(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 283 205**

(21) Número de solicitud: 200503260

(51) Int. Cl.:
G07C 13/00 (2006.01)
H04L 9/32 (2006.01)

(12) PATENTE DE INVENCIÓN CON EXAMEN PREVIO B2

(22) Fecha de presentación: **30.12.2005**

(43) Fecha de publicación de la solicitud: **16.10.2007**

Fecha de la concesión: **18.08.2008**

(45) Fecha de anuncio de la concesión: **01.09.2008**

(45) Fecha de publicación del folleto de la patente: **01.09.2008**

(73) Titular/es: **Ignacio Fernández Moreno**
c/ Cierzo, 28 - 3º D
28223 Pozuelo de Alarcón, Madrid, ES
Pablo J. González Granados y
Luis Marful Fernández

(72) Inventor/es: **Fernández Moreno, Ignacio;**
González Granados, Pablo J. y
Marful Fernández, Luis

(74) Agente: **Fuentes Palancar, José Julián**

(54) Título: **Sistema de votación telemática a través de Internet.**

(57) Resumen:
Sistema de votación telemática a través de Internet, realizado en un escenario de comunicación en el que intervienen un conjunto de sistemas automáticos que funcionan bajo unos programas predeterminados de sistema operativo, gestores de bases de datos, aplicaciones web y seguridad en Internet, constituido en su arquitectura básica por una Autoridad de Certificación, un Sistema de Anonimato, un Sistema de Voto, un Sistema de Recuento, un Sistema Verificador, una base de datos Relación Usuario-Identidad, una base de datos Universo de Votantes, y una base de datos Urna electrónica, además de las interconexiones y flujos de datos entre estos elementos. El sistema crea un proceso de votación totalmente electrónico y a distancia, aplicable de forma independientemente del lugar físico donde se encuentre el votante, rápido y de fácil utilización.

ES 2 283 205 B2

DESCRIPCIÓN

Sistema de votación telemática a través de Internet.

La presente invención se refiere a un sistema de votación telemática a través de Internet, es decir, un sistema de votación que emplea Internet como forma más universal de comunicación electrónica para conectar a los votantes, previamente autentificados, con un registro de opciones de voto y con una urna electrónica remota.

El sistema crea un proceso electoral totalmente electrónico y seguro en base a Internet, desde el lugar de la votación, un terminal de un ordenador personal, teléfono móvil u otro aparato electrónico que tenga acceso a la Red, hasta los dispositivos que acreditan la identidad de los votantes, con códigos de seguridad y autoridades de autentificación de fe pública, pasando por los sistemas de urna electrónica, de recuento y de verificación de votos, lo cual permite proporcionar un servicio de votación que es independiente del lugar físico donde se encuentre el votante, rápido y de fácil manejo, compatible con el sistema de votación tradicional en elecciones administrativas, pero a la vez, con capacidad de adaptación a cualquier normativa que rija un proceso electoral particular, entre otras muchas ventajas.

Esta invención, que se encuadrada en el campo técnico de la ingeniería y arquitecturas telemáticas, desarrolla un sistema de votación telemática que no se basa en un tipo de software específico, sino que simplemente se especifican las capacidades, funcionalidades y mecanismos de seguridad que debe tener el sistema, y en qué lugar y de qué modo debe utilizarse. Por tanto, puede que para una empresa pequeña, o incluso un colegio o reuniones de ciertas comunidades se pueda utilizar software de código abierto en la implementación, dado que es gratuito y, aunque no ofrece garantías, suele estar muy bien terminado en la mayoría de los casos, y para una gran empresa u organismo público se pueda realizar un sistema con los programas más caros y sofisticados.

Estado de la técnica

Se entiende por "voto electrónico" todos aquellos escenarios que basándose en los métodos clásicos de votación, sustituyen alguno de los elementos físicos y procedimientos manuales por algún tipo de sistema o procedimiento electrónico.

Los procesos a automatizar son los que se realizan comúnmente en el colegio electoral, pudiéndose sintetizar en tres: la autenticación del votante, el proceso de la emisión del voto, y el procesado del contenido de la urna electoral. Todos los componentes electrónicos utilizados en estos escenarios tratan de automatizar alguno de estos procesos, entrando en esta catalogación los sistemas que utilizan alguno o varios de los siguientes elementos: tarjetas magnéticas (para autenticar al votante o incluso para emitir el voto), urna electrónica (para la recepción y recuento de los votos), pantalla o tablero de votación (para seleccionar la opción de voto elegida), cabina electrónica (para garantizar la privacidad) y software de distintos tipos (para el proceso de escrutinio).

Sistemas basados en votaciones electrónicas del comentado tipo, es decir, realizadas en colegios electorales en los que algunos elementos físicos del procedimiento de votación tradicional es sustituido por algún tipo de proceso electrónico, están ampliamente desarrollados. De hecho, existe una gran variedad de patentes sobre esta cuestión, en las que incluso se reivindican los aparatos y dispositivos electrónicos para su puesta en práctica. Así, por ejemplo, patentes de este tipo con efectos en España son las nacionales con número de publicación ES2230994A1 "Sistema de votación electrónica", y ES2165289B1 "Sistema de votación electrónico y correspondiente papeleta evaluable opto-electrónicamente", o la patente europea con números de publicación ES2103730T3 "Nuevo proceso de voto y medios para su puesta en obra".

Algunas de las patentes se centran exclusivamente en los aparatos o dispositivos integrantes de un sistema de votación electrónica, como es el caso de las patentes nacionales ES2174753B1 "Urna electrónica" y ES8706988 "Perfeccionamientos en los aparatos electrónicos para la gestión automatizada de colegios electorales", o de los modelos de utilidad ES1053026U, "Urna rodante para sistemas de votación electrónica", y ES1050757U "Papeleta para sistemas de votación electrónico".

En un nivel más avanzado de sistema de voto electrónico se busca la realización del proceso de votación mediante el uso de las redes telemáticas, entrándose entonces en el denominado sistema de "Voto Telemático". En este caso, la urna no se encuentra a la vista del votante, lo que ocurre con el voto electrónico convencional antes citado, sino que es un agente telemático ubicado físicamente en un lugar remoto, al igual que el resto de los agentes que intervienen en la supervisión y realización del sistema.

Dentro del sistema de voto telemático se pueden distinguir a su vez dos subgrupos. El primero es el compuesto por aquellos sistemas que utilizan redes telemáticas para la interconexión de los distintos colegios electorales, efectuando el elector el voto desde el mismo colegio electoral o centro equivalente, lo que permite una recolección, recuento y publicación de los resultados casi inmediata, dejando al organismo encargado de la supervisión final la misión de identificar y autenticar a los votantes. El segundo subgrupo lo constituyen aquellos sistemas en los que la votación se realiza de modo remoto, típicamente a través de Internet, siendo más atractivo de cara a los votantes y permitiendo *a priori* una drástica reducción de costes, pero con la necesidad de establecer mecanismos de seguridad, identificación y autenticación mucho mayores.

