datos están cifrados con la clave pública de la Urna, solo ésta pueda leerlos.
- 11) La Urna tras eliminar el *Sobre Seguro U* que protege lo recibido (y que solo la Urna es capaz de “abrir”), obtiene la *clave simétrica* y la pieza de información que constituye el *Sobre Seguro C* (que solo el Contador puede “abrir” y que contiene el voto cifrado, la clave k_{dV} y la clave k_{dV} firmada por el Administrador y los Sistemas de Intervención). La Urna almacena estos “sobres” seguros C hasta el final del periodo de votación.

Además, la Urna, a partir de los datos protegidos con el *Sobre Seguro C* que recibió en el paso anterior, devuelve al Punto de Votación un comprobante de la votación realizada, preservando el anonimato del Votante. Para generar *el comprobante* realiza las siguientes operaciones: a) la Urna cifra el *Sobre Seguro C* con la clave pública de la Autoridad de Elección y b) la Urna firma lo anterior con su clave privada. A continuación la Urna cifra el comprobante con la clave simétrica que recibió del Punto de Votación. Una vez hechas las tres operaciones envía lo resultante al Punto de Votación.
- 12) El Punto de Votación entrega lo recibido a la Tarjeta de Votación que elimina el cifrado con la clave simétrica, obteniendo *el comprobante*. Después verifica la corrección de la firma por parte de la Urna (si bien no puede conocer su contenido al estar cifrado con la clave pública de la Autoridad de Elección). El comprobante de voto es guardado en la Tarjeta del Votante y sólo la Autoridad de Elección podrá acceder a los datos de ese comprobante en caso de reclamación

⁵ El mecanismo utilizado para este *sobre seguro* se corresponde con el que se denomina habitualmente como *canal seguro* que ofrece mayores protecciones de seguridad que el *sobre* o *envoltura digital* convencional (*digital envelope*). Para la configuración de este *sobre seguro* se emplea una clave simétrica de sesión, una cadena aleatoria, algoritmos *hash* y el cifrado con la clave pública del receptor.

(según estipulen las reglas que se dicten), una vez haya finalizado el proceso de votación.

El Punto de Votación informa al Votante de que ha terminado el proceso de entrega de su voto. Una Tarjeta de Votante que haya completado el proceso anterior y haya almacenado su comprobante, rechazará realizar de nuevo el proceso de entrega de voto, aunque su Votante propietario lo intente (la tarjeta es resistente ante manipulaciones), lo que garantiza que cada votante vota solo una vez.

3.2 Apertura de la Urna y recuento de los votos

Todos los votos permanecen en la Urna hasta el final del periodo de recepción de votos. Solo el contador puede abrir (leer) esos votos por estar protegidos en *Sobres Seguros C*.

- 1) Para proceder a la apertura de la Urna se necesitará la presencia física del Gestor del Sistema Administrador y de una cantidad suficiente de Interventores (según estipulen las reglas que se dicten), que introducirán sus respectivas tarjetas inteligentes en los lectores habilitados para ello y ante las cuales se autenticarán de forma biométrica o mediante un PIN. El proceso de apertura consiste en que la Urna aleatoriza todo lo que ha ido recibiendo (modifica el orden de aparición de los registros) y lo envía al Contador, publicando a su vez una lista con lo enviado (aquí están los votos cifrados dentro de *Sobres Seguros C*). En ese momento, se borra toda la información que ha ido adquiriendo la Urna durante su funcionamiento. El proceso mediante el cual se produce el borrado será auditable por parte de aquellas personas o entidades que políticamente se determine tengan autorización para ello.
- 2) A continuación se procede al recuento de los votos. Antes de iniciar la lectura de los resultados, nuevamente el Gestor del Sistema Administrador y los Interventores, con sus tarjetas inteligentes (mediante un procedimiento de secreto compartido) proporcionarán de forma conjunta al Contador su clave privada (que ha permanecido guardada y oculta hasta este momento) necesaria para que el Contador entre en funcionamiento. El Contador, después de recibir toda la información procedente de la Urna “abre” los *Sobres Seguros C* que contienen la información sobre el voto descrita en el paso 9: voto cifrado con k_{cV} , la clave k_{dV} y la clave k_{dV} firmada por el Administrador y los Sistemas de Intervención. Para cada voto, verifica que la k_{dV} (que sirve para abrir el voto cifrado) esté correctamente firmada por el Administrador y los Sistemas de Intervención. A continuación el Contador descifra todos y cada uno de los votos. Por último realiza el recuento de los votos y publica el resultado.

