tecnimap 2002
www.tecnimap.com
VII JORNADAS SOBRE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA MODERNIZACIÓN DE LAS ADMINISTRACIONES PÚBLICAS
A CORUÑA
15, 16, 17 y 18 de octubre de 2002
Palacio de Congresos y de la Ópera
Ponencias

Procedimiento de Voto Electrónico implementado para el Cuerpo de la Guardia Civil

Gonzalo Quiles Albert

Consultor de Indra Sistemas S.A.

Ingeniero Superior de Telecomunicación por la ETSET de Barcelona, perteneciente a la Universidad Politécnica de Cataluña

1 Introducción

El Avance de las nuevas tecnologías, a medida que penetra en la vida cotidiana, está propiciando cambios en casi todos los niveles de la sociedad. La aplicación de estas tecnologías a un proceso electoral (público o privado) resulta un evento especialmente atractivo, si bien no sencillo, dado las importantes implicaciones que tiene en una actividad de tanta repercusión social.

En el caso que nos ocupa, Indra Sistemas se ha encargado de realizar el sistema empleado por el cuerpo de la Guardia Civil para la elección de los vocales del recién inaugurado Consejo Asesor de Personal. La relevancia de este proyecto es notable, dado que se trata del primer caso de Votaciones electrónicas para un estamento oficial realizado en nues-

tro país y una de las primeras en el mundo. De esta forma, Indra se coloca en una privilegiada posición para el futuro en un mercado, el de Procesos Electorales, en el que ya actuaba como líder destacado.

La incertidumbre y recelos que cualquier proceso informático provoca, dada la común falta de conocimientos por el público en general, es el principal escollo a salvar en un proceso electoral electrónico. De esta forma, a la hora de poner en práctica el presente proyecto las características fundamentales que se han tenido en cuenta han sido la seguridad y la fiabilidad del sistema. Técnicamente, el proceso electoral implantado está completamente informatizado y hace uso de la Intranet de la Guardia Civil para las comunicaciones internas de los Sistemas.

2 Planteamiento

Definimos un proceso electoral electrónico como unas elecciones en las que los votos son introducidos a través de un sistema informático y almacenados digitalmente hasta el fin del periodo hábil de voto, momento a partir del cual se realizará el escrutinio automatizadamente.

El procedimiento de voto es la parte de un proceso electoral electrónico que determina la arquitectura general del sistema, define los flujos de intercambio de información entre los sistemas que intervienen y delimita algunas de las prestaciones intrínsecas a un proceso electoral más importantes.

El proceso electoral planteado por la Guardia Civil para formar el Consejo Asesor de Personal definido en la resolución dictaminada por el Director del Cuerpo, finalizaba con la definición de los integrantes del consejo asesor y su posterior instauración como órgano.

El proceso electoral está dividido en dos fases, unas primeras elecciones en las que los electores eran todos los miembros de la Guardia Civil, del orden de 85.000 (se tenían en cuenta los miembros en activo y de la reserva de todas las escalas y comandancias) y los candidatos tenían que presentarse explícitamente de entre el electorado. De esta primera vuelta electoral surgieron los compromisarios (unos 450) que en una segunda vuelta electoral eligieron a los vocales y suplentes del consejo asesor.

Las funcionalidades que estas características provocaban requerían un diseño de aplicaciones flexible, de forma que el mismo sistema sirviera para realizar una segunda elección con nuevos datos de entrada de forma sencilla y eficiente.

Para el proceso electoral, se han realizado una serie de aplicaciones encargadas de:

- Gestionar el censo electoral (altas, bajas, informes, solicitud y tramitación del voto por correo, etc.)
- Gestionar los candidatos de la primera vuelta (solicitudes, aprobaciones, difusión en la Intranet de perfil y propaganda, etc.).
- Gestión del proceso electoral, concretamente las fases por las que éste iba pasando: apertura de urnas, cierre de urnas, descifrado, introducción de votos por correo, escrutinio, recuento y presentación de actas electorales).
- Aplicaciones de voto, todas aquellas que mecanizan la ejecución del voto, el almacenamiento y su posterior recuento.
- Presentación general de actas y resultados electorales.

