Uso del DNIe para reforzar el anonimato en el voto telemático mediante tarjetas inteligentes

Emilia P. Belleboni1 y Justo Carracedo Gallardo2
Departamento de Ingeniería y Arquitecturas Telemáticas. Escuela Universitaria de Ingeniería Técnica de Telecomunicación. Universidad Politécnica de Madrid
Ctra. Valencia km. 7. 28031 Madrid.
Teléfono: (+34) 91 336 78 02. Fax: (+34) 91 336 78 17,
{belleboni[1],carracedo[2]}@diatel.upm.es

Resumen. Debe llegar el momento en cual el documento de identidad electrónico, DNIe, que en España expide la Dirección General de Policía, sea una herramienta que goce de la confianza ciudadana a la hora de operar como tal documento electrónico. Este artículo avanza en las ventajas que conlleva introducir la utilización de este DNIe en un sistema de voto telemático (Votescript+) basado tanto en criptografía avanzada como en la fortaleza que proporcionan las tarjetas inteligentes. Se incorpora la utilización del DNIe como elemento determinante para la identificación del votante, tanto dentro del proceso de obtención de la autorización para votar como dentro del proceso de verificación individual de resultados, y se describe resumidamente el protocolo de funcionamiento del sistema en sus distintas fases.

Palabras clave: DNI electrónico, voto electrónico, voto telemático.

1. Introducción y antecedentes

El voto es solo un mecanismo para posibilitar la democracia. Por ello, la automatización y modernización de los sistemas de votación solo se justifica si se adapta a las necesidades de los electores y si contribuye a mejorar la forma en la que la ciudadanía manifiesta su opinión y traslada sus decisiones.

1.1 Voto electrónico, voto telemático y voto por Internet

Actualmente, en distintos países (por ejemplo, Brasil (1) y Venezuela(2) se han implantado, con bastante éxito, sistemas de voto electrónico consistentes en la de automatización de todo el proceso de emisión y recuento del voto. Para ello se dispone de urnas electrónicas ubicadas a la vista del votante en las que éste deposita el voto mediante un procedimiento electrónico (en sustitución de las antiguas urnas donde se introducen los votos en papel). En algunos casos se dispone, además, de redes de comunicación para transmitir los resultados del recuento realizado en las urnas electrónicas.

En el caso del *voto telemático* la votación se lleva a cabo mediante el uso de redes telemáticas y agentes telemáticos específicos de tal forma que los votos se depositan

en una *urna remota* fuera de la vista del votante. Tanto la *autorización* para votar como el *voto* "viajan" por la red.

En líneas generales, se pueden distinguir dos escenarios para voto telemático: a) el votante puede votar desde cualquier sitio, también desde casa; y b) para votar es necesario acudir a *puntos específicos de votación.*

Con frecuencia se denomina también *voto electrónico* (*eVoting*) a lo que aquí denominamos *voto telemático.* Nosotros mantenemos una nomenclatura diferenciada debido a que el voto en urna "in situ" y el voto en urna remota son dos alternativas con una dimensión tecnológica y unos requerimientos sociopolíticos radicalmente distintos, y no distinguirlo claramente crea confusión en la ciudadanía. Podría optarse por decir a cada paso "voto electrónico con urna in situ" o "voto electrónico remoto", pero eso supondría una complicación innecesaria.

Por último, algunas propuestas de voto telemático que permiten votar desde cualquier sitio (también **desde casa**) usando los servicios convencionales de Internet podrían denominarse *voto por Internet*. En los casos en los que, como el que se presenta en este artículo, la votación se realiza utilizando agentes telemáticos propios y una red propia, consideramos más adecuado utilizar la denominación *voto telemático*. (Aunque en la práctica esa "red propia" no sea sino una red virtual "apoyada" en la infraestructura de transporte de datos de Internet).

1.2 Requerimientos para el voto telemático

Al formular una propuesta de *voto telemático* se debe ser consciente de la magnitud de los ataques que busquen alterar el resultado final de la elección, mucho más significativos que cuando se trata de ataques a los sistemas de votación tradicional o en los sistemas de voto electrónico con urna *in situ*. Cualquier ataque puede venir tanto de agentes externos como de agentes internos o de colusión entre ellos, que por motivaciones políticas, económicas o técnicas quieran producir una alteración en los resultados finales. Existe la necesidad de proteger a los votantes de las amenazas y coacciones de los que puede ser víctima si el sistema no toma precauciones específicas ya que la automatización de los procedimientos puede derivar también en la automatización y masificación de la adición, eliminación o alteración de los votos y de la coacción hacia los votantes (3).

Con el fin de contrarrestar estas amenazas, los sistemas de votación telemáticos usan técnicas robustas de criptografía que bien combinadas garantizan la confidencialidad e integridad de la información, así como garantías de que son emitidos por fuentes válidas.

Como paso previo al diseño de los sistemas de votación que se describen en el presente artículo, se llevó a cabo una investigación sociológica mediante la cual se identificó y desglosó una larga lista de requisitos (se discuten en (4) páginas 497 a 501) que podrían resumirse en los siguientes principios básicos:

1. Es imprescindible que se realice una identificación fiable de los votantes, impidiendo la suplantación de identidad, la emisión de múltiples votos y la denegación arbitraria del derecho a voto.
2. Una vez satisfecho el paso anterior, es necesario permitir al votante ejercer su derecho con garantías de que nadie (en solitario o coludiendo con otros) es capaz

de relacionar el voto con el votante que lo ha emitido. Estas garantías deben tener en consideración que no se debe exponer al votante a tener en su mano información que pueda ponerle en riesgo de sufrir una potencial coacción. Aquí adquiere especial importancia el esmero que se pone en la información que el votante usará para verificar el tratamiento seguido por su voto.