La clave k_{dV} firmada por el Administrador y los SI constituye una garantía para el Contador de que nadie excepto un Votante autorizado puede entregarle un voto válido. Aunque la Tarjeta de Votante impide que el Votante pueda votar más de una vez, si esta protección fuese violada, el Contador detectaría y subsanaría esa incidencia.

Una vez realizado el recuento, el Contador hace públicos los resultados de la votación y genera una lista en la que para cada una de las entradas aparecen: a) el voto

en claro, b) la clave k_{dV} , c) la clave k_{dV} firmada por el Administrador y d) la clave k_{dV} firmada por cada uno de los n Sistemas de Intervención. Esta lista servirá para el *proceso de verificación*.

3.3 Verificación de los resultados de la votación

VOTESCRIPT permite dos tipos de verificación: la *verificación individual* por parte del Votante y la *verificación global* de los resultados por parte de las candidaturas o agrupaciones de electores autorizados para ello.

3.3.1 Verificación individual

Verificación a través de los Puntos de Verificación

Una vez haya finalizado la votación, cada Votante puede comprobar de forma independiente que su voto ha sido correctamente tenido en cuenta. Para ello basta con que el Votante se dirija a un Punto de Verificación y, siempre de forma individual, utilice su tarjeta y pida que se le muestre el voto asociado. El sistema ubicado en el Punto de Verificación está habilitado para leer la k_{dV} almacenada en la tarjeta del Votante, de manera que, una vez obtenida dicha clave de la tarjeta, accede vía telemática a la lista de parejas k_{dV} en claro-voto generada por el Contador y le muestra el voto asociado, de forma que el Votante y sólo éste pueda leerlo. En el caso de que el Votante no esté conforme con la opción visualizada, puede iniciar un proceso de reclamación ante la Autoridad de Elección.

Reclamación: verificación ante la Autoridad de Elección

En este tipo de verificación la Autoridad de Elección, tras recibir la tarjeta del Votante, puede demostrar sin ninguna ambigüedad un tratamiento correcto o incorrecto del voto, pues tiene acceso a:

- o La k_{dV} del Votante almacenada en su tarjeta.
- o El comprobante enviado por la Urna al Votante (firmado por la Urna y garantizada su inviolabilidad por la clave pública de la Autoridad de Elección) donde se contiene el voto emitido.
- o Los registros del Contador que relacionan la k_{dV} firmada por el Administrador y los Sistemas de Intervención, la k_{dV} en claro y el voto cifrado con k_{cV} .

Con todo ello la Autoridad de Elección, apoyándose en pruebas criptográficas robustas, dictaminará si el Votante no tiene razón o si ha existido una falsificación por parte del sistema.

3.3.2 Verificación global

Una vez finalizado el periodo de entrega de votos a la Urna y publicado el resultado, con la intención de que las distintos Interventores obtengan una prueba del correcto funcionamiento del Contador, se le entrega a cada uno de ellos una copia de las piezas de la información obtenidas por el Contador tras “abrir” los distintos *Sobres Seguros C* recibidos de la Urna.

Cada Interventor dispondrá de su propia máquina donde se cargará dicha copia. Esta máquina será previamente auditada por peritos de confianza del Sistema para conseguir total seguridad de que solamente podrá realizar el recuento de votos. Haciendo uso de esta copia y de la información recogida durante el proceso de Autenticación de votantes, cada uno de los Interventores podrá verificar si el procedimiento de recuento en el Contador se ha realizado o no de forma correcta, y si los resultados que ha obtenido en su recuento coinciden con los publicados.

Tanto para las listas de registros recibidos por el Contador como para las listas de información entregadas a cada candidatura se establecerá un periodo de validez de manera que, una vez transcurrido el tiempo estipulado y considerada válida la elección, deberán ser destruidas.

4 Aportaciones del proyecto VOTESCRIPT a los sistemas tradicionales de voto

En este apartado se destacan las principales aportaciones del proyecto VOTESCRIPT 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.