En este artículo se entra a describir el procedimiento electoral y las medias de seguridad que en torno a él se han empleado. En cuestión de aplicaciones desarrolladas, el estudio se limita aquellas que tienen un componente técnico más elevado y novedoso, que son las que tienen directa relación con la fase del proceso electoral en la que el voto es llevado a cabo, es almacenado en la urna electrónica y es posteriormente contado. El estudio hace especial hincapié en la arquitectura, metodología y seguridad del procedimiento de voto implementado.

2.1. Características del voto electrónico

Las características que las nuevas tecnologías y una red de comunicaciones avanzada (privada o pública) aporta a un proceso de electoral se puede resumir en los siguientes conceptos:

- Velocidad tanto de gestión previa como de escrutinio.
- Economía de medios a la hora de recoger o difundir datos electorales y votos.
- Movilidad, permite el voto desde cualquier lugar habilitado para votar, sin importar a qué circunscripción perteneces.
- Conveniencia, que facilita el voto a personas con disfunciones físicas.

Las prestaciones en términos de seguridad de un procedimiento de Voto que se han cubierto con el sistema desplegado son las siguientes:

- Confidencialidad: La información viaja y se almacena secretamente. En el caso de una votación se puede concretar en que la votación realizada y enviada no podrá ser espiada por terceros.
- Autenticación: Ambos interlocutores tienen la certeza de que el otro es quien dice ser, es decir, en nuestro caso la identificación inequívoca del votante y del sistema de voto.
- Integridad de contenidos: Es detectado si la información enviada es manipulada por un tercero. Es decir, el voto recibido y almacenado es el mismo que el que fue enviado.
- No Repudio: Las partes de una comunicación pueden probar la participación de la otra. Que en una votación se traduce a que no se puede negar el envío de un voto por parte del votante.
- No trazabilidad Voto-Votante: No se puede asociar el voto al votante.

Como tecnología de apoyo, importante para la seguridad del sistema, se ha empleado una Infraestructura de Clave Pública (PKI) basados en Algoritmos Criptográficos de pareja de Clave Pública – Clave Privada.

Esta Infraestructura de Clave Pública incluye una Autoridad de Certificación de carácter general encargada de emitir Certificados Digitales para los sistemas y los votantes involucrados en el Proceso Electoral.

2.2. Alternativas en el procedimiento de voto

Como se comentaba en la introducción, los recelos que produce la paulatina introducción de la informática en elementos relevantes y cotidianos de nuestras vidas, como tramitaciones oficiales, declaración de la Renta por Internet o la banca por Internet, es importante. Con respecto a un proceso electoral elecciones por Internet (o cualquier tipo de red de comunicaciones telemática, pública o privada), desde hace ya bastantes años, fundamentalmente en la década pasada, se han desarrollado numerosos procedimientos con la intención de resolver los problemas intrínsecos que unas elecciones electrónicas pueden acarrear.

En la actualidad los métodos de votación electrónica siguen dos tendencias claramente marcadas:

- Voto basado en una única conexión al sistema. La principal característica de este procedimiento es que tanto la identificación del votante como el envío del voto se realiza frente al mismo sistema. La garantía de no trazabilidad voto-votante se basa en la diversificación de identidades y funcionalidades en el sistema, apoyada por la entrega de la responsabilidad de descifrado de votos a la Junta Electoral únicamente. Esta diversificación de funciones combinada con un cifrado asimétrico del voto, posibilita que la parte del sistema encargada de identificar al votante no tenga acceso al contenido del voto.

- Se trata de un sistema que se apoya en la sencillez de la arquitectura empleada, fiable y apropiado para grandes votaciones, dado que reduce los puntos de fallo del sistema.