3. En ningún momento deber ser posible que se añadan votos ilegítimos, ni que se modifiquen o eliminen votos legítimos.

Una de las dificultades que presenta el diseño adecuado de un sistema de votación telemática es que dentro de los requisitos se presentan exigencias que son, en principio, aparentemente **contradictorias**. Destaquemos las siguientes:

a) El sistema de votación debe garantizar que solamente las personas con derecho a voto pueden emitir un voto y a la vez debe garantizar que es imposible relacionar a esta persona, fehacientemente identificada, con el voto que ha emitido. Es decir, hay que combinar (aunque en fases distintas) dos servicios de seguridad habitualmente contrapuestos: **autenticación** y **anonimato**.
b) El sistema de votación telemático debe proporcionar mecanismos para que los votantes **verifiquen** el tratamiento que se le ha dado a su voto, pero ese mecanismo no debe permitir al votante probar ante terceros cuál ha sido el contenido de ese voto (para evitar la coacción y la venta de votos).

1.3 Las propuestas Votescript

Desde principios del año 2000 los autores del presente artículo han estado participando el diseño, prueba e implementación de sistemas de votación telemática en el marco del Proyecto Votescript (5)[1]. En 2003 se llevó a cabo en el municipio de Hoyo de Pinares (provincia de Ávila, España) una experiencia piloto de una implementación simplificada de Votescript desarrollada en colaboración con la Fábrica Nacional de Moneda y Timbre (6). Se han desarrollado diversas mejoras y prototipos sobre los que se han ido realizando diversas publicaciones (cabe destacar CIBSI 2003(7); (4) pág. 458 a 480 y 495 a 531]; (8) y (9).

En todas estas versiones se mantienen una serie de características comunes que giran en torno la utilización de una tarjeta inteligente, del tipo *JavaCard*, que previamente a la votación se habrá hecho llegar a todos los votantes, en la que se ejecutarán los algoritmos propios de Votescript y se almacenarán de forma segura todos los datos sensibles, como pueden ser las claves usadas para cifrar la información. En el presente artículo, a partir del apartado **3**, se describe una nueva versión del sistema, que hemos denominado **Votescript+**[2], que incorpora la

[1] La primera financiación pública se obtuvo a través del proyecto "Votación Electrónica Segura basada en criptografía avanzada" patrocinado por Plan Nacional de I+D+I (TIC 2000-1630).

[2] Este artículo se enmarca dentro de los trabajos que este grupo de investigación lleva a cabo en el proyecto TSI2006-4864 *Plataforma telemática de Administración Electrónica basada en coreografía de servicios* subvencionado por el Ministerio de Educación y Ciencia, en el Plan nacional de I+D+I

utilización una tarjeta inteligente adicional, el DNIe, para separar de forma más robusta la fase de identificación-autorización de la fase de emisión del voto.

2. Resumen de las características de Votescript

Como se acaba de comentar, la propuesta Votescript+, que incorpora la utilización de dos tarjetas inteligentes para la votación telemática, una de ellas el DNIe del votante, se realiza mediante modificaciones a Votescript. En los párrafos que siguen se resumen las características más relevantes de este sistema.

Es fundamento básico de Votescript que toda la información que transita por la red lo haga con garantías de integridad, prueba de origen y confidencial. Toda vez que sea posible, las labores que se realizan en los componentes que podemos denominar oficiales estarán supervisadas por otros equipos informáticos a cargo de interventores o testigos que actúan en representación de los distintos colectivos de ciudadanos que participan en la votación. Además, se almacena la información suficiente para permitir que la auditoría contraste el valor de los registros con los resultados finales publicados. Con todo es posible realizar adecuadamente las verificaciones que soliciten interventores a título colectivo y votantes a título individual.

2.1 Escenario de comunicación

Para dar satisfacción a los requisitos demandados por los ciudadanos, se ha establecido (9) la utilización de tres redes independientes: una para identificar al votante, otra para emitir el voto y la tercera para permitir que el votante pueda realizar la verificación sobre el tratamiento de su voto (figura 1). Todos los recursos utilizados en cada una de estas tres redes deber ser auditables y haber sido auditados antes del inicio el proceso electoral.

El escenario de comunicación de Votescript incluye un conjunto de sistemas automáticos que se describen a continuación:

. Puntos de autenticación (Authentication Points, APs): son equipos informáticos, sin capacidades criptográficas, que permiten al votante realizar el procedimiento de autenticación para obtener la autorización que le permitirá emitir el voto.

. Un sistema Administrador (Administration System, AS) que puede considerarse como sistema *oficial* el cual emite las autorizaciones solicitadas por los votantes.

. Varios Sistemas de Intervención (Intervention Systems, Iss) encargados de supervisar y contrastar el funcionamiento del sistema Administrador *oficial*.

. Cabinas de Votación (Voting Cabin, VoCs), que facilita el aislamiento del votante protegiéndolo de injerencias externas y le permite, una vez que ha sido ya autorizado, emitir el voto de forma segura guardando en su tarjeta de votación el comprobante de voto que, en su caso, le permitirá aportar la prueba para la verificación.

. Una Urna (Ballot Box, BB) que almacena los votos hasta el momento del recuento y devuelve los comprobantes de de votación.