- o 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 sus diferentes fases en base a requisitos demandados por los ciudadanos y determinados por la investigación sociológica (en [1] se recoge un somero resumen de ellos). Cabe señalar que algunos de estos requisitos fueron en principio detectados más bien como procedimentales, pero a la luz de la investigación social, aparecen como garantes del sistema de votación al satisfacer demandas que surgen con fuerza en los trabajos de campo realizados. 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.
- o 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. El sistema diseñado se ha concebido para permitir la verificación tanto a nivel global como a nivel individual.
- o El sistema VOTESCRIPT proporciona un sistema de verificación individual que permite a cada votante comprobar en lugares precisos y durante un tiempo determinado si su voto se ha tenido en cuenta y ha sido correctamente contabilizado. La novedad respecto a otras soluciones radica en que el proceso de verificación es privado, de manera que en ningún momento el votante puede demostrar ante terceros no autorizados qué es lo que ha votado, lo que **impide la compra-venta de votos o la extorsión**. Esto representa una significativa mejora incluso con respecto a los sistemas de

votación convencionales, en los que, mediante opciones como el voto delegado o el voto por correo, se hace posible este tipo de agresiones masivas a la soberanía popular.

- o La existencia de los Sistemas de Intervención es una de las principales aportaciones de este sistema, puesto que permite el control de todo el proceso electoral por parte de las agrupaciones de ciudadanos o candidaturas autorizadas para ello. Además, se les dota de la posibilidad de realizar de forma sencilla una auditoría no sólo del resultado final sino de todo el proceso. 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 o no de forma fraudulenta.
- o Cada interventor tiene la posibilidad, mediante una serie de procedimientos concretos que se han diseñado, de comparar la información que posee su Sistema de Intervención 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.
- o En el desarrollo del proyecto VOTESCRIPT se decidió emplear tarjetas criptográficas específicamente diseñadas para este proyecto, que no sólo permitieran garantizar la identidad del votante sino que realizaran todas las funciones de cifrado/descifrado, generación de claves de sesión y comprobación de firmas dentro de la propia tarjeta, con objeto de impedir el acceso a información crítica por parte de usuarios maliciosos. Asimismo, la tarjeta almacena cierta información asociada al proceso de emisión del voto, *el comprobante*, con vistas a una posible verificación posterior. La tarjeta está diseñada para ser resistente a manipulaciones (*tamper-resistant*), de forma que nadie no autorizado pueda leer o modificar su contenido.
- o Para evitar el riesgo de que la ocultación del código fuente de los programas desarrollados impida la plena confianza de todos los participantes en el proceso de votación [9], un requisito para la implantación futura del proyecto VOTESCRIPT en votaciones públicas consiste en que el código de los programas desarrollados deba ser aprobado por la Administración después de un proceso de información pública, en el que los distintos agentes sociales puedan avalar (a través de peritos de su confianza) que los programas operan conforme al diseño convenido.
- o 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.
- o 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).

El sistema VOTESCRIPT viene a solucionar las principales críticas que se hacen a los sistemas de voto telemático y que fueron recogidas por Mercuri [7] en su intervención en la Cámara de Representantes del Comité de Ciencia de EEUU (mayo de 2002). Estas críticas 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.

Como se justifica a lo largo de la descripción anterior, el sistema propuesto resuelve la mayoría de estos puntos, por lo que representa una importante aportación a los sistemas de votación electrónica.

5 Desarrollo de un prototipo y pruebas en El Hoyo de Pinares

A finales de 2001 la Subdirección General de Política Interior y Procesos Electorales del Ministerio del Interior de España inició un proyecto conjunto con la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda con el objeto de estudiar la viabilidad de la implantación de un sistema de voto electrónico, alternativo al actual voto por correo, para los españoles residentes en el extranjero.

El grupo de investigación VOTESCRIPT vinculado desde sus orígenes al citado proyecto, desarrolló un modelo teórico de sistema de votación, denominado Sistema VERA (*Votación Electrónica para los Residentes Ausentes*). En base a este modelo, la FNMT-RCM ha desarrollado un sistema propio de votación, de cuyo prototipo se han realizado las pruebas de campo en El Hoyo de Pinares (Avila) en marzo de 2003.

El Sistema VERA se concibe a partir de los planteamientos desarrollados en el proyecto VOTESCRIPT, adaptándolos a las características propias de este entorno, por lo que de hecho supone una particularización de la propuesta original. No obstante, existen algunas diferencias entre ambas propuestas que se comentan a continuación:

- o En primer lugar, se determinó 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, además de las serias amenazas al sistema que pudieran derivarse de un ataque de denegación de servicio originado por *hackers*. Por tanto, se consideró que el sistema con más expectativas de éxito a corto plazo en este entorno era aquel en el que se empleasen Puntos de Votación que se comunicaran con una Urna Central mediante una red privada virtual (véase Fig. 2).