Si bien dentro del primer subgrupo de sistemas de votación telemática, el realizado en colegios electorales a través de redes de ordenadores públicas de interconexión de centros, han sido publicados varios trabajos, entre los que cabe destacar el proyecto VOTESCRIPT de la Universidad Politécnica de Madrid, o algunos otros que han sido protegidos por patente en España, caso de la patente nacional número P200450051 "Método para la votación electrónica segura y protocolos criptográficos empleados", o las patentes europeas con número de traducción ES2158241T3 "Método y aparato para la transmisión segura de mensajes anónimos y votación electrónica segura" y ES2156594T3 "Método y aparato para votación electrónica segura", no se sabe de ningún proyecto publicado en relación con un sistema de votación telemática realizado en modo remoto, a través de Internet, es decir, sin necesidad de la presencia física del votante en el centro electoral en el momento de la votación.

Considerando que, en teoría, los componentes para el desarrollo de un sistema de voto telemático por Internet son bastantes sencillos: un registro de votantes, un registro de opciones de voto, y un sistema de contadores o urna electrónica, todo ello conectado a través de Internet, el que no exista hasta ahora un proyecto para su implantación práctica es seguramente debido a los exigentes mecanismos de seguridad que este sistema debe llevar asociado.

Téngase en cuenta, que para la implementación de un sistema de votación por Internet en el que los votantes puedan emitir su voto a distancia mediante, por ejemplo, un teléfono móvil, se requiere de mecanismos de seguridad, identificación y autenticación que afronten los siguientes problemas:

Definición del universo de votantes.- Uno de los primeros problemas es definir quién tiene derecho a voto y quién no. El sistema no sería admisible si tras la votación hubiese más votos que votantes.

Identificación unívoca de cada votante.- Una vez establecido el rango de votantes, hay que asegurar que cada usuario del sistema tiene una representación única en el mismo, de modo que no pueda haber suplantaciones de personalidad.

Autentificación del votante.- Este problema ya ha sido resuelto en el mundo del comercio electrónico.

Anonimato del votante.- El sistema no debe vincular un voto con el emisor del mismo, es decir, que no se pueda saber de ningún modo qué voto ha emitido un usuario determinado. Para ello se necesitan mecanismos de secreto en las comunicaciones, en la contabilidad y en la información de datos parciales.

Seguridad del sistema.- El sistema debe ser capaz de protegerse ante ataques externos, caídas y fallos en el software o en el equipo, etcétera.

Queda claro, pues, que el principal problema del voto telemático a través de Internet es a nivel de seguridad, más que a nivel de implementación del mismo.

Teniendo en cuenta este estricto marco de seguridad que debe rodear a un sistema de votación telemática a través de Internet, con el presente proyecto se presenta un modelo innovador que responde de la mejor manera posible a cada uno de los problemas planteados.

En su desarrollo se han tenido en cuenta todos los requisitos que debe cumplir un sistema de votación de estas características, relacionados con el universo de votantes, el proceso de votación, la seguridad del sistema y el recuento final de los votos, los cuales se relacionan a continuación.

a) Universo de votantes.- i) Definición del universo de votantes por la autoridad que solicite el proceso de votación, como fase previa al proceso de votación; ii) fragmentación de los datos, de modo que los datos del votante no queden incluidos en un mismo sistema; iii) una vez iniciado el proceso de votación, el universo de votantes no podrá ser alterado, sino sólo consultado; iv) los datos definidos en el universo de votantes podrá ser opcionalmente consultados por parte del usuario, siendo sólo posible la modificación de los mismos previamente al inicio del proceso de votación, a través de las autoridades competentes y según un proceso externo a la votación.

b) Proceso de votación.- i) El sistema deberá garantizar la libertad del voto, esto implica que el usuario deberá poder ejercer su derecho a voto desde cualquier terminal, independientemente del sistema operativo y del navegador, debe poder conocer *a priori* cualquier cuestión acerca de las elecciones, los candidatos, la metodología de voto, y los presupuestos e implicaciones de cada opción posible en una consulta dada, además el usuario deberá ser libre a la hora de votar o a la omisión del mismo, no es aceptable que se tomen votos por defecto; ii) el sistema deberá identificar unívocamente a los usuarios; iii) el sistema deberá garantizar la unicidad del voto, la imposibilidad de coacción de los votantes y el anonimato de los mismos; iv) el votante no podrá cambiar su voto una vez emitido el mismo; v) el sistema debe ser capaz de funcionar en condiciones adversas y ante posibles fallos; vi) la aplicación de cara al usuario debe ser transparente, accesible, amigable, intuitiva y fácil de usar.

c) Seguridad.- i) El sistema deberá tener mecanismos de autentificación, que garanticen la autentificación y certificación tanto de la máquina desde la que opera el votante como del servidor o servidores del sistema de votación, además de la verificación del sistema de voto; ii) se garantiza que el sistema funciona solamente como se prevé que va a funcionar, sin puertas traseras ni trampas ocultas que modifiquen los resultados; iii) el sistema debe proporcionar

mecanismos de seguridad específicos; iv) el sistema deberá proporcionar mecanismos de control de acceso al sistema, de modo de que sólo puedan acceder los usuarios autorizados en los momentos establecidos, v) el sistema deberá proporcionar a las autoridades competentes transparencia, es decir, se deberá: tener acceso al código fuente y a los registros de funcionamiento, obtener certificados de autenticidad por parte de terceros, presentar procedimientos de log que permitan resolver dudas e impugnaciones, manteniendo el carácter de secreto del voto; vi) se deberá definir una estrategia de seguridad que abarque los siguientes puntos: el plan de seguridad deberá tener una estrategia pro-activa, deberán realizarse inspecciones o auditorías legales para la certificación del sistema, políticas de seguridad explícitas (contra ataques externos e internos).

d) Recuento.- El sistema deberá tener mecanismos de recuento fiable que garanticen: i) la exactitud, es decir, que el número de votantes sea igual al número de votos; ii) la independencia, con respecto al proceso de votación; iii) la verificación global de los datos.

Compendio de la invención

La solución propuesta para que el sistema de votación telemática en Internet concebido cumpla con todas las anteriores exigencias y, por tanto, para que en la práctica pueda llevarse a cabo, pasa por una arquitectura formada por un conjunto de sistemas automáticos que funcionan bajo unos programas predeterminados de sistema operativo, gestores de bases de datos, aplicaciones web y seguridad en Internet.