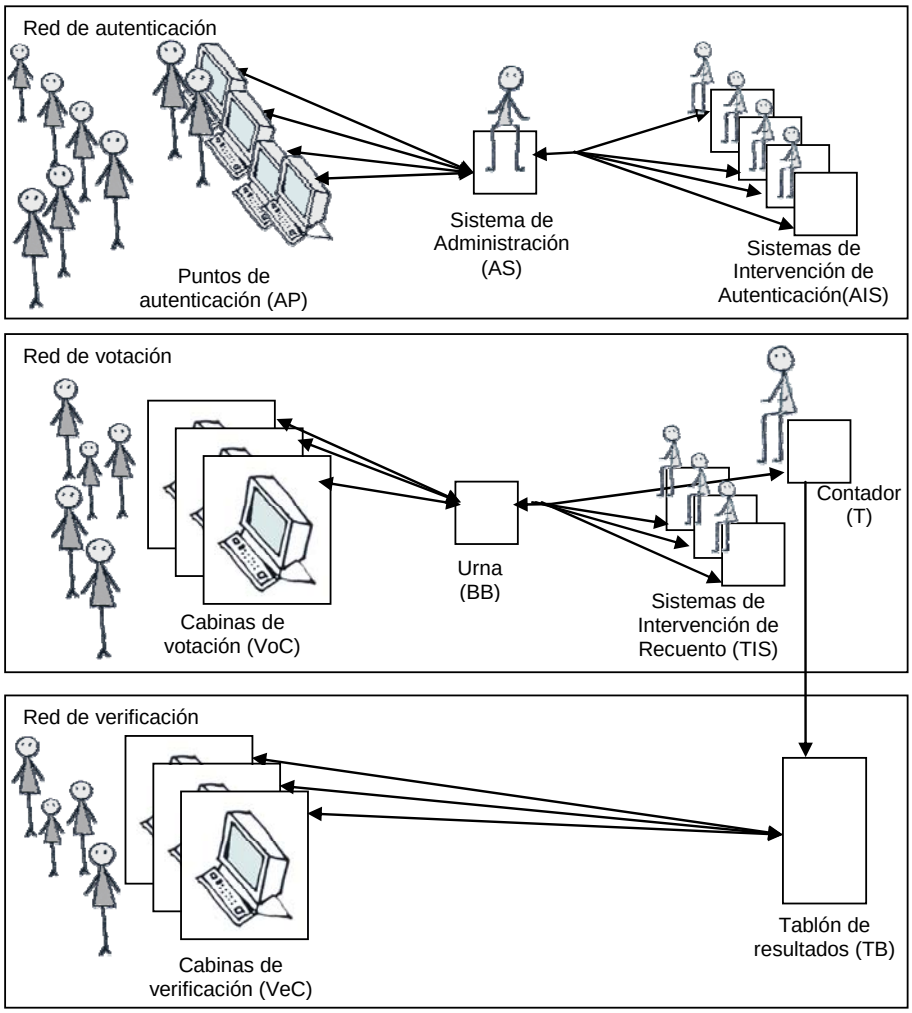

Figure 1: Visión general: 3 redes independientes componen el sistema Votescript

. Un Contador (Tallier, T). que *abre los votos* y realiza el recuento *oficial* teniendo en cuenta toda la información existente en el interior de los denominados Sobres Seguros.

.Varios Sistemas de Intervención de Recuento (Tally Intervention Systems, TIS) que realizando en paralelo la tarea del Contador impedirán la introducción, modificación o eliminación de votos válidos.

. Un Tablón de Resultados (Tally Board, TB), donde el Contador hace públicos los resultados, y a partir del cual los Sistemas de Intervención de Recuento comparan los resultados.

. Cabinas de verificación (Verification Cabin, VeC), que tal como las Cabinas de Votación, aíslan al votante para permitirle acceder a los recursos de la red que se

encargan de verificar que los datos almacenados en la tarjeta de votación y en los registros publicados por el sistema son congruentes.

2.2 Comportamiento global de Votescript

Cada una de las personas implicadas en el proceso de votación posee la tarjeta inteligente que le permite realizar su tarea. Junto con los procedimientos diseñados para permitir la auditoría del software y de los resultados, el otro pilar en el que se sustenta la fortaleza de la propuesta Votescript es la posesión por parte de todos y cada uno de los votantes de su Tarjeta Inteligente de Votación (Smart Voting Card, SVC). Esta tarjeta incluye mecanismos de protección contra intentos de lectura o escritura por parte de dispositivos no autorizados y permite al votante ofrecer prueba de origen, descifrar información confidencial y además ejecutar en su interior otros procesos criptográficos. A partir de ahí, la actividad se realizará de la siguiente forma:

Comienza con las fases 1 (autenticación) y 2 (votación), las cuales son consecutivas desde el punto de vista del votante, quien como primer paso debe presentarse ante la red de autenticación del sistema, y luego dirigirse a la red de votación donde entregará su voto. Desde el punto de vista del sistema estas dos fases son simultáneas durante todo el periodo dedicado a que los votantes acudan a los sitios donde se encuentran los equipos adecuados y emitan cada uno su voto.

En la fase 1, el votante, haciendo uso de su tarjeta inteligente de votante se identifica frente a uno cualquiera de los Puntos de Autenticación del sistema y solicita la autorización para emitir el voto la cual será denegada si el votante ya ha realizado previamente la misma gestión o no pertenece al cuerpo de votantes. Los Sistemas de Intervención de Autenticación y el Sistema de Administración realizan las mismas tareas para decidir emitir o no la autorización. La solicitud de autorización que realiza la tarjeta consiste en una clave (K_{dV}, ocultada por la tarjeta con un factor de opacidad para que posteriormente no se pueda relacionar el voto con el votante) que más tarde servirá para descifrar el voto. Esta *autorización*, clave (K_{dV}), firmada a ciegas por el Sistema de Administración y por los Sistemas de Intervención de Autenticación servirá de garantía de que el voto ha sido emitido por un legítimo votante.

La fase 2 (votación) empieza para el votante después de haber obtenido la autorización. El votante debe acudir con su tarjeta a una cualquiera de las Cabinas de Votación. En el interior de la cabina y aislado de injerencias externas, el votante encuentra los recursos que le permite emitir su voto que irá cifrado con una clave solo conocida por la tarjeta que la genera, (K_{cV}), simétrica de (K_{dV}). El voto está cifrado de forma que la Urna no puede descifrar la pieza de información que recibe. Después se almacena en la tarjeta, de forma protegida, el comprobante de voto que ésta recibe.