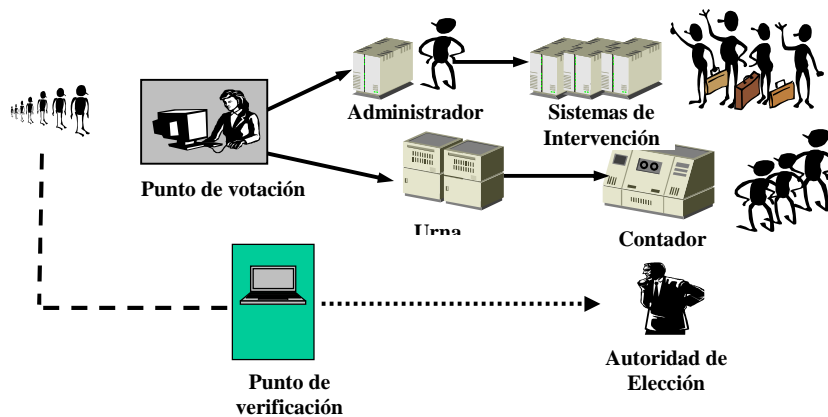


Fig. 2. Arquitectura del Sistema VERA

- o A diferencia de la propuesta VOTESCRIPT en la que los Puntos de Votación (y los de Autenticación) son máquinas con software específico, dedicadas en exclusiva al proceso de votación, los Puntos de Votación en el sistema VERA son computadores convencionales dotados de lectores de tarjetas inteligentes y con capacidad de acceso a través de Internet. Además, en VERA los Puntos de Votación actúan tanto como puntos de autenticación como puntos de emisión de votos. A través computadores, los votantes descargan un *applet* de votación que les irá guiando en los pasos a seguir y desde donde se controlará todo el diálogo seguro entre el votante, la tarjeta y los distintos agentes telemáticos (Administrador, Urna, Contador, etc.) que intervienen en el sistema. El hecho de que el votante deba descargarse un *applet* desde una dirección conocida y además pueda examinar su contenido hace más vulnerable al sistema frente a posibles ataques organizados de inundación que provoquen que los votantes se vean imposibilitados de ejercer su derecho al voto.
- o El sistema VERA se basa en el empleo de la tarjeta criptográfica CERES, desarrollada por la FNMT-RCM que contiene el certificado del usuario, junto con otros datos relativos a la votación particular. Se trata de una tarjeta criptográfica convencional con capacidades criptográficas limitadas, lo que obliga a que ciertas operaciones necesarias durante el proceso de emisión de voto deban ser realizadas desde el *applet* de votación, con el consiguiente riesgo

de que alguna persona con conocimientos suficientes pudiera utilizar de forma maliciosa la información allí recogida.

- o El sistema VERA mantiene el concepto de verificación individual a través del comprobante y los Puntos de Verificación tal y como se recogen en la propuesta VOTESCRIPT, así como el procedimiento de verificación global. Este último procedimiento ofrece a los interventores un número limitado de registros, elegidos aleatoriamente, con todos los datos relativos al proceso de votación para que puedan determinar sin ningún tipo de ambigüedad, si el proceso de votación y recuento ha sido correcto.

Para llevar a cabo la experiencia piloto se eligió el municipio de El Hoyo de Pinares (Ávila), población rural cercana a Madrid con un reducido número de habitantes (el censo electoral ascendía a 1786 personas). Por razones de tiempo y oportunidad, la FNMT-RCM implementó un subconjunto de las especificaciones del sistema VERA para la realización de esta experiencia piloto y modificó alguno de los comportamientos previamente definidos.

En concreto, los cambios más significativos entre el Sistema VERA y la implementación desarrollada por la FNMT-RCM fueron los siguientes:

- o No se generó el comprobante en la tarjeta del votante, por lo que se eliminó el procedimiento de verificación individual y, por tanto, no se implementaron los Puntos de Verificación.
- o Las operaciones criptográficas necesarias en todo el proceso de votación no se realizaron en la tarjeta criptográfica, sino desde el *applet* que los votantes se descargaban al conectarse al servidor predeterminado. La única funcionalidad de la tarjeta era la de servir como herramienta de autenticación del votante, a través del certificado contenido en ella.
- o Durante todo del proceso de votación se crearon pruebas criptográficas que permitirían determinar la corrección de todo del proceso (verificación global), sin embargo no se pusieron en marcha los procedimientos de acceso a esta información por parte de los interventores.