Este conjunto de sistemas lo forman los siguientes elementos principales que más abajo se describen en detalle: a) Una Autoridad de Certificación en Internet, encargada de cifrar las comunicaciones y autentificar tanto al votante como al sistema de votación, b) un Sistema de Anonimato, encargado de presentar a los candidatos, controlar el acceso, garantizar el anonimato de los votantes y seguimiento de los mismos durante el proceso, c) un Sistema de Voto, encargado de recibir, gestionar y almacenar los votos emitidos de un determinado departamento, d) un Sistema de Recuento, encargado de contabilizar el número de votos, e) un Sistema Verificador, encargado de validar los comicios electorales, f) una base de datos Relación Usuario-Identidad, encargada de almacenar los datos del usuario, su identidad en el sistema y el estado de los votantes, g) una base de datos Universo de Votantes, encargada de establecer un rango de votantes del sistema, y h) una base de datos Urna electrónica, encargada de almacenar los votos emitidos por los votantes, además de las interconexiones y flujos de datos entre los anteriores elementos.

I. *Elementos del sistema*

a) *Autoridad de Certificación (AC)*

El sistema Autoridad de Certificación es el ente externo encargado de autenticar a través de Internet tanto al votante, mediante la asignación on-line de una clave personal para cada votante, como a las máquinas implicadas en el sistema de votación, mediante un proceso previo a la votación, además de mantener la confidencialidad e integridad de los datos gracias a la encriptación de las comunicaciones. Con ello, se puede garantizar que los extremos en las comunicaciones son quien dicen que son.

En la actualidad hay diferentes Autoridades de Certificación (VeriSign, Radius, Thawte, etc.) que implementan por defecto el cifrado SSL (Secure Socket Layer), que es el protocolo estándar mundial de la seguridad Web, diseñado y propuesto por Netscape Communications Corporation. Este proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico y cifrando la clave de sesión mediante un algoritmo de cifrado de clave pública. La clave de sesión es la que se utiliza para cifrar los datos que vienen del y van al servidor seguro. Se genera una clave de sesión distinta para cada transacción, lo cual permite que aunque sea reventada por un atacante en una transacción dada, no sirva para descifrar futuras transacciones.

En el presente caso se ha diseñado el sistema en base a Autoridades de Certificación de fe pública que utilicen el cifrado SSL, como empresas dedicadas a la emisión y comprobación de los certificados con contrastada capacidad para impedir la suplantación, dejando abierta la posibilidad de la utilización de certificados emitidos por la Administración Pública, ahora mismo en desarrollo, como ente de máxima confianza. Se debe tener en cuenta siempre que este tipo de Autoridades deben ser ajenas al sistema de votación y proporcionar un servicio con la suficiente profesionalidad, dependiendo de las necesidades de la implementación en cada caso.

Hay que dejar claro que este tipo de sistemas, pese a ser relativamente modernos, han dado muy buenos resultados a la hora de asegurar algo tan importante como las transacciones de dinero a través de la red, no solo en sitios de comercio electrónico, sino también en entidades bancarias de reconocido prestigio.

b) *Sistema de Anonimato*

En la proyección telemática del escenario de votación convencional, el sistema anonimato ha de garantizar que solamente depositan su voto en la "urna" las personas autorizadas para ello y que sólo votan una vez y por una sola opción.

En el proyecto abordado el Sistema Anonimato utiliza las siguientes tecnologías para la presentación de la información:

- Base XML (*eXtensible Markup Language*), con capacidad para empaquetar los datos en un formato que pueda validarse, como XML Schemas.

- Lenguaje XSLT (*Extensible Stylesheet Language Transformations*), que permite presentar la información contenida en los ficheros .XML en el lenguaje de programación que requiera el usuario (Html, C-Html, Wml), según a su dispositivo (PC, móvil i-mode, móvil-Wap).

Los módulos que componen el Sistema Anonimato son:

- *Gestión de Sesión*, encargado de personalizar la presentación de cara al usuario y crear un perfil (que se destruirá cuando el votante cierre la sesión) volátil del mismo, una vez validado en la base de datos Universo de Votantes, al inicio de la sesión, conteniendo los datos personales del mismo, pudiendo cambiar éstos por la Identidad en el Sistema cuando ésta se le asigne al usuario. También realiza la jerarquización de los usuarios, es decir, da más peso a unos votos que otros en función del perfil del usuario, si así se desea la entidad que solicita la votación.

- *Check Status*, encargado de comprobar el estado del votante en el sistema mediante dos verificaciones: primero, si se le ha otorgado una Identidad en el Sistema, y segundo si ha votado. Gracias a este módulo, en el caso de que haya un fallo en las comunicaciones, en una segunda conexión por parte del votante, una vez validada la sesión, se le dirigirá al punto en donde se quedó.

- *Check Universo de Votantes*, encargado de verificar que el usuario que se conecta al sistema pertenece al rango de votantes definido por la autoridad que solicita el proceso electoral. En caso afirmativo se creará la sesión, en otro caso se le denegará el acceso.

- *Generador de Identidades*, encargado de generar Identidades en el sistema, para preservar el anonimato de los Votantes. Estas identidades son números aleatorios, de tal modo que sea inviable poder establecer algún tipo de relación entre el votante y la identidad en el sistema. Para ello el generador utilizado será un Generador congruencial estándar, que debidamente ajustado por diferentes contrastes (X^2 Pearson, Rachas, Permutaciones y Huecos) se aproximará a una Distribución Uniforme.

- *Inserción de Identidad*, encargado de registrar en el sistema la asignación de una identidad a un votante. Esto lo consigue introduciendo en la base de datos Relación Usuario-Identidad, la clave unívoca que le identifica (el número aleatorio). Esta funcionalidad es esencial para que el módulo *Check Status*, pueda realizar de manera satisfactoria la primera verificación.

- *Alta Ideas Candidato*, encargado de recoger la presentación y vínculos personales de los candidatos, una vez se hayan validado en el Universo de Votantes, dándolas de alta en una página Web accesible por todos los usuarios.

Todos los datos son gestionados en el sistema anonimato con tecnologías LDAP y SGBD:

- LDAP (*Lighweight Directory Access Protocol*) es el protocolo (OpenLdap) utilizado para acceder a los diferentes recursos e información de la red creada, actúa como middleware entre la capa de procesamiento y los diferentes Sistemas de Gestión de Base de Datos. Por lo tanto es encargado de proporcionar la posibilidad de asignación de permiso, portabilidad a diferente plataformas, autentificación entre los diferentes servidores, y encriptado de las comunicaciones a nivel de transporte y aplicación.

- SGBD (*Sistema de Gestión de Base de Datos*) es el encargado de proporcionar acceso a la base de datos, de una manera consistente y manteniendo la integridad, con un nivel de seguridad en las bases de datos, al poder establecer grupos y perfiles de usuario, limitando el acceso a los datos sensibles y su manipulación. Será este módulo quien interaccione con el Servidor LDAP y le proporcione los datos que solicite.

c) *Sistema de Voto*

Las diferentes tecnologías mencionadas para la presentación de la información en el sistema anonimato (XML, XSLT, XML Schemas) no difieren en cuanto a su funcionalidad se refiere de las del Sistema de Voto, salvo que ahora la interacción con el votante será menor, ya que la presentación se limitará a notificar al votante la finalización correcta del proceso, o en caso contrario comunicarle el error (por ejemplo un fallo en las comunicaciones).