- Sistemas basados en Firma Ciega: Su principal característica es que garantizan la no trazabilidad voto-votante mediante criptografía implementada en el puesto cliente de voto, no recayendo esta responsabilidad en el sistema que ofrece el servicio. Se trata de un procedimiento interesante que aun así se toma con una serie de elementos en contra, como son una mayor complejidad del sistema, una operativa de voto más compleja de cara al votante y el hecho de que la no-trazabilidad, resulta vana si no se implementa verificabilidad por parte del votante y, por lo tanto recibo de voto.

- La verificabilidad y el recibo de voto conllevan una serie de inconvenientes:

    - Dificultades técnicas a la hora de implementar el recibo, puesto que ya sea en forma de papel, archivo informático o cualquier otra forma, en cualquier caso debilita la fiabilidad del sistema, sobretodo en elecciones a gran escala.

    - El abrir una fase de verificación al votante habilita posibles 'ataques de procedimiento' en el periodo de reclamación.

    - Por último y lo más importante, el recibo de voto que permite comprobar al votante que su voto fue contabilizado correctamente posibilita la coacción al votante por parte de un tercero o la venta del voto, dado que puede demostrar a una tercera parte cual fue su voto.

    Por debajo del procedimiento de voto, la seguridad del proceso electoral se distribuye en una serie de ámbitos comunes independientes de los diferentes procedimientos planteados, que hemos agrupado de la siguiente forma:

- Infraestructura de Clave Pública.

- Hardware Criptográfico.
- Otros elementos de seguridad.

A continuación se realiza una descripción del procedimiento de voto y aplicaciones desplegadas, así como de los otros elementos de seguridad implicados. Posteriormente, se lleva a cabo una evaluación, punto por punto de cómo el sistema desarrollado garantiza las premisas de seguridad que acabamos de describir.

3 Procedimiento del voto

El procedimiento de voto determina las características en cuestión de prestaciones y seguridad del proceso electoral. En el proceso electoral implementado para la Guardia Civil se ha empleado el mecanismo con una única conexión al sistema, por decisión del cliente y basado en una mayor simplicidad del sistema y de la operativa por parte del votante.

El procedimiento de voto empleado se basa en un sistema central al que se conectan mediante red telemática las estaciones de voto remotas. Este sistema se encarga de realizar la identificación del votante, comprobar que está en el censo, recibir los votos y realizar el recuento de votos. A su vez, la estación remota de voto, debe cifrar el voto, firmar una prueba de voto y enviar ambas elementos al sistema central.

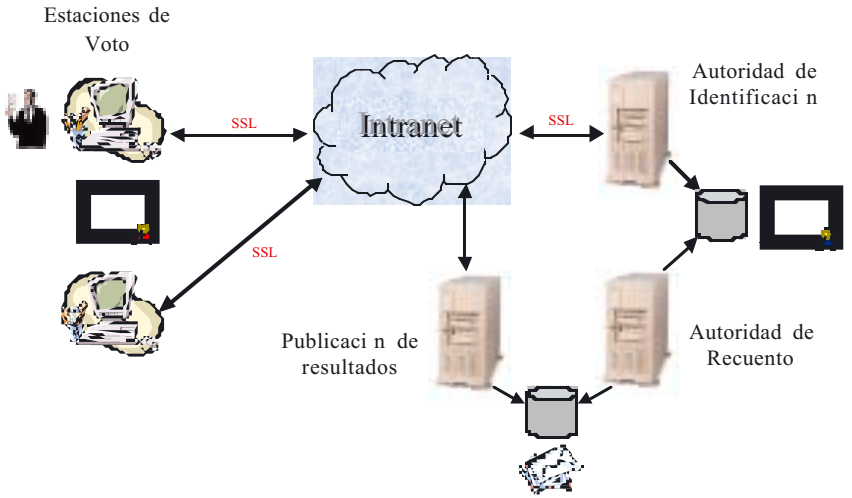
El procedimiento de voto implantado se basa en identificación mediante Firma Digital y Cifrado de datos, todo ello basado en Certificados expedidos por una Autoridad de Certificación de dominio público. Si bien en este caso se han utilizado certificados personales contenidos en tarjeta inteligentes para la identificación personal de los votantes, el sistema es compatible con otro tipo de identificaciones como por ejemplo, usuario y contraseña o identificadores biométricos, debido a su modularidad.