La fase 3 (escrutinio) dará comienzo una vez cerradas las dos fases anteriores. En esta fase se procede a la *apertura de la Urna*, la cual trasvasa al Contador (T) y a los Sistemas de Intervención de Recuento los votos custodiados por ella mientras las fases 1 y 2 estaban activas. Cada receptor del contenido de la Urna, actuando en paralelo, realizará el recuento con los mismos datos. El Contador envía los resultados al Tablón de Resultados, para que todos los Interventores puedan corroborarlos.

La fase 4 (verificación) se divide en dos partes. En la primera (fase 4.1) se procede a aclarar todas las posibles divergencias que puedan aparecer entre los resultados

obtenidos en el recuento *oficial* y el que realicen los interventores, pues todos han recibido los mismos datos de la Urna. En la segunda parte (fase 4.2) el votante vuelve a tomar protagonismo ya que es el momento en el que puede acceder a la *red de verificación*, donde podrá revisar el tratamiento que ha tenido su voto, presentando algunos de los datos almacenados en su tarjeta inteligente que se contrastarán con la información hecha pública por el Tablón de Resultados, pudiendo presentar reclamación ante la Autoridad de Elección en caso de desacuerdo, aportando pruebas robustas como el comprobante de voto recibido de la Urna. La Autoridad de Elección accederá a los registros de los distintos agentes, a la información almacenada en la tarjeta inteligente de votante y a la información publicada para dirimir todas las reclamaciones presentadas tanto por votantes como por interventores.

La fase 5 (publicación) es la última, una vez tomadas las decisiones oportunas por parte de la Autoridad de Elección, se procede a la publicación definitiva de resultados y a la destrucción de toda la información generada en el proceso, en atención a la duda razonable por parte de ciudadanos que argumentan que los sistemas que son seguros hoy en día pueden no serlo en un futuro. (3)

3. Dos tarjetas inteligentes para la votación telemática

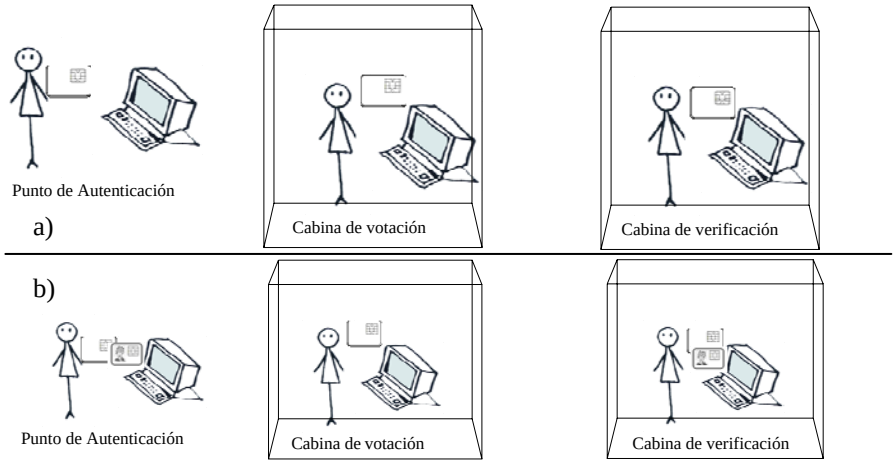

Figure 2: Uso de tarjetas inteligentes en Votescript y Votescript+

En la figura 2 a) se representa de forma esquematizada la forma en que el votante utiliza la Tarjeta Inteligente de Votación en el esquema Votescript; a esta tarjeta, en la explicación que sigue, la denominaremos, para simplificar, tarjeta Votescript. En la parte b) de la misma figura se representa el proceso seguido en Votescri+, en donde se refleja además la utilización que se hace del DNIe. En este caso a la Tarjeta Inteligente de Votación la denominaremos simplificadamente SVC+.

Por cuestiones de espacio y de oportunidad no se describe aquí de forma pormenorizada las características y procedimientos previstos para el uso del DNIe

cuya información oficial es pública (10). Para Votescript+ el dato de mayor importancia es la presencia en el chip de los certificados electrónicos reconocidos de autenticación y de firma.

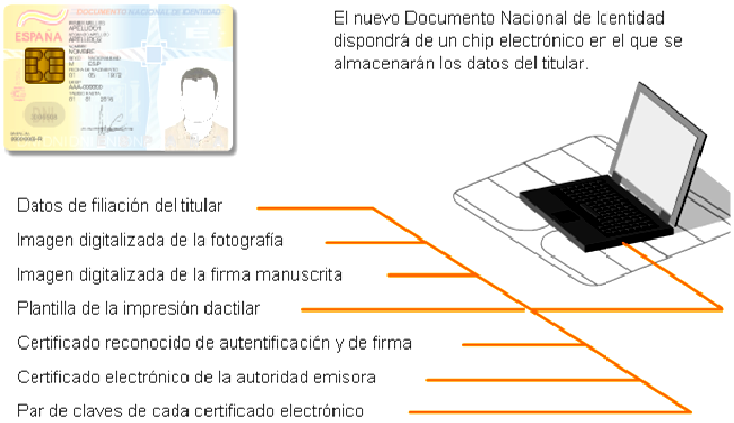

Figure 3: Datos del Chip en el DNIe español

En la figura 3 se recoge el aspecto físico del DNIe y los datos que contiene el chip.

