PLATAFORMA INDIVIDUAL DE VOTO ELECTRÓNICO

La Ley de acceso de los ciudadanos a los Servicios Públicos establece el derecho del ciudadano a relacionarse con las Administraciones Públicas por medios electrónicos, y por tanto establece también la obligación de éstas de proveer los medios necesarios para un ejercicio fácil, eficiente y seguro de ese derecho.

Lógicamente esta ley deja fuera de su ámbito de aplicación el voto electrónico al no considerar afectada por ella a la Administración Electoral, competente en esa materia. No podría ser de otra manera, ya que ésta es una ley ordinaria y la Ley Orgánica del Régimen Electoral General, que desarrolla tanto el derecho de sufragio, comprendido en el artículo 23 de la Constitución, como la existencia y funcionamiento de la Administración Electoral, es una ley orgánica y por tanto superior en rango.

Sin querer, ni poder, entrar en el terreno de juristas o de representantes políticos, y considerando que una de las relaciones más importantes que establecen los ciudadanos con una Administración es la del ejercicio del derecho de sufragio, piedra angular de nuestro estado democrático de derecho, éste tendrá que ser, antes o después, un aspecto básico en el desarrollo de la Administración Electrónica, aunque como ya se ha dicho, aún no esté contemplada ni su existencia ni su posible implementación en la normativa en vigor.

De hecho la LOREG, que se aprobó el 19 de junio de 1985, y ha sido modificada por otras leyes orgánicas posteriores, no recoge más procedimientos de voto que los que se refieren al voto ordinario en mesa electoral, el voto por correo y el voto de los residentes ausentes, dejando sólo un pequeño margen al Gobierno para proveer otros procedimientos, refiriéndose a este último tipo de votantes, en el apartado 6º del artículo 75.

Sin embargo, parece que la opinión general, incluida la muy importante de la Junta Electoral Central, es que para regular esta forma de voto es imprescindible modificar la ley orgánica, lo que, como es fácil imaginar, no resultará fácil, por lo que habrá que esperar aún algún tiempo para que la normativa contemple este aspecto.

Así las cosas, dejando de lado algún aspecto de gran importancia, como puede ser la necesidad de registrarse o no para ejercer este tipo de voto, y centrándonos en los aspectos más técnicos del mismo, lo primero y más señalado que hay que recordar son las características fundamentales que debe tener el voto y que la Administración competente debe asegurar: en primer lugar la unicidad, artículo 4 apartado 2 de la LOREG, que obliga al mantenimiento de un censo de votantes y a que estos se identifiquen adecuadamente antes de votar, y en segundo lugar, pero no menos importante, el secreto, artículo 86 apartado 1 de la LOREG, para cuyo mantenimiento hay que poner los medios necesarios de forma que el votante ejerza su derecho con la seguridad de que la opción que elige no puede ser conocida más que por él mismo.

Asimismo conviene aclarar que cuando nos referimos al voto electrónico en este artículo, no estamos hablando de ninguna de las formas de voto electrónico que exigen la presencia del votante en un centro u oficina electoral dispuesto al efecto y controlado por la Administración competente, sino al que se podría efectuar en lugar indeterminado, sin control de esa Administración, usando para ello equipos y medios accesibles al votante sin más trámite, ya sea en su casa, en su trabajo o en cualquier lugar donde pueda obtenerse acceso telemático a una aplicación centralizada de voto, ésta sí, dispuesta al efecto por la Administración.

Sólo a efectos de comparación, diremos que en las formas de voto electrónico presencial, ya sea la de apariencia tradicional con papeleta con la opción elegida codificada y legible electrónicamente y una urna con los elementos necesarios para realizar la lectura de las papeletas en el momento de su introducción en ésta, o la más conocida, basada en mecanismos en los que el ciudadano elige la opción de su preferencia en un equipo informático ubicado en una oficina o centro de votación controlado por la Administración, que le presenta todas las opciones posibles en una pantalla, el secreto del voto deberá asegurarse por los mismos métodos que en la votación tradicional, aunque la posible necesidad de ayuda por parte de representantes de la Administración para el uso correcto del equipo de votación puede complicar este aspecto.

En estos casos, la identificación del votante, el otro elemento fundamental del ejercicio del derecho al voto, puede producirse, o por los procedimientos tradicionales con documentos impresos, o por medio de certificados electrónicos en tarjetas dotadas de chip criptográfico, preferentemente el DNI electrónico, para lo cual la urna, o algún otro elemento auxiliar, debe estar preparado para leer ese tipo de tarjetas y verificar la identidad del votante.