Si bien el tema de la consulta a los ciudadanos de El Hoyo de Pinares estuvo concebido como prueba piloto y se eligió un tema sin implicaciones políticas de fondo (qué día se quería celebrar la romería de la Virgen), tenía cierta trascendencia en el pueblo y se estableció que los resultados tenían carácter vinculante. El porcentaje de votantes ascendió al 58% de los electores que recogieron la tarjeta y la experiencia fue considerada un éxito tanto a nivel mediático como por los organizadores y por el conjunto de los que votaron. Aunque en la puesta en marcha de esta experiencia hubo serios defectos de forma y fondo (analizados en profundidad en el documento [8]), esta experiencia demuestra que desde una perspectiva estrictamente técnica es viable la puesta en marcha de un sistema de votación a través de redes telemáticas, mediante el empleo de cabinas de votación.

Sin embargo, esta puesta en práctica en El Hoyo de Pinares no tuvo en cuenta el nivel de formación en el uso de computadores de los participantes, la facilidad de uso de los interfaces o el hecho de que la presencia de asistentes en cada punto de votación (necesarios para superar las dificultades en el manejo del computador) vulneraba gravemente el secreto de voto. Estas circunstancias, no significativas en el análisis de viabilidad técnico, desde el punto de vista politológico son de gran importancia, pudiendo dar lugar incluso a invalidar experiencias que no tengan en

cuenta estos condicionantes sociales. Esto confirma la tesis de partida de VOTESCRIPT en cuanto a la necesidad de abordar la votación telemática desde equipos multidisciplinares, necesarios no solo en la fase de diseño o desarrollo sino también en la fases de implementación y puesta en práctica.

6 Conclusiones

Las soluciones técnicas que se adopten a la hora de diseñar un sistema de votación tienen un impacto social muy relevante en lo tocante al mantenimiento y mejora de los derechos y libertades de los ciudadanos y, consecuentemente, en el desarrollo de la democracia en la Sociedad de la Información.

El diseño de sistemas de Democracia Digital debe partir de un análisis crítico y exhaustivo de las experiencias y propuestas formuladas con anterioridad e incorporar metodologías multidisciplinares (tecnológica, sociopolítica y jurídica) tanto para la determinación de los requisitos y condicionantes como para la evaluación del sistema final que se desarrolle.

El sistema VOTESCRIPT, aplicando esta metodología multidisciplinar, ha conseguido soluciones más eficaces que propuestas anteriores, aportando procedimientos válidos para la resolución de objeciones que descalificaban globalmente la viabilidad de las votaciones electrónicas (Informe Mercury [7], por ejemplo).

A juicio de los autores del presente artículo, todo el esfuerzo intelectual y material volcado en este área tiene sentido si da como resultado una mejora cualitativa de la democracia que refuerce su legitimidad. Entendemos que esta mejora radica fundamentalmente en estudiar la potencialidad de las redes telemáticas para facilitar y desarrollar la participación ciudadana. Es decir, profundizar en dinámicas de democracia participativa, que eduquen, permitan y agilicen la participación de los ciudadanos a través de la discusión y solución de las cuestiones que les son comunes.

7 Referencias

1. J. Carracedo, A. Gómez, J. Moreno, E. Pérez y J. D. Carracedo: Votación electrónica basada en criptografía avanzada (Proyecto VOTESCRIPT). II Congreso Iberoamericano de Telemática. CITA'2002. Mérida, Venezuela (2002).
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-Verlag, 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 (1996).
4. 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).
5. Riera i Jorba, Andreu. Design of Implementable Solutions for Large Scale Implementable Voting Schemes, Tesis doctoral Universidad Autónoma de Barcelona, 1999.

6. J. Carracedo y J. D. Carracedo. Telemática y sociología. Apuntes para una investigación mutlidisciplinar: tarjetas de crédito anónimas y democracia electrónica. I Congreso Iberoamericano de Telemática. Cartagena, Colombia, 2001.
7. 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>
8. Informe sociológico sobre la experiencia en El Hoyo de Pinares, disponible en Observatorio para la Democracia Digital y los Derechos de Ciudadanía en Internet. <http://www.ucm/info/demodigi>
9. T. Kohno, A. Stubblefield y A.D. Rubin. Analysis of an Electronic Voting System, Julio 2003. <http://avirubin.com/vote.pdf>