Dada la importancia de garantizar la no trazabilidad del Votante a partir del voto en el proceso electoral, el procedimiento de voto planteado se ha diseñado para ofrecer esta garantía. Esto se consigue (además de por numerosas medidas complementarias de seguridad) mediante la disociación de los papeles de identificación y de recuento en el Sistema Central, de la forma siguiente:

- Autoridad de Identificación: Comprueba la validez de los votantes mediante sus Certificados y su inclusión en el Censo Electoral. Conoce la identidad de los votantes pero no puede leer los votos.
- Autoridad de Recuento: Se encarga del Descifrado y recuento de los votos. Recibe los Votos Cifrados pero nunca conoce la Identidad de los votantes.

Cabe resaltar que el proceso de voto se ha implementado como un servicio Web, que garantiza la universalidad y reutilización del código generado.

El esquema general del sistema es el siguiente:



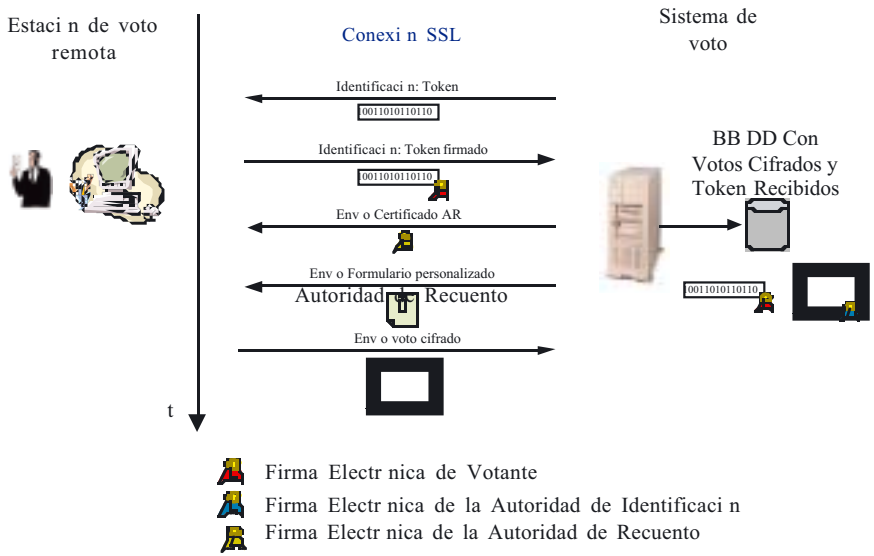
Esquema general de la arquitectura

Fases en el Procedimiento de voto

Como paso previo al comienzo del proceso de voto es necesario realizar la ceremonia de inicialización de la Autoridad de Recuento (AR). En esta ceremonia se generan las claves privada y pública de la AR y se distribuye su secreto, en forma de Tarjeta criptográfica, entre los diferentes representantes de la Junta Electoral. De esta forma sólo mediante

la participación de K de los N representantes (K y N son configurables) se puede acceder a la clave privada correspondiente al certificado de la AR que es imprescindible para descifrar los votos. Posteriormente a esta ceremonia será necesario que la Autoridad de Certificación genere el certificado correspondiente a la AR. Debe quedar claro que la responsabilidad final en los términos de seguridad planteados y con especial hincapié en la no trazabilidad, recae sobre los responsables de la Junta electoral, ya que únicamente ellos podrán habilitar el acceso a la clave privada del certificado de la AR y, por lo tanto, al descifrado de los votos.