Los módulos que componen el Sistema de Voto son:

- *Gestión de Sesión*, muy parecida a su análoga en el Sistema de Anonimato, salvo que no se creará ninguna sesión, sino que la recibirá del Sistema de Anonimato. Esto implica nuevamente que en caso de una conexión remota al sistema de votación, al verificar la validez de la sesión de dicha conexión, quedará de manifiesto que es un acceso fraudulento, por lo que será redirigido al Sistema de anonimato, es decir, no se podrá alterar el flujo de la aplicación.

- *Inserción de voto*, encargado de almacenar el voto emitido por el usuario y la identidad en el sistema que le representa. Este voto se introduce en una base de datos diferente a la de autentificación de los usuarios, preservando así (junto con un buena política de administración de base de datos), el anonimato.

- *Fragmentación del voto*, encargado de fragmentar el voto mediante un algoritmo de alto consumo de procesamiento.

- *Generador de informes*, encargado de generar unos informes de cara al votante en el que le confirme la validez de su voto, o si hay algún contratiempo, como un fallo en las comunicaciones o denegación del servicio, dárselo a conocer.

- *Inserción de bloqueo de voto*, encargado de validar el voto, reflejándolo en el sistema insertando un "1" donde antes había un "0", en la base de datos Relación Usuario-Identidad Sistema. Este módulo es muy parecido al de "Inserción de Identidad", del Sistema de Anonimato, y al igual que el mismo es muy importante para que el módulo "Check Status" realice de forma satisfactoria la segunda verificación.

Los datos son gestionados en el Sistema de Voto con las mismas tecnologías LDAP y SGBD utilizadas para el Sistema Anonimato, que no difieren respecto a este primer sistema en cuanto a su funcionalidad.

d) *Sistema de Recuento*

Las diferentes tecnologías mencionadas para la presentación de la información en el Sistema Anonimato (XML, XSLT, XML Schemas) tampoco difieren en cuanto a su funcionalidad de las del Sistema de Recuento, salvo que esta presentación no es para interaccionar con el sistema, sino para presentar los resultados de los comicios electorales, dejando abierta la posibilidad de publicarlos en un servidor Web, en cuyo caso se recomienda la tecnología GUI (*Graphical User Interface*), que proporciona al usuario un entorno amigable e intuitivo para interaccionar con el sistema.

Los módulos que componen el Sistema de Recuento son:

- *Control de Acceso*, encargado de filtrar el acceso al sistema, dejando libre transito sólo a aquél usuario que esté registrado. El conjunto de usuarios que pude utilizarlo es reducido, por lo que se encuentran especificados en un fichero "Ldif" suministrado por Ldap.

- *Contador de Votos*, encargado de leer el informe presentado por el Sistema Verificador. En caso de que todo sea correcto se accederá a la base de datos Urna electrónica y se contabilizarán los votos, mediante un algoritmo de desfragmentación de votos, en el apartado "Diseño lógico del Sistema". En otro caso, es decir, si se detecten irregularidades en el proceso electoral, no se contabilizarán los votos, pasando directamente al módulo *Generador de Informes Votos-Verificación*.

- *Generador de Informes Votos-Verificación*, encargado de presentar un informe de los comicios electorales (en caso de que el sistema de Verificación no detectara ningún tipo de fraude), o la de generar un informe con los resultados del Sistema Verificador.

Los datos son gestionados en el Sistema de Voto con las mismas tecnologías LDAP y SGBD utilizadas para el Sistema Anonimato, que tampoco difieren respecto a este primer sistema en cuanto a su funcionalidad. Cabe destacar en este caso que el servidor Ldap no solo proporciona el acceso seguro a las bases de datos, sino que además proporciona los perfiles y grupos de usuarios que pueden. utilizar el Sistema de Recuento, actuando el mismo como repositorio de los datos de usuarios.

e) *Sistema de Verificación*

En este caso la tecnología XML (*eXtensible Markup Language*) se utiliza como archivo de configuración de los diferentes parámetros de la aplicación. Entre ellos cabe destacar la hora del cierre electoral, que será el arranque de dicha entidad.

Módulos que componen el Sistema de Verificación:

- *Verificación Parcial y Total*, encargado de realizar la doble comprobación de que el número de votos es igual o inferior al número de votantes locales (comprobación parcial) y de que el número de votantes del sistema es igual o menor al número de votantes globales (comprobación total), es decir, que no hay más votantes en el Sistema que votantes censados en el universo de votantes.

- *Peso de los Votos*, encargado de determinar el debido cumplimiento de las reglas establecidas por la entidad que solicitó el proceso electoral. Para ello se consulta el departamento o región del voto y su peso, verificando así su validez.

- *Envío de Informes*, encargado de recoger los resultados obtenidos, darles un determinado formato y enviárselos al Sistema de Recuento.

Los datos son gestionados en el Sistema de Verificación con las mismas tecnologías LDAP y SGBD utilizadas en los sistemas anteriores, como el Sistema Anonimato.

f) *Base de datos Relación Usuario-Identidad*

Es la encargada de almacenar los datos del usuario, la identidad en el sistema (fragmentada) y el estado de los votantes (caso "se ha identificado, pero no ha votado", incidencias, etc.).

g) *Base de datos Universo de Votantes*

Es la encargada de establecer un rango de votantes del sistema (censo), que será emitido por la autoridad que solicite el proceso electoral.

h) *Base de datos Urna electrónica*

Es la encargada de almacenar los votos emitidos por los votantes.

II. *Flujos de datos entre los elementos del sistema*

Entre los elementos que constituyen la arquitectura básica del sistema (Sistema Anonimato, Sistema Voto, Sistema Recuento, Sistema Verificación, Base de datos Urna Electrónica, Base de Datos Universo de Votantes y Base de Datos Relación Usuario-Identidad) se producen las siguientes doce interconexiones o flujos de datos:

1) Clave Pública-Certificado.- El sistema Autoridad de Certificación envía al votante las claves públicas certificando las mismas.

2) Identidad Usuario.- El votante envía al Sistema de Anonimato los datos personales, y la clave asignada para su autentificación. Esto se hace por medio de claves de seguridad y un firewall.

3) Datos Usuario.- El Sistema de Anonimato, a través del módulo *Check Universo de Votantes*, lee de la base de datos Universo de Votantes datos unívocos de cada usuario para la autentificación en el sistema, además del número total de votantes.

4) Identidad en el sistema.- El Sistema de Anonimato re-direcciona al Sistema de Voto la identidad del votante en el sistema sin fragmentar.