Fase de Autenticación. El proceso diseñado en Votescript (a) y el correspondiente a Votescript+ (b), se describe brevemente continuación, para cada fase, con el fin de facilitar la comparación entre ambas propuestas.

a) La tarjeta Votescript contiene los datos y las claves que sirven para identificar al votante, en base a las cuales puede demostrar su pertenencia al cuerpo electoral cuando solicita la autorización para votar. Esta tarjeta es también utilizada en la fase de emisión del voto, según se describió en el apartado 2.2.
   La tarjeta Votescript tiene que ser individualizada para todos y cada uno de los votantes ya que soporta la identidad del votante mediante un par de claves, privada y pública (ésta última es, como su nombre indica, conocible por todos los actores presentes en el protocolo y está asegurada por el correspondiente certificado digital).

b) Para reforzar aún más la emisión anónima del voto, el esquema de votación telemática **Votescript+** que se describe en este artículo incorpora la utilización una tarjeta inteligente adicional, el DNIe, que no se utiliza en la fase de votación. Con ello se consigue separar de forma más robusta la fase de identificación-autorización de la fase de emisión del voto.
   La SVC+ **carece de elementos de identificación** del votante, es una tarjeta genérica e igual para todos los votantes, en tanto que la tarjeta Votescript tiene que ser personalizada para cada uno de ellos.
   El votante, figura 2 (b), haciendo uso de una SVC+ y de su DNIe se identifica frente a uno cualquiera de los Puntos de Autenticación del sistema y solicita la *autorización* para emitir el voto. Para ello, el Punto de Autenticación, que no tiene capacidades criptográficas, dispone de dos lectores de tarjeta para poder insertar ambas simultáneamente.

La validación de la identificación del ciudadano que pretende votar se realiza mediante el DNIe y con la colaboración del *Centro de Validación del DNIe*[3] conforme a los procedimientos y protocolos establecidos por los poderes públicos. Es decir, Votescript+ delega en el esquema DNIe el aseguramiento de la identidad de los votantes. A medida de que, con el tiempo, este aseguramiento vaya siendo cada vez más robusto y vaya ganando la confianza ciudadana por la incorporación de su uso en la vida cotidiana, esa mejora la heredará Votescript merced a la delegación que estamos comentando.

La posesión de un documento de identidad válido no significa necesariamente tener derecho a voto (por motivos de edad, de sentencia judicial, de residencia en región ajena a la votación en curso, etc.). Por tanto, en la *fase de autenticación* la tarjeta Votescript+, "alter ego" del votante ante el sistema de votación telemática, deberá seguir ejecutando los protocolos correspondientes hasta obtener la *autorización* para votar que será almacenada en la tarjeta Votescript+.

Fase de votación

a) En Votescript tanto la fase de *autenticación* (que incluye la identificación) como la fase *emisión del voto* se realizan con la misma tarjeta y en base a la información en ella contenida.

   La exigencia de que el voto se emita de forma anónima, de manera que ningún dato identificativo del votante pueda ser utilizado en la red de votación está garantizada por los pasos seguidos en el protocolo de votación que se ejecuta en la CPU de la tarjeta (que han sido verificados y auditados previamente). Gracias al carácter *tamper-proof* de la tarjeta se garantiza que los programas en ella contenidos no pueden ser manipulados ni las claves almacenadas pueden ser leídas o alteradas fraudulentamente.

b) En el esquema Votescript+, el DNIe, que es la tarjeta que posee los datos identificativos del votante, no se usa en la *fase de de votación*. Solo se utiliza la tarjeta Votescript+ (que también es *tamper-proof*) en la que están almacenados los protocolos seguros para emitir el voto. Como la tarjeta Votescript+ solo contiene una autorización para que su poseedor pueda votar, existe una garantía procedimental añadida que asegura que el voto es anónimo. No obstante, debido a ese desacoplo, es necesario garantizar que el votante, desde el instante que retira su DNIe y su tarjeta Votescript+ al finalizar la fase de autenticación (para ese votante) no pueda tener contacto con persona alguna con la que pueda intercambiar o ceder su tarjeta, situación que, caso de permitirse, facilitaría la venta o cesión de voto. Esta prevención procedimental no tiene porqué establecerse en Votescript porque en la fase de votación el votante tiene que autenticarse de nuevo ante su tarjeta.

Fase de Verificación

a) En Votescript el votante acude a las cabinas de verificación solo con su tarjeta Votescript. Para garantizar la corrección de la operación y evitar la coacción o venta de votos se exige al votante se autentique ante su propia tarjeta Votescript.

[3] El Centro de Validacion es un recurso externo a Votescript, ofrecido por la infraestructura del DNIe.

b) En el caso de Votescript+ será necesario algo más que portar la tarjeta Votescript+ ya que ésta no contiene la identificación del votante. Por ello en la Cabina de Votación se exige al votante que aporte también su DNIe. Para no tener que recurrir a verificar de nuevo la identificación del votante (usando el *Centro de Validación del DNIe*) con los consiguientes riesgos de establecer conexiones entre voto y votante, se recurre a un artificio consistente en que en la fase de autenticación la tarjeta Votescript+ genera un testigo aleatorio para verificación que el DNIe firma con su clave privada. Este testigo en claro y firmado es almacenado en la tarjeta Votescript+, y en la fase de verificación la tarjeta solo tiene que pedir al DNIe que se introduce en el lector correspondiente que firme de nuevo el testigo para verificación. Comprobando esta firma con la que tenía almacenada (que no conlleva identificación del votante) podrá averiguar si se trata o no del propietario verdadero de la tarjeta Votescript+. También en este caso, Votescript+ delega en el esquema DNIe la garantía de que el portador del DNIe es su verdadero propietario.

Como se ha comentado, todos los actores que intervienen en el proceso (Administrador, Interventores, Autoridad de Elección, etc.) lo hacen a través de tarjetas inteligentes diseñadas "ad hoc", de tal modo que esas tarjetas contienen de forma segura todos los datos y todas las claves que se corresponden con el rol que desempeñan en el sistema.

4. Breve descripción de los protocolos en Votescript+

La fase de autenticación del votante comienza con el proceso de identificación del mismo de acuerdo a los protocolos y recursos de Votescript teniendo en consideración la existencia del DNIe con capacidad para autenticar a un ciudadano y firmar en su nombre, así como los procedimientos para su uso. Con esta disposición (figura 4) se pone en contacto el votante con el Sistema Administrador, realizando los pasos consecutivos que, con la colaboración del Centro de Validación del DNie, conducen a la identificación del ciudadano por canal seguro.