El esquema general del procedimiento de voto que será descrito más adelante es el siguiente:



Esquema de intercambio de información entre Estación de voto y Sistema de voto

Teniendo en cuenta que el votante dispone de un certificado, el procedimiento de voto se divide en las siguientes fases:

• **Ejecución del Voto por parte del Votante.**

Una vez puesta en marcha la Votación, el acto de ejecución del voto se realiza mediante una conexión segura (SSL) a la Autoridad de Identificación vía protocolo https, que implica los siguientes pasos:

- Acceso al servicio Web.
- Identificación del usuario mediante su Certificado Digital. Para identificarse, el votante firma digitalmente un token que se guardará y puede utilizarse como prueba de acceso al sistema.
- Recepción del Certificado correspondiente a la Autoridad de Recuento.
- Recepción de las papeletas de voto personalizadas, a rellenar.
- Selección del Voto.
- Cifrado del Voto mediante el Certificado recibido de la Autoridad de Recuento.
- Firmado del voto cifrado por el votante.
- Envío del Voto Cifrado y firmado.

En los terminales remotos de voto (PCs conectados a la Intranet de la Guardia Civil) el dispositivo de creación del mensaje criptográfico que encapsula al voto está implementado mediante un applet.

Este applet está firmado digitalmente utilizando un certificado de firma de código (mediante tecnología "authenticode") emitido por la FNMT a nombre de la Guardia Civil.

La firma de este applet garantizará el origen del software, evitando código malicioso o virus y otorgará a dicho applet los permisos necesarios para su ejecución.

• **Procesado del Voto por la Autoridad de Identificación.**

La Autoridad de Identificación realizará los siguientes pasos:

- Identificación del votante mediante la comprobación de su firma sobre el token enviado.

- Comprobación de que el votante no ha ejercido ya su derecho al voto.

- Recepción del voto cifrado y firmado por el votante.

- Verificación y retirada de la firma del votante del voto cifrado.

- Firma por la Autoridad de Identificación del voto cifrado.

- Almacenamiento del token firmado por el votante como prueba de acceso y del voto firmado por la AI.

La Autoridad de Identificación esta implementada en Java utilizando el J2SE de Sun y librerías que implementan el procesamiento de los formatos CMS (PKCS7) sobre plataforma Unix (Solaris). Al igual que el código de la estación de voto, esta implementación la caracterizan como ampliamente reutilizable en futuros desarrollos similares.

- **Recuento del Voto por la Autoridad de Recuento.**

Una vez finalizado el plazo de la votación, el Administrador de Recuento lleva a cabo las siguientes acciones:

- Apertura de la clave privada del certificado de la Autoridad de Recuento mediante una combinación de usuarios K de N. Lo cual implica que se necesitan K usuarios de N totales. Este mecanismo está implementado automáticamente por el Hardware Criptográfico encargado de custodiar la Clave privada de la Autoridad de Recuento.

- Recuperación de los votos cifrados, firmados y almacenados por la Autoridad de Identificación. Comprobación de validez del certificado de la Autoridad de identificación empleado en la firma del voto. Verificación de la firma de la Autoridad de Identificación.

- Descifrado de los Votos haciendo uso de la clave privada del certificado de la Autoridad de recuento.

- Realización del Conteo de Votos Válidos y depósito del resultado en una tabla donde serán añadidos los votos por correo recibidos una vez recontados.

Es importante resaltar que la información que la Autoridad de Recuento recibe de la Autoridad de Identificación es únicamente los votos cifrados y firmados por la Autoridad de Identificación.

De igual forma que la Autoridad de Identificación, la Autoridad de Recuento esta implementada en Java utilizando el J2SE de Sun y librerías que implementan el procesamiento de los formatos CMS (PKCS7) sobre plataforma Unix (Solaris).

- **Publicación de resultados por una aplicación Web.**

  Finalmente mediante un servicio de Web se difunden los resultados del proceso electoral.