5) Identidad en el sistema-voto.- El votante entrega al Sistema de Voto su voto, junto con la identidad sin fragmentar que le proporciona el Sistema de Anonimato.

6) Voto id-sistema.- El Sistema de Voto, a través del módulo *Inserción de Voto*, envía estos datos a la base de datos Urna electrónica y la actualiza con el voto y la identidad en el sistema sin fragmentar.

7) Nº de votos totales-Peso Voto.- El Sistema Verificador, a través del módulo *Verificación Parcial y Total*, consulta a la base de datos Urna electrónica, en la que se da el total de los votos contabilizados. Por otro lado, se consulta el peso cuantitativo de cada voto en el caso de que se trate de accionistas, esto lo hace a través del módulo *Peso de los Votos*.

8) Nº de votantes. El Sistema Verificador, a través del módulo *Verificación Parcial y Total*, consulta a la base de datos Relación Usuario-Identidad, en la que se da el número de votantes parciales que han hecho uso del sistema, y el de totales censados.

9) Cod.bloq.Id-usuario (bidireccional).- El Sistema de Anonimato, a través módulo *Check Status*, comprueba en la base de datos Relación Usuario-Identidad que el votante se ha autentificado. Por otro lado, el Sistema de Anonimato, a través del módulo *Inserción de Identidad*, actualiza la base de datos local, en donde se introducen los datos personales y la identidad del votante en el sistema (fragmentada).

10) Cod.Bloq.voto.- El Sistema de Voto, a través del módulo *Inserción de Bloqueo Voto,* valida el voto del votante en la base de datos Relación Usuario-Identidad generando un bloqueo para que no vote una segunda vez. El Sistema de Anonimato, a través del módulo *Check Status*, consulta en la base de datos Relación Usuario-Identidad, que el votante ha votado.

11) Test.- El Sistema Verificador, a través del módulo *Envío de Informes*, le envía al módulo Contador de votos del Sistema de Recuento, el informe de verificación de los comicios electorales, para que lo lea.

12) Nº de Votos. El Sistema de Recuento, a través del, módulo *Contador de votos*, accede a la base de datos Urna. electrónica y contabiliza los votos almacenados, mediante un algoritmo de desfragmentación de votos.

El siguiente cuadro refleja cómo acceden los distintos sistemas a cada base de datos, que puede ser en modo lectura (LEC) o en modo escritura (ESC). El número indica el flujo de datos que corresponde a cada caso:

Sistema / BdD	Anonimato	Voto	Recuento	Verificador
Universo de Votantes	LEC (3)	---	---	---
Relación Usuario - Identidad	LEC (10) ESC (9)	ESC (10)	---	LEC (8)
Urna electrónica	---	ESC (6)	LEC (12)	LEC (7)

Obsérvese que el Sistema Anonimato accede a la base de datos Universo de Votantes en modo lectura, a través del flujo Datos usuario (3), y a la base de datos Relación Usuario-Identidad en modo lectura, a través del flujo Cod.Bloq.voto (10), y en modo escritura, a través del flujo Cod.Bloq.Id-Usuario (9). El sistema de Voto accede a la base de datos Relación Usuario-Identidad en modo escritura, a través del flujo Cod.Bloq.voto (10), y a la base de datos Urna electrónica también en modo escritura, a través del flujo Voto id-sistema (6). El Sistema Recuento únicamente tiene acceso a la Urna electrónica en modo escritura, a través del flujo Nº de Votos, mientras que el sistema de Verificación lo tiene a la base de daros Relación Usuario-Identidad y a la Urna electrónica, ambos en modo lectura, a través de los respectivos flujos nº de votantes (8) y Nº de votos totales-Peso Voto (7).

III. *Seguridad*

a) *Seguridad inherente a la votación*

Es la seguridad del sistema de votación telemática en su conjunto, consecuencia de sus componentes y funcionalidades ya descritas anteriormente.

Esta seguridad inherente al sistema es garantía de los siguientes requisitos que deben darse en todo proceso de votación:

La autentificación del Votante.- Gracias a la intervención de una Autoridad de Certificación (que autentifica tanto a las maquinas implicadas como al votante, mediante la asignación de una clave personal para cada votante, se puede garantizar que los extremos en las comunicaciones son quien dicen que son.

El anonimato.- Para garantizar el anonimato del votante el sistema divide el proceso de votación en dos: la autentificación, donde el votante se le desarraiga de su identidad (proporcionándole otra para el sistema) y la votación. De este modo se sabe que un usuario "a" vota, pero no qué es lo que ha votado.

La imposibilidad de Coacción.- Al no poderse garantizar que un votante "V" ha votado a un candidato "C", por la resolución del punto anterior, no es viable la posibilidad de coaccionar a un votante ya que no habrá ninguna garantía de que lo haga.

La identificación unívoca de los Votantes.- Esto se consigue con una especificación off-line por parte de la entidad que solicita las elecciones, en la definición del universo de votantes, unido además a la intervención de una Autoridad de Certificación, y las medidas de cifrado que se citan en el punto referente a "la seguridad en la comunicaciones", evitándose así cualquier posibilidad de que un votante sea suplantado y se vea privado de su derecho a voto.

La unicidad de Voto.- Tras la resolución del punto anterior y la funcionalidad del sistema de anonimato (*Gestión de sesión y Check status*) se puede controlar que cada votante sólo vota una vez, al quedar registrado su voto en el sistema.

El control de acceso.- Esto se consigue gracias a una clave personal transmitida junto con los certificados antes de la votación y el módulo de Gestión de sesión de los diferentes sistemas. Cabe destacar que si bien el sistema de voto no crea ninguna sesión sino que le viene dada, no admite ningún acceso que no haya pasado previamente por el Sistema de anonimato, quien sí verifica la existencia del usuario en el universo de votantes.

El control de flujo.- En una arquitectura distribuida en dos Sistemas (en lo referente a los votantes) es importante controlar que no se pueda acceder remotamente a uno de ellos sin pasar previamente por el anterior. Para ello se gestiona la sesión, es decir, el sistema de Anonimato crea una sesión cuando se verifica que es un votante valido. Esta

sesión contiene unos atributos específicos, que adquieren un valor determinado, y una vez obtenida la identidad en el sistema es redirigido al sistema de voto. Si un votante accediese remotamente al sistema de voto, este lo primero que comprobará es su sesión, verificando que no tiene la misma y por consiguiente que no ha pasado por el sistema de anonimato, redirigiéndole al mismo, para que siga un procedimiento habitual.

b) *Seguridad antes de la votación*

Es un proceso previo a la votación para controlar que las comunicaciones serán seguras; se relaciona con la seguridad del elemento *Autoridad de Certificación*.

Para el autenticado y el cifrado de las comunicaciones el sistema utiliza una Autoridad de Certificación, lo que se conoce como notaria electrónica, que devolverá la CSR firmada por correo electrónico, y lo que es más importante, el Sistema de Voto enviará las claves personales y el certificado por correo electrónico.