En la forma de voto electrónico no presencial, se necesitan tres componentes principales: un servidor central, de colegio, zona, circunscripción o general, un servicio de comunicaciones y un terminal de votante. Para éste último se utilizará cualquier dispositivo capaz de presentar de forma clara y ordenada las opciones a elegir, con capacidad para transmitir datos, y dotado de medios para la identificación fehaciente del votante. Es decir, habría que disponer de un ordenador personal con conexión a Internet, o un teléfono móvil que incorpore tecnología de transmisión de datos, y ambos con medios para la lectura y gestión de certificados digitales.

Estos dispositivos serían el soporte de un cliente que, por medio de una conexión con un servidor de voto, permitirá elegir entre las varias opciones políticas de forma secreta y segura. El procedimiento que se basa en estos principios de funcionamiento es el que podríamos llamar voto por Internet, quizá el que podría ser considerado plenamente de Administración Electrónica.

Al igual que en los procedimientos presenciales, éste presenta sus principales problemas de implementación en lo que se refiere a la identificación del votante y el secreto del voto, pero enormemente amplificados, ya que este voto se produce en ubicación desconocida y con comunicaciones y equipos cuya seguridad no está controlada, pudiendo ser modificados la identidad del votante y el sentido del voto por la actuación de agentes como virus, troyanos, etc. inoculados al efecto en el equipo por los procedimientos habituales en Internet.

Al decir esto no se pretende quitar importancia a la implementación y aseguramiento del servidor o servidores centrales de voto, asunto que consideramos también muy importante y comprometido. Pero mientras estos componentes centrales se desarrollarán y funcionarán bajo el control de la Administración competente, los medios locales de voto electrónico sólo estarán

controlados por el propio votante, que en la mayoría de los casos no tendrá ni los conocimientos ni los recursos para asegurarse un medio de votación libre de problemas o compromisos como los señalados anteriormente, lo cual les hace muy vulnerables.

Para tratar de estudiar a fondo esta problemática del equipo local o individual de voto, la Subsecretaría de Interior solicitó y obtuvo financiación, a través del Plan Avanza, para poner en marcha los trabajos para implementar una plataforma de voto individual que pudiese ser entregada al votante para el ejercicio seguro del voto por Internet. En esta primera aproximación sólo se consideró el voto a través de un ordenador personal, dejando para otro momento el estudio de estos mismos problemas en equipos de mano como teléfonos móviles, PDA, etc.

El proyecto, al cual denominamos PIVE (Plataforma Individual de Voto Electrónico), quería alcanzar dos objetivos básicos:

- Asegurar que la persona que quiere realizar la votación de forma no presencial es quien dice ser, y

- Asegurar que todos los procesos ubicados en el equipo del votante e implicados en el acto del voto, están completamente aislados y protegidos de posibles problemas de seguridad de ese equipo.

El proyecto, tuvo una primera fase en 2006, de la cual se obtuvieron los siguientes productos:

- Un prototipo operativo de la plataforma individual de voto en CD-ROM

- La especificación detallada de las configuraciones de ordenadores personales sobre los que podría desplegarse

- La cobertura que estas configuraciones representan en cuanto a ordenadores personales instalados en España

- Un análisis de los riesgos de la plataforma desarrollada, y

- Una serie de recomendaciones sobre nuevos trabajos y enfoques para mejorar tanto la plataforma como la logística necesaria para su distribución.