4 Elementos que intervienen en la seguridad del proceso

A parte del procedimiento de voto, existen una serie de elementos que de una forma u otra intervienen en el proceso electoral en cuestiones de seguridad, fiabilidad y robustez. Estos elementos son los siguientes:

4.1. INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

El procedimiento de voto implementado apoya su seguridad en los certificados emitidos por una Autoridad de Certificación que es la tercera parte de confianza y forma parte de una Infraestructura de Clave Pública (PKI). Esta Autoridad de Certificación es la que garantiza la autenticidad de las identidades contenidas en los certificados digitales.

Concretando, en el presente proyecto el primer paso a realizar por el Votante es la obtención del certificado digital de una autoridad certificadora propia o ajena previamente concertada. En nuestro caso, teniendo en cuenta la compatibilidad del sistema desarrollado, la Guardia Civil escogió como Autoridad de Certificación desplegada por la Fábrica Nacional de Moneda y Timbre mediante el proyecto CERES. Las practicas de Certificación implantadas en el proyecto

CERES garantizan un Certificado de forma avanzada reconocido internacionalmente hablamos de un certificado de Clase 2 X.509 v3 soportado en Tarjeta Criptográfica de 32k.

Además de los certificados de usuario, la CA de la FNMT se encargó de emitir los certificados de servidor, tanto para la Autoridad de Identificación (firma de código y establecimiento de conexión SSL) como para la Autoridad de Recuento (cifrado de votos).

4.2. HARDWARE CRIPTOGRÁFICO (módulo HSM)

A medida que la criptografía de clave pública ha ido consolidándose como base de la seguridad informática, el punto débil de la seguridad ha ido desplazándose desde los datos en sí hacia las claves que los protegen. Los datos solo son seguros en la medida en que lo sean dichas claves. Para solucionar el problema, es posible utilizar productos que almacenan las claves con la debida seguridad, en el interior de módulos hardware (HSM), protegidos y fiables. Adicionalmente, es necesario un proceso de control del ciclo de vida de las claves protegidas por el HSM para lo que se requiere un software que actué como interfaz entre el HSM y el mundo externo.

En la máquina que hace las funciones de Autoridad de Recuento se ha implantado un módulo hardware de seguridad (HSM) nShield F3-UltraSign del fabricante nCipher. El HSM se utiliza para la protección de la clave privada asociada a la clave pública utilizada por los usuarios para cifrar los votos, así como para la aceleración de los algoritmos criptográficos.

El HSM tiene unos administradores que gestionan la vida de las claves almacenadas y pueden iniciar un proceso de recuperación de claves en caso de desastre. Por otro lado están los operadores que poseen las tarjetas con el secreto de la clave privada distribuido y que son los operadores necesarios para hacer uso de la clave estos operadores son los individuos que forman la Junta Electoral del proceso electoral.

Inicialización del Recuento

Terminada la fase de votación, los miembros de la mesa electoral procederán a la apertura de la urna y el inicio del recuento de los votos, para lo que es necesario descifrar todos los votos cifrados de los usuarios. Para descifrar un voto, es necesario utilizar la clave de la Autoridad de Recuento, para ello, es necesario la presencia de KO operadores (miembros de la mesa) y la inserción de sus tarjetas inteligentes en el lector del HSM.

Cumplimiento de estándares

El HSM está validado conforme a lo establecido en la Norma Federal de Procesamiento de la Información (FIPS) 140-1 Nivel 3. Este nivel impide la exportación de claves fuera del sistema, por lo que la clave privada utilizada durante el cifrado de los votos es totalmente inaccesible.

El HSM tiene certificación del cumplimiento de las siguientes normas:

- FCC: CRFA47, Parte 15, Subparte B, Clase A
- CE: EN 55022 Clase A, EN 55024-1, EN 60950.

4.3. OTROS ELEMENTOS DE SEGURIDAD

Además de los elementos ya mencionados existen otros que complementan la seguridad y fiabilidad en el proceso de votación planteado.