El problema es que hoy en día hay numerosas herramientas que facilitan capturar, el tráfico de la red, y por consiguiente "espiar" los correos de los usuarios (bastaría con un Sniffer). Por ello, para proteger la integridad y la confidencialidad de los datos se acude a la criptografía, que ofrece diferentes herramientas para el envío de correos electrónicos certificados. No obstante, lo más importante es que ofrezcan un potente cifrado SSL y que sean transparentes de cara al Sistema.

c) *Seguridad en las comunicaciones*

Es sinónimo de seguridad en los flujos de datos.

Comunicaciones con el votante.- Para asegurar la comunicación entre el votante y el Sistema se utilizan certificados autenticados, a través de la Autoridad de Certificación, que ofrecen un cifrado de clave pública que garantizan la confidencialidad, la integridad y la accesibilidad.

Las tecnologías empleadas a este efecto son: Emisión de Certificados Autenticados (por una AC) basados en el estándar X.509, por parte del Servidor y del cliente, y Protocolo SSL (Secure Socket Layer), que es un estándar mundial de la seguridad Web que en este caso se utiliza para el cifrado del canal de las comunicaciones.

Los requisitos mínimos exigibles a las distintas Autoridades de Certificación candidatas para la implantación de este soporte tecnológico, son dos: Ofrecer un cifrado SSL no inferior a 128 bits, e implementar el protocolo SGC (Server Gated Cryptography).

Comunicaciones entre los elementos del sistema.- El estándar de comunicación entre los distintos recursos de la aplicación (servidores, bases de datos, impresoras, etc.) es LDAPv3 (*Lightweight Directory Access Protocol*), que proporciona el control y la seguridad que este sistema requiere. En concreto se emplea *OpenLDAP*, debido a su transparencia absoluta (Open Source) ya que es compatible con todos los módulos.

Algunas características interesantes de cara al sistema de LDAPv3 son: i) Poseer un soporte de autentificación fuerte gracias al uso de SASL (*Simple Authentication and Security Layer*), para ello hay que hacer uso del software *Cyrus Sasl*, ii) ofrecer mecanismos de protección de confidencialidad e integridad gracias al uso de TSL (o SSL), para ello hay que hacer uso del software *OpenSSL*, iii) control topológico, es decir, ofrecer la posibilidad de configurar el servicio (Slapd) para restringir el acceso a la capa de socket en base a la información topológica de la red, iv) mecanismos de control de acceso a los recursos del sistema, mediante creación de grupos y perfiles de usuarios, restricción de IPs, nombres. de dominio, etc., v) elección de Backend para las bases de datos, vi) posibilidad de levantar muchas instancias a diferentes (o iguales) bases de datos al mismo tiempo, vii) uso de hilos de ejecución para obtener un alto rendimiento, viii) altamente configurable.

Transmisión en los canales de comunicación.- Hay tres posibilidades: Unir los equipos implicados con tarjetas de red aparte y un cable cruzado; criptografía; certificación y Autenticación de las máquinas implicadas. La elección dependerá del grado de seguridad que se pretenda adquirir, la opción 1 es la más básica y la tres la más segura (ya que incluye el cifrado). También se puede optar por combinaciones de ellas.

d) *Seguridad Administrativa*

Seguridad en el acceso a los servidores web

Los servidores web dependerán del presupuesto de la autoridad que solicite las elecciones, pero en todo caso deberán tener los siguientes parámetros mínimos de configuración para que se establezca la seguridad deseada en el sistema, los cuales deberán ser verificados por el Administrador:

- ServerType: Indica al Servidor cómo debe manipular internamente las peticiones de los navegantes. El valor que deberá tener es Inetd, al dar prioridad a la seguridad, que al rendimiento del sistema (consumo de recursos, standalone).

- ServerRoot: Indica donde se sitúan los archivos de configuración, errores, y registros. Es muy útil en seguridad administrativa en combinación con DocumentRoot.

- TimeOut: Indica el número de segundos antes de enviar un timeout. Este parámetro es muy importante para optimizar el rendimiento del sistema, más con la configuración del ServerType con Inetd. Imagínese que por cualquier motivo entra el servidor en un bucle infinito, esto consumiría muchos recursos (memoria, micro, una instancia en el sistema...), por lo tanto este parámetro tiene que estar muy ajustado para obtener un alto rendimiento.

- Port: Permite determinar el puerto de servicio de la aplicación. En principio, el puerto 8080 (el más corriente) será el puerto de acceso, pero el resto de puertos deben ser controlados por el Firewall del Sistema con el objetivo de evitar la obtención de información que pueda ser utilizada en contra.

- ServerAdmin: Ofrece la posibilidad de incluir la dirección de correo electrónico del Administrador con el objetivo de que si sucede algún error, informarle del mismo.

- ServerName: Parámetro para modificar la IP o el nombre del dominio puesta durante la instalación del Servidor.

- DocumenRoot: Este parámetro, también llamado root virtual, indica al servidor dónde puede obtener las paginas Web solicitadas, es decir, le indica que ha de considerar el directorio especificado como el path del nivel superior. La elección de este directorio es *muy importante*, por ejemplo si el valor del DocumenRoot fuese "./" o "c:/", podría acceder a todo el disco duro, (obviamente no tendría permisos de directorios).

Si fuera preciso aumentar la seguridad, se podría, para un mayor orden y seguridad-administrativa, separar en dos discos duros los archivos del sistema operativo, junto con la instalación del Servidor, y en el otro disco, las páginas Web.

Para acceder a los diferentes recursos e información web del sistema se utiliza un protocolo OpenLdap. Los servidores de directorio LDAP (Lighweight Directory Access Protocol) almacenan sus datos jerárquicamente, de una forma muy parecida a la forma en que un Sistema Unix estructura sus directorios. Esta estructura jerárquica es beneficiosa por varias razones: Primero, porque permite establecer unos determinados privilegios a un grupo de individuos basándose en el árbol de directorios, segundo, porque permite realizar búsquedas de recursos o información de una manera más eficiente, y, tercero, porque también permite el control de acceso a determinados recursos por determinados usuarios, definiendo cómo trabajan con ellos (lectura, escritura o ambas).

LDAP proporciona un complejo control de instancias o ACIs, que permite definir cómo se almacena o recupera la información, en base a los perfiles de los usuarios y éstos deben ser administrados.

Seguridad en el acceso a las bases de datos

El administrador de la base de datos deberá definir los perfiles de usuario de todos los clientes que puedan acceder a los almacenes de datos, especificando la manera de acceder a los mismos (lectura, escritura o ambas) y a qué datos pueden o no acceder. Esto depende de la implementación de las bases de datos, y éstas a su vez pueden variar atendiendo a la entidad que solicite las elecciones.