En esta fase, se generan piezas de información que permiten aportar pruebas robustas a una auditoría, que detectaría la denegación arbitraria del derecho a voto en caso de producirse. En el paso "a", la Tarjeta Votescrip+ (SVC+) solicita al DNIe que comience el procedimiento de identificación, el DNIe contesta con la información "b" que es enviada por medio de la SVC+ y del Sistema Administrador hacia el Centro de Validación (paso "c"), cuya respuesta (paso "d") es la aprobación (o no) de la información presentada por el DNIe. El Sistema Administrador enviará hacia la Tarjeta SVC+ una pieza de información firmada (paso "e") con el resultado de la operación. Esta pieza de información, en caso de denegación debe indicar el motivo por el que produjo este evento. La SVC+ comprueba la firma sobre dicha información del Sistema Administrador y la almacena en un sitio seguro, que impida su borrado o modificación, accidental o voluntario. Estas piezas de información guardadas en los registros del Sistema Administrador y en la SVC+ permitirán a un auditor, desvelar la causa del impedimento a votar, disuadiendo con ello de la tentación de aplicar en este punto una denegación arbitraria al derecho a voto de determinados ciudadanos.

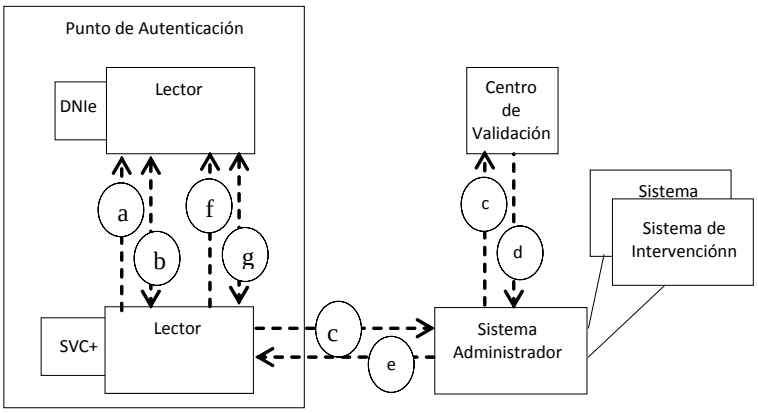

Figura: 4 Proceso de Identificación del ciudadano.

Puesto que el DNIe no está pensado para descifrar información que se le envíe de forma confidencial al votante y que con el acto anterior solamente se ha satisfecho un paso previo de la autenticación de ciudadano (todavía no se puede decir que es un votante), la SVC+ genera una clave para la recepción confidencial de información (K_{aut}), un *testigo de verificación*, un par de claves (k_{dV}, k_{cV}) y los factores de opacidad necesarios para opacar k_{dV}. Los pasos "f" y "g" representan la firma con el DNIe de la clave k_{dV} opacada para todos los destinatarios, el identificador del votante y del *testigo de verificación.*

La figura 5 representa el intercambio de información que se explica a continuación (el número de la viñeta coincide con el número dentro da cada círculo en la figura):

En la red de **autenticación**

1. El paso 1 representa que el proceso de Identificación descrito anteriormente se ha realizado satisfactoriamente. La Tarjeta SVC+ almacena de forma segura y protegida el *testigo de verificación*, el identificador de votante (*Voter Id*), y la k_{dV} opacada para el sistema administrador y para cada uno de los sistemas de intervención, todo ello firmado por el DNIe.
2. La identificación del votante y las claves opacadas y firmadas por el votante, concatenada con la clave de sesión (k_{aut}) que se usará en la comunicación de vuelta, es enviada confidencialmente desde la SVC+ hacia el Sistema Administrador a través del Punto de Autenticación.[4]

   AS_P *[(*k_{aut}*),* V_s *(Voter Id), (*O_{AS} *(*k_{dV}*),* V_s *(*O_{AS} *(*k_{dV}*)), AS),*
   (O_{IS1} *(*k_{dV}*),* V_s *(*O_{IS1} *(*k_{dV}*)), IS1), ...]*

[4] AS_P[xx] significa que el mensaje xx es cifrado con la clave pública de AS (Administrator System)
V_s[xx] significa que el mensaje xx es cifrado con la clave secreta de V (Voter)
O_{AS}[xx] significa que el mensaje xx ha sido opacado para que AS lo firme a ciegas.