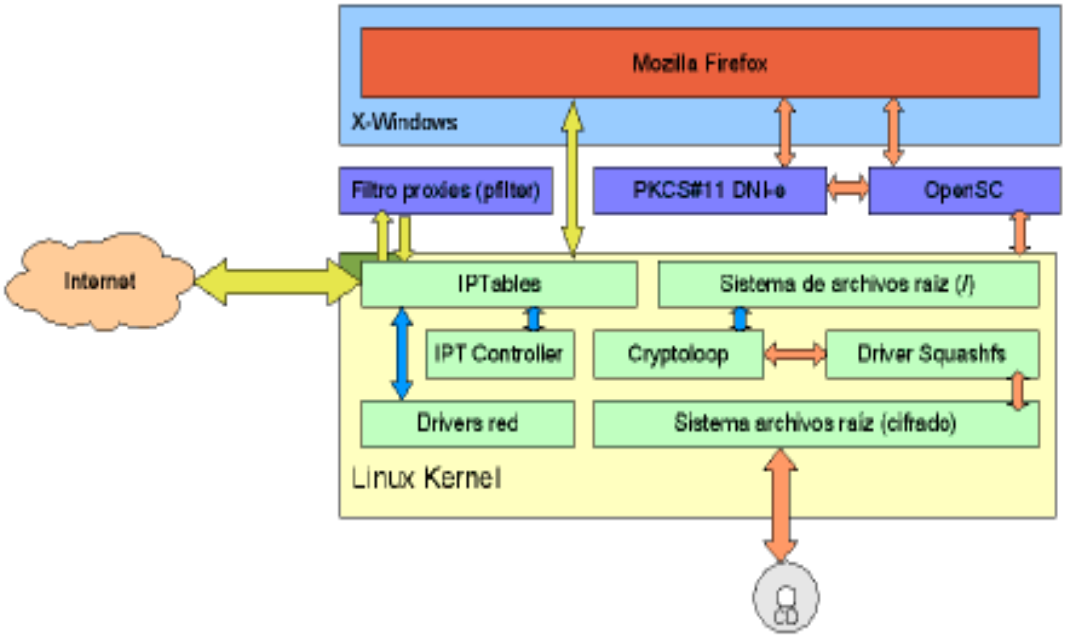
Para ello se procedió a crear una plataforma con las siguientes requisitos:

- Que sea un entorno seguro, portable y autocontenido que pueda ejecutarse sobre cualquier ordenador personal.
- Que permita usar el DNI electrónico para garantizar la autenticación del ciudadano de forma unívoca.
- Que tanto la configuración del kernel que sustenta el sistema, como la configuración específica de navegación del usuario sean seguras.
- Que incluya además de sistemas de cifrado del software, todos los posibles mecanismos internos de seguridad.

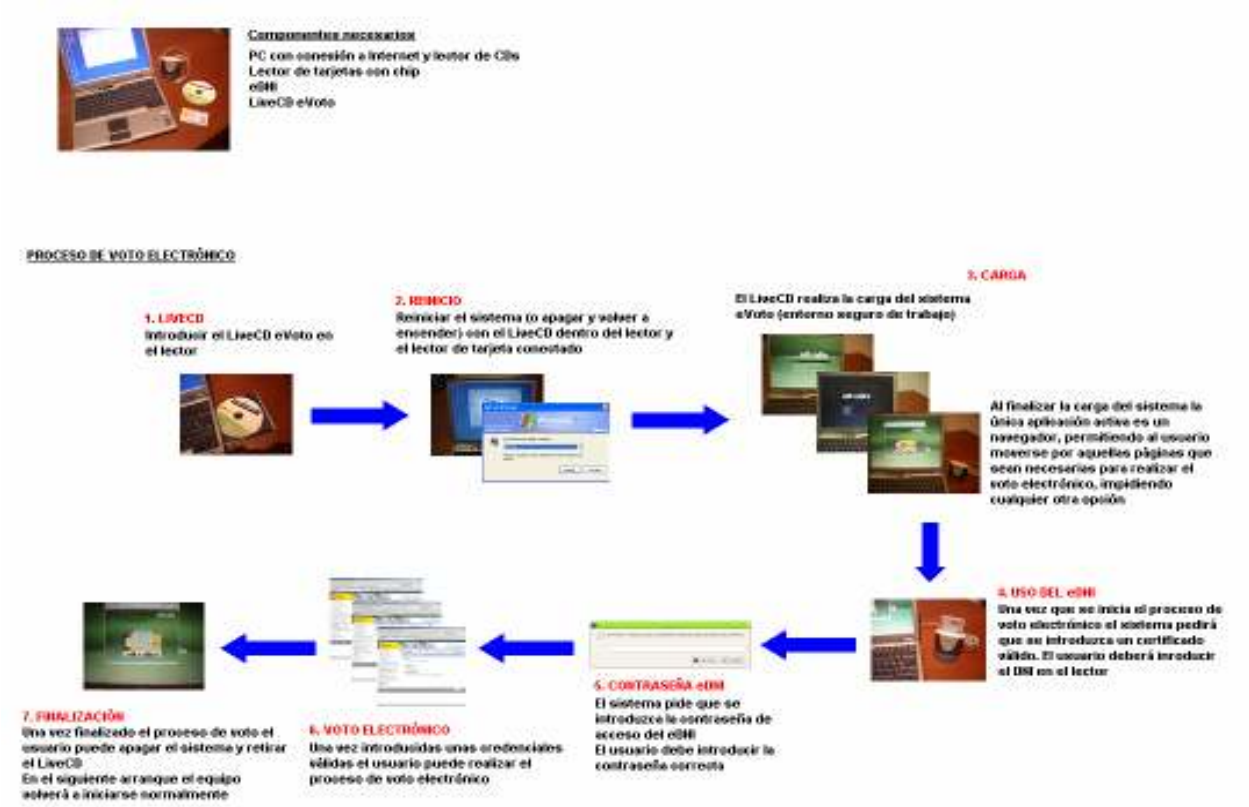
Al finalizar los trabajos se dispone de un sistema con las siguientes características:

- Desarrollo sobre la distribución Linux Ubuntu 6.06 (“Dapper”), una de las distribuciones con mayor compatibilidad con el hardware estándar.
- Permite al usuario autenticarse, mediante el uso del DNI electrónico, introduciendo el PIN de acceso y dejando a la parte servidora la comprobación de la validez de los certificados almacenados en éste.
- La información almacenada en el soporte es privada, impidiendo su lectura o utilización por quién no esté autorizado. Para ello se mantiene toda la información del soporte cifrada, excepto lo estrictamente necesario para poder iniciar el sistema de autenticación previo al arranque (PBA).
- Está preparado para que no se puedan realizar accesos como administrador, de forma que el usuario o el potencial *atacante*, no puedan realizar modificaciones en el sistema.
- No usa ningún sistema de DNS para acceder a Internet y tiene limitadas las direcciones IP a las que puede conectarse.

El esquema lógico de la arquitectura del sistema es el siguiente:



El proceso de voto electrónico se efectuaría como sigue:



En cuanto al grado de universalidad de la solución obtenida, partiendo del conjunto de marcas y modelos de los componentes hardware probados, cuyos drivers se alojan en el CD-ROM, se realizó un estudio sobre el parque de ordenadores vendidos en España en los últimos 5 años, llegándose a la conclusión de que la cobertura está en torno al 80% de los equipos de sobremesa o portátiles que los españoles usan en casa o en el trabajo, con lo que ésta puede considerarse una de las características más importantes de la solución obtenida.

Como ya se ha dicho, en este mismo proyecto se realizó un análisis de riesgos mediante la herramienta PILAR (Procedimiento Informático y Lógico de Análisis de Riesgos), centrándose en aquellos riesgos que afectan al puesto de votación, al CD-ROM y su medio de distribución, así como al intercambio de información. Los puntos más vulnerables resultaron ser:

ACTIVO	AMENAZA	RIESGO
Software LiveCD	Manipulación de programas	5
Software LiveCD	Difusión de software dañino	5
Software LiveCD	Suplantación de la identidad del usuario	5
Software LiveCD	Manipulación de la configuración	5
Software LiveCD	Alteración de secuencia	5
Software LiveCD	Errores del administrador	5
Software LiveCD	Vulnerabilidades de los programas	5
Software LiveCD	Errores de los usuarios	5
Software LiveCD	Abuso de privilegios de acceso	5
Software LiveCD	Acceso no autorizado	5
Software LiveCD	Errores de configuración	5

Como puede verse las principales amenazas identificadas se encuentran en la aplicación cliente de voto electrónico y su entorno, así como en el canal de distribución, punto éste último a estudiar en próximas fases del proyecto.

Finalmente, de este trabajo pudimos extraer una serie de objetivos para una segunda fase del proyecto que estamos a punto de afrontar:

- Optimizar el sistema desarrollado en aspectos como el tamaño o la eficiencia del arranque, firma de las aplicaciones que lo forman, acceso a parámetros de configuración.
- Estudiar y desarrollar distintas alternativas para la mejora de la seguridad del sistema, incluyendo la utilización de sistemas criptográficos de terceros.
- Estudiar y desarrollar alternativas para la personalización del sistema utilizando los certificados del votante.
- Acometer la problemática de la distribución masiva de la solución estudiando, entre otras, una posible distribución telemática.
- Implementar y probar el uso de otros soportes, distintos del CD-ROM, para la solución.

Autores

Manuel Martínez Domínguez
Subdirector General del Centro de Sistemas de Información
Subsecretaría de Interior

Antonio José García de la Paz
Subdirector General Adjunto del Centro de Sistemas de Información
Subsecretaría de Interior