El modelo conceptual que se implemente para el acceso a los almacenes de datos es independiente de la forma (lectura/escritura) en que los distintos sistemas de la arquitectura acceden a las bases de datos mediante las correspondientes interconexiones o flujos de datos (ver última tabla).

Seguridad en la gestión de los Logs del Sistema

Los ficheros logs y los registros de incidencias son esenciales para una posible reclamación individual del voto.

Los ficheros tipo log son archivos, generalmente de texto, que crea el propio ordenador para almacenar o registrar todos los eventos que ocurren en el sistema.

Los ficheros de log es una opción del sistema que proporciona las trazas de ejecución de una determinada instancia. Estos ficheros se reparten entre los diferentes sistemas de modo que una persona que quisiese reconstruir una instancia determinada (de un votante), debería tener los permisos y el acceso en todos los sistemas implicados.

Los registros de incidencias se diferencian del los ficheros de log, en que se centran más en la interacción con el sistema que en los datos que entran y salen de los diferentes sistemas. Por otra parte, éstos se almacenan en las diferentes bases de datos, mientras que los ficheros de log se almacenan en los distintos servidores.

En el sistema de voto telemático en cuestión los ficheros logs tienen la función de registrar los eventos que ocurren en el Sistema (operativo), aplicaciones incluidas. Por lo tanto son de gran importancia para monitorizar el sistema antes, durante y después del proceso de votación, para garantizar la ausencia manipulación alguna, o, si la hay, determinar donde y quien ha sido.

Muchos de los ficheros de logs son en texto plano y, por lo tanto, su edición y manipulación es relativamente sencilla (una vez adquiridos los permisos), por lo que se han establecido mecanismos de logs distribuidos o remotos (seguros) y administrados por personal distinto.

La información mínima a recabar en los logs, es la siguiente:

- Todas las autentificaciones, buenas o fallidas.
- Los mensajes provenientes del Kernel.
- Los mensajes de arranque del sistema.
- Un registro de logins fallidos cuando supera un número de errores determinado.
- Un registro con la información sobre las ejecuciones de la orden "su".
- Un fichero de log que almacene todos los log por defecto, y así sirve para comprobar posibles modificaciones en un fichero de log determinado.

Para logear toda esta información hay que configurar correctamente el fichero /etc/syslog.conf, lo que será tarea del Administrador de sistema. Sin embargo, esto crea varios interrogantes, derivados de que el Administrador del sistema podría tener algún fallo o podría llegar a ser capcioso. Por ello, se ha previsto que no sea un único Administrador del sistema el encargado de configurar el fichero /etc/syslog.conf, sino que por cada sistema principal del Sistema VT (de anonimato, de Voto, de recuento y de verificación), existan tres administradores del sistema que diseñen conjuntamente el fichero syslog.conf, y que posteriormente cada uno de ellos monitorice los ficheros de log en tres máquinas diferentes, es decir, que los log no se registren de manera local en la maquina en cuestión sino en tres computadoras diferentes y aisladas del mundo exterior (sin conexión a Internet, sólo a su Sistema).

Este sistema de logs distribuidos tiene varias ventajas: En primer lugar, es difícil de atacar, ya que el atacante deberá no sólo poner en cuestión al sistema "padre" sino también a cada "hijo", en caso contrario quedaría al descubierto y peligraría su integridad en el sistema. Por otro lado, como está previsto que la información de los tres sistemas "hijos" sea la misma, se consigue una mayor consistencia, y menor posibilidad de manipulación de datos por parte de un administrador capcioso. Y al estar previsto también que estos sistemas "hijos", de logeo, estén dedicados exclusivamente a su función, el número de procesos contenidos el sistema es muy reducido, y por lo tanto fácil de proteger.

En este caso el Firewall es una entidad fundamental, ya que la transmisión de los logs es por el puerto 514 UDP, y por tanto nos asegurar el tener controlados los diferentes puertos e ips.

e) *Seguridad de los datos*

Es la seguridad de los datos almacenados en los elementos bases de datos, al margen de las restricciones de uso que se puedan hacer de ellas según el sistema del que se trate.

Los datos referentes a los Votantes y al proceso de votación se almacenan en bases de datos. Desde el punto de vista del almacenamiento físico los datos están contenidos en uno o varios ficheros, atendiendo al sistema de gestión de base de datos que se utilice. Por ejemplo, en Mysgl, los datos son contenidos en ficheros .txt, legibles por cualquier usuario que tenga permisos de lectura, y editable, por cualquiera que tenga permisos de lectura, escritura. En Oracle, la información de una tabla se distribuye en diferentes ficheros, que unido a la codificación de su contenido (no es legible, sino es por medio del SGBD), nos da una mayor seguridad.

En cualquier caso, para garantizar la integridad y la confidencialidad de los datos siempre se puede recurrir a un cifrado de claves simétricas del contenido de la, información sensible de la base de datos (los mismos SGBD, los proveen), por lo que es lógico pensar que un supuesto atacante lo hará a través del SGBD (Sistema de Gestión de Base de Datos), y no directamente sobre los ficheros donde físicamente están contenidos los datos. Atendiendo a esta hipótesis, el usuario fraudulento debería suplantar a un usuario del sistema, a un administrador, o incluso a un super-administrador. Esto podría llegar a suceder, bien por la pericia del atacante o bien porque sea el propio administrador o super-administrador (más probable).

Las medidas lógicas a establecer para evitar este posible ataque, son las siguientes:

Log del sistema de gestión de base de datos.- Todo sistema gestor de base de datos que se precie como tal tiene herramientas de log que permiten registrar, desde quien abre una instancia en el sistema, hasta posibles errores en el inicio, transcurso y parada. De este modo se puede establecer quién manipuló ilícitamente el contenido de la base de datos.

Administración de la base de datos.- Restringir el acceso a determinas tablas o columnas atendiendo al usuario suplantado (o al que pertenezca el atacante, en caso de fraude interno).

Diseño lógico del Sistema.- Diseñar las bases de datos de tal modo que la información sensible que contenga cada tabla necesite de un procesamiento para tener sentido. Para ello, tanto los usuarios (la identidad en el Sistema), como el voto, y lo votado, serán números, y estos estarán en la base de datos fragmentados, necesitando así de diversos algoritmos contenidos en los diferentes sistemas para unificarse en un sólo número y así tener sentido.

Cabe destacar que el diseño de fragmentación y desfragmentación es de caja abierta, es decir, no obligamos a que sea un algoritmo en concreto sino que se deja abierta la puerta a una implementación libre atendiendo al tipo de respuestas esperadas. Para la implementación del sistema se exige la elección de un algoritmo que sea inviable la resolución manual aun conociendo el mismo, por ejemplo un sistema de n ecuaciones con n incógnitas siendo $n > 50$. O un algoritmo exponencial tal que si no se programa de una forma adecuada, se produzca un desbordamiento de la memoria.