- Alta disponibilidad: Todos los sistemas desplegados para llevar a cabo el proceso de votación están configurados en alta disponibilidad. Estos sistemas son los siguientes: cortafuegos, servidor web, base de datos y la Autoridad de Recuento.
- Base de Datos: Como medida de seguridad los usuarios de acceso a la BBDD se encuentran almacenados en ficheros cifrados a cuyo acceso sólo tienen acceso las aplicaciones de Identificación y Recuento. Como medidas adicionales se ha evitado la existencia de sellos de tiempos en el almacenamiento de datos y se ha Inhabilitado la traza de acciones tanto por Instancia como por sesión en la configuración de la Base de Datos.
- Seguridad de red: Dada la criticidad de la información manejada en el proyecto, se ha diseñado una arquitectura de red dividida en diferentes subredes separadas entre ellas por un sistema cortafuegos. Cada una de estas redes sufrirá un distinto grado de exposición y sólo los servicios y protocolos imprescindibles estarán visibles desde la Intranet.

- Seguridad física: Dado que la ubicación de los sistemas dedicados al proceso electoral se encuentran ubicados en las dependencias de la Guardia Civil, la responsabilidad sobre el acceso físico a estos sistemas quedará asumida por la seguridad que ya mantienen en la actualidad en el CPD.

5 Conclusiones

Como ocurre con otro tipo de aplicaciones, principalmente todas aquellas dedicadas a los sistemas de control en tiempo real, un proceso electoral informático resulta un sistema especialmente crítico y sensible a imprecisiones y eventualidades, dado que en el momento de puesta en producción, el sistema debe de estar funcionando al completo y sin posibilidad de errores. Puesto que no hay marcha atrás, las repercusiones de una inconsistencia del sistema pueden ser catastróficas.

Desde este punto de vista el equipo de desarrollo puso un espacial énfasis en la elaboración de pruebas previas a la puesta en producción movilizando en repetidas ocasiones al cuerpo de la Guardia Civil para simular procesos electorales.

En el ámbito de la robustez y fiabilidad del sistema, cabe resaltar que durante la implantación del sistema y previamente a la puesta en producción para la primera de las elecciones convocadas, se llevó a cabo una auditoría de seguridad encargada por la propia Guardia Civil. Esta auditoría fue llevada a cabo por a una tercera empresa independiente de la Guardia Civil y de Indra Sistemas S.A., de contrastada experiencia y solvencia, auditoría que el sistema superó sin inconvenientes y en la cual fueron revisados todos los elementos de seguridad concernientes a un proceso electoral por red de comunicaciones telemática.

En la actualidad están proliferando cada vez las iniciativas de voto por Internet, ante lo cual es necesario destacar comparativamente lo elaborado de los procedimientos y técnicas desplegados, la importancia del evento dada su oficialidad, el reto que este desarrollo ha supuesto para todo el equipo formado por técnicos tanto de Procesos Electorales como de Centros de Competencias y la recompensa que para todos ha supuesto el poder superar las dificultades que conllevaba.

Un proyecto como es la implantación de un procedimiento electoral electrónico posee un carácter estratégico fuera de toda duda, y resulta ser sólo el principio de una carrera para la que la sociedad poco a poco inexorablemente va a ir

acostumbrándose que es la introducción de las Tecnologías de la Información en nuestra cotidianidad. La pregunta a realizarse no es si será posible realizar unas elecciones por Internet en un futuro, sino cuando. En estos términos, a medida que las prestaciones en términos de seguridad y comunicaciones progresan, la introducción de dispositivos móviles como teléfonos móviles (con tecnologías WAP, GPRS, UMTS), teléfonos inteligentes con capacidad de navegación y soporte de aplicaciones JAVA y potentes PDA's con comunicaciones móviles, resulta desde luego, inevitable y de tremendamente atractiva.