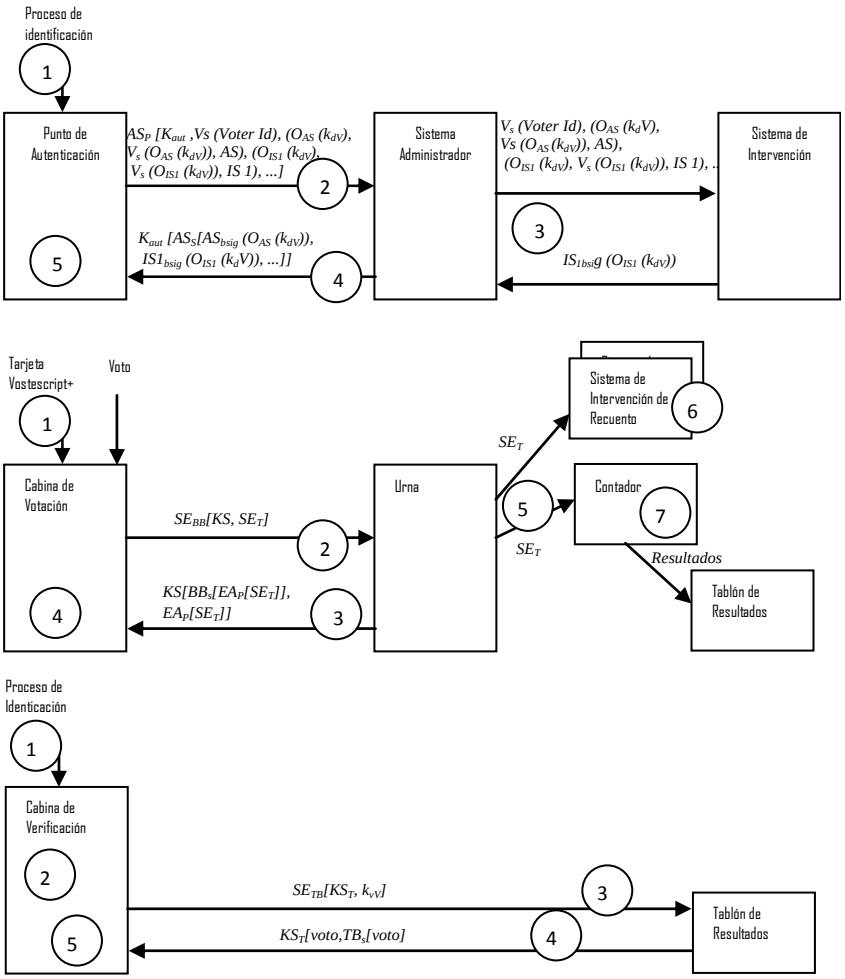

Figura 5: Protocolo Votescript+ en las tres redes virtuales

3. El Sistema Administrador descifra los datos recibidos y los reenvía hacia todos los Sistemas de Intervención de autenticación:
   [Vs (Voter Id), (O_{AS} (k_{dV}), V_s (O_{AS} (k_{dV})), AS), (O_{IS1} (k_{dV}), V_s (O_{IS1} (k_{dV})), IS1), ...]
   A continuación tanto el Sistema Administrador como los Sistemas de Intervención verifican la identidad del votante y su firma, y si no le han firmado la autorización con anterioridad, proceden a firmar a ciegas la clave k_{dV} opacada correspondiente. El Sistema Administrador recolecta toda esta información.[5]
   IS_{1bsig} (O_{IS1} (k_{dV}))
4. Este paquete de claves opacadas y firmadas es firmado a su vez por el Sistema Administrador y cifrado con la clave de sesión de autenticación del votante para

[5] IS_{1bsig} [xx] significa que el mensaje xx ha sido firmado a ciegas por IS_1 (Intervention system 1)

enviarlo al Punto de Autenticación de forma confidencial con prueba de origen.[6]
k_{aut} *[AS_S[AS_{bsig} (O_{AS} (k_{dV})), IS_{1bsig} (O_{IS1} (k_{dV})), ...]]*

5. El Punto de Autenticación pasa la información a la Tarjeta SVC+, que es el único dispositivo capaz de conocer el contenido y verificar las firmas. Una vez desopacadas las k_{dV} firmadas, conformarán la *autorización* para votar que en la siguiente fase será ligada de forma inseparable al voto.

En la red de votación

Finalizados los pasos que se dan en la red de autenticación, el votante se dirige a la Cabina de Votación donde procede a entregar el voto usando únicamente de la SVC+.

1. En el dispositivo que se encuentra dentro de Cabina de Votación el votante inserta su SVC+.
2. La Cabina de Votación le solicita el voto el cual es cifrado dentro de la SVC+ con k_{cV} (pareja de k_{dV}), concatenado con k_{dV} y con la autorización (k_{dV} firmada por los Sistemas de intervención de autenticación y por el Sistema de Administrador). Esta información, que en última instancia será descifrada por el Contador y por los Sistemas de Intervención de Recuento podría posteriormente poner en riesgo el secreto del voto, por lo que se protegerá dentro de un *Sobre Seguro entre la tarjeta y el Contador* (*Secure Envelope*, SE_T).
   SE_T=*[k_{cV}[Voto], k_{dV},AS_{bsig} (O_{AS} (k_{dV})), IS_{1bsig} (O_{IS1} (k_{dV})), ...]]*
   Se genera una clave simétrica KS, que junto al *Sobre Seguro* anterior, es introducida en un *Sobre Seguro* externo, esta vez *entre la tarjeta y la Urna*. Esta pieza de información es enviada a la Urna (Ballot Box)*: SE_{BB}[KS, SE_T]*
   3. La Urna elimina el *Sobre Seguro* externo y separa las dos piezas de información: SE_T y KS. El SE_T es almacenado en la Urna hasta el que culmine el período destinado a la emisión de votos y a la vez es convertido en *comprobante* al ser cifrado con la clave pública de la Autoridad de Elección, firmado por la Urna y cifrado con KS para ser enviado confidencialmente hacia la Cabina de Votación. *KS[BBs[EA_P[SE_T]], EA_P[SE_T]]*
4. La Cabina de Votación entrega la información a la SVC+ la cual obtiene y verifica la firma de la Urna y almacena de forma segura el *comprobante* que solamente podrá ser desvelado si el votante decide presentarlo a la Autoridad de Elección.
5. Finalizado el período de recepción de votos se requiere la presencia de las personas que ejercen de Administrador y de Interventores para, entre todos, construir la clave necesaria para *abrir la Urna* e iniciar el proceso de volcado de su contenido hacia el Contador y los Sistemas de Intervención de Recuento, ofreciendo así garantías de que nadie ha poseído previamente los resultados intermedios de la votación a modo de información privilegiada. En realidad se requerirá la presencia del Administrador y de una cantidad "suficiente" de

[6] k_{aut} [xx] significa que el mensaje xx ha sido cifrado con la clave simétrica $k_{aut.}$

Interventores (para impedir que uno de ellos, o un número reducido de los mismos, puedan boicotear todo el proceso electoral) los cuales insertarán sus DNIe y las tarjetas inteligentes que identifican sus respectivos roles frente al sistema y tras un proceso de identificación biométrica recompondrán la clave que permite abrir la Urna. Se establecen los mecanismos de comparación que permite verificar que todos los sistemas reciben la misma información.

6. Nuevamente se requiere la presencia de las personas que ejercen de Administrador y de Interventores para, entre todos, construir esta vez la clave privada del contador. Esta clave es entregada al Contador y a todos los Sistemas de Intervención de Recuento para que puedan conocer el contenido interno de cada uno los votos cifrados que han recibido de la Urna. Una vez abiertos todos los sobres SE_T se lleva a cabo el recuento
7. El Contador envía al Tablón de Resultados (Tally Board, TB) la información compuesta por la clave k_{aV} y las firmas del Administrador y los Sistemas de Intervención sobre clave k_{aV}, junto con el voto descifrado. Una vez publicados los resultados, cada Interventor verificará que esta información coincida con la que su sistema tiene y en caso contrario, si hace falta, recurrirá a la autoridad de Elección para que se realicen las comprobaciones de registros necesarios.

En la red de verificación

1. Después la publicación de resultados, durante un período limitado de tiempo, cualquier votante puede dirigirse, con su DNIe y su SVC+, a una Cabina de Verificación (VeC) donde encuentra los dos dispositivos adecuados que le permiten inicialmente autenticar tal como lo hizo para obtener la autorización que le dio derecho a votar, aunque en esta ocasión no se usa el Centro de Validación.
2. La SVC+ le presenta al DNIe el *testigo de verificación* y comprobado que el votante está presentado su propia SVC+, continúa la operación de verificación.
3. La tarjeta introduce la k_{aV} y una clave de sesión KS_T en un *sobre seguro* entre la cabina de verificación y el Tablón de Resultados SE_{TB} y lo envía al Tablón. ($SE_{TB=}[k_{aV,} KS_T]$) El Tablón de Resultados recupera k_{aV} y localiza el voto que ha sido descifrado con dicha clave, firma el voto y lo cifra con KS_T para enviarlo de vuelta a la Cabina de Verificación: $KS_T[voto, TB[voto]]$
4. La VeC pasa la pieza de información a la SVC+ la cual abre el sobre, verifica la firma y envía el voto a la Cabina para que lo muestre al votante.

Si el votante no está de acuerdo con el voto que visualiza, puede presentar su SVC+ (acompañado o no por un perito de su confianza) ante la Autoridad de Elección, dónde, tras recuperar el comprobante de voto firmado por la Urna, se determinará si el comportamiento del sistema ha sido correcto o por el contrario ha existido error o fraude. Esta posibilidad de verificación actúa como disuasión frente a cualquier intento de destruir votos por parte de la Urna. La inserción de votos o modificación de voto quedaría en evidencia debido al conjunto de mecanismos criptográficos propuestos.

4. Conclusiones, trabajos futuros y agradecimientos

Con el desarrollo del esquema Votescript+ vuelve a ponerse de manifiesto que la seguridad del proceso de votación telemática no debe descansar solamente en la honestidad y capacitación profesional de los gestores del sistema sino fundamentalmente en la existencia de mecanismos criptográficos y protocolos telemáticos seguros que impiden la comisión de errores involuntarios, actuaciones ilícitas y la colusión maliciosa entre los distintos agentes que participan en la votación.

En los sistemas convencionales de votación (al menos en el caso de España) las garantías sobre la identidad de los votantes (y otros actores) descansan en la confianza en la fiabilidad del DNI convencional. De igual forma, en Votescript+, que propone una traslación del voto al ciberespacio, el aseguramiento de la identidad de los votantes se delega en el esquema DNIe. A medida de que, con el tiempo, este aseguramiento vaya siendo cada vez más robusto y vaya ganando la confianza ciudadana, esa mejora la heredará, consecuentemente, Votescript+.

Como trabajos futuros cabe destacar la necesidad de adaptar el sistema de votación a personas con diferentes discapacidades, así como la necesidad de contemplar votaciones multi-urna para los casos en los que los recuentos deban realizarse separadamente para distintos grupos de votantes.

Agradecimientos. Los autores de este artículo quieren manifestar su agradecimiento a los restantes miembros del grupo de investigación que han participado en las anteriores propuestas y desarrollos enmarcados en el Proyecto Votescript. De forma especial quieren trasladar este agradecimiento a Ana Gómez Oliva, Sergio Sánchez García, José David Carracedo Verde y Jesús Moreno Blázquez.

Referencias

1. http://www.brunazo.eng.br/voto-e/textos/index.htm#portugues
2. http://www.cne.gov.ve/.
3. Mercuri R. Testimony presented to the U.S. House of Representatives Committee on Science. http://www.nist.gov/hearings/2001/votetech.htm.
4. Carracedo Gallardo, J. Seguridad en redes telemáticas. Madrid, McGraw-Hill, 2004. EAN 9788448141578.
5. Proyecto Votescript. http://vototelematico.diatel.upm.es/.
6. Hoyo de Pinares. http://vototelematico.diatel.upm.es/pag/pinares.htm.
7. Carracedo Gallardo, J. Gómez Oliva, A. Carracedo Verde, J.D. Sistema VOTESCRIPT: Una propuesta innovadora desarrollada para resolver los problemas clásicos de votación electrónica**,** Actas CIBSI '03. México DF. Servicio de Publicaciones del Instituto Politécnico Nacional, 2003. ISBN: 970-36-010409.
8. Gómez Oliva, Sánchez García, S. Pérez Belleboni, E. Electronic Voting: pg39-49.Contributions to Traditional Electronic Voting Systems in order to Reinforce Citizen Confidence. Bregenz, Austria : Robert Krimmer, 2006. ISBN 978-3-88579-180-5.
9. Pérez. Belleboni, E., Carracedo, J. trabajo tutelado. http://tsic.diatel.upm.es/docs/Trabajo _tutelado_Emilia.pdf
10. Portal oficial sobre el DNIe. http://www.dnielectronico.es