En consecuencia, se buscan algoritmos de elevado coste de procesamiento. Además estos algoritmos se ubican en dos partes diferentes del Sistema: la fragmentación del voto, se encuentra en los diversos Sistemas de Voto, mientras que la desfragmentación se encuentra en el sistema de Recuento.

El Sistema de Voto, en cuanto a carga de procesamiento, es leve, debido a que es un sistema distribuido entre los diferentes departamentos o regiones (reducido grupo de usuarios), encargándose de recibir los voto de los votantes y devolver la validación de la votación. Toda la anterior interacción con los votantes recae sobre el Sistema de Anonimato.

En cuanto al Sistema de Recuento, su carga de procesamiento es justo esa, contabilizar los votos, que puede llegar a ser grande atendiendo al algoritmo de desfragmentación, aunque la característica de ser un proceso off-line, es decir, que entra en funcionamiento cuando los votantes ya han emitido sus votos, juega a su favor.

Esta división de algoritmos (Sistema de Voto, fragmenta los votos, y Sistema de recuento los vuelve a unificar) proporciona una capa más de seguridad (sobretodo ante ataques internos), al repartir la responsabilidad entre diferentes partes del Sistema y por consiguiente se necesita la cooperación y permisos de los mismos.

f) *Seguridad del Sistema de Verificación*

La seguridad del sistema de verificación queda ya definida por las funciones propias de este elemento de la arquitectura básica, el cual favorece la transparencia de los comicios, así como la imposibilidad de fraude electoral por parte de terceros.

Verificación global.- Realizada por el propio Sistema de Verificación, quien se encarga de hacer tres verificaciones: 1) Que el número de votantes es igual o inferior al número de votos; 2) que el número de votantes es igual o inferior al Universo de Votantes; y 3) que el peso de los votos es el correcto, para cada voto.

Verificación Individual.- Esta posibilidad técnicamente es factible. Su objetivo es que cada votante pueda comprobar durante un periodo de tiempo su voto, sin perder el anonimato. Sin embargo, en caso de una reclamación, se levantaría la instancia en cuestión en sentido inverso (adquiriendo previamente todos los privilegios en los diferentes Sistemas), perdiendo así el anonimato, y por consiguiente vulnerando la ley, por lo que en este proyecto no ha sido contemplada.

En definitiva, el sistema de la presente invención no se limita a introducir un sistema de voto telemático en los sistemas de voto actuales, sino que propone una reestructuración de los procesos electorales en sí mismos, lo que supone una auténtica innovación, ya sean procesos públicos o privados.

Esta reestructuración se da porque se crea un proceso de votación totalmente electrónico, con todas las fases informatizadas, pudiéndose aplicar independientemente del lugar donde se encuentre el votante, a diferencia de todos los sistemas de voto electrónico desarrollados e implementados hasta la fecha, que necesitan de la presencia física del votante en el momento de la votación.

Pero además de dicha ventaja fundamental de poder votar por Internet, el sistema introduce otras ventajas importantes, algunas de las cuales consecuencia directa de la misma, que a continuación se comentan.

Informatización y centralización del proceso.- El sistema guarda la información sobre el voto, así como la información sobre quién ha votado, en bases de datos centrales, aunque independientes entre sí. Esto mejora el sistema tradicional en el que los encargados de la mesa electoral tenían información sobre quien votaba y quién no lo hacía, vulnerando así la premisa de la identidad del votante en cualquier caso, no solo en el de voto.

Disminución de la posibilidad de coacción.- Debido a que no es necesaria la presencia física en el lugar de la votación, pudiendo hacerlo desde casa, queda anulada cualquier posibilidad de coacción en el momento del voto, quedando reducida a la misma seguridad y privacidad que puede tener uno en su propio hogar.

Capacidad de adaptación.- Se ha diseñado un sistema con capacidad modular, es decir, cualquiera de sus elementos puede ser modificado para adaptarse a la normativa que tenga el proceso de voto en cuestión. Se podría, por ejemplo, permitir más de un voto por persona, votos no anónimos, o el uso de porcentajes de decisión por voto.

Facilidad de manejo.- Otra ventaja a destacar es la facilidad de manejo de cara al votante, para él todo ocurre en tres pantallas diferentes, una última que le informa de que su voto ha sido contabilizado correctamente.

Eliminación del voto por correo garantizando la posibilidad de ejercer el derecho a voto en cualquier caso.- Con este sistema los usuarios que se encuentren fuera de España o no puedan desplazarse hasta los colegios electorales podrán votar desde su propia casa, como todos los demás.

Compatibilidad con el proceso electoral actual.- El sistema de la presente invención se ha diseñado de tal manera que fuese compatible con el proceso tradicional. Para una implantación híbrida del proceso de voto estatal más cercana a los votantes solo sería necesario contar con listas centralizadas donde los vocales pudiesen informar de que esa persona ha votado por el sistema tradicional.

Publicidad gratuita a las ideas de todas las candidaturas.- Este sistema ofrece las mismas oportunidades a todos los participantes, independientemente de su ideología o afiliación política. Por ello, durante el proceso de alta de candidatos se ha incluido un módulo con el cual todos los candidatos poseen un espacio en el servidor para exponer sus ideas, así como para incluir vínculos externos a sus propias páginas.

Generación automática e instantánea de los resultados.- Dado que este proceso de voto se basa en sistemas informáticos por completo se dispone de todas las características y facilidades que éstos ofrecen: permite que las urnas electorales se abran y cierren exactamente a unas horas prefijadas, el recuento de votos, que normalmente tarda algunas horas, podría ser prácticamente instantáneo, pudiendo ser los resultados publicados en Internet.

Aplicación con un flujo robusto.- Otra cuestión que se ha tenido en cuenta en el diseño es que el proceso de votación debe darse en una serie de pasos concretos y seguidos, de manera que ningún usuario malicioso pueda tomar un camino alternativo. Por ello se han introducido las sesiones volátiles, aumentando la seguridad puesto que ningún usuario puede saltarse ningún paso del proceso. Además, esto permite tener en cuenta ciertas particularidades para cada usuario. Hay que destacar que el uso de este tipo de sesiones volátiles no permite más de un voto por persona, aunque haya comenzado veinte sesiones volátiles desde el inicio de la votación solo podrá votar una vez y no podrá iniciar ninguna después.

Verificación automática de los resultados.- Una ventaja más que presenta el presente sistema de votación telemática es la verificación automática de los resultados.. Esto no se puede permitir, pero si ocurriera deben existir m Este sistema presenta mecanismos que detectan y notifican a las autoridades pertinentes si se ha intentado modificar los resultados por intereses particulares.

Seguridad del sistema.- Como es un sistema en el que todos los procesos dependen solo de máquinas, el error y la maldad humana no son aplicables. Como se ha explicado, cada máquina utilizada es una caja cerrada inaccesible con una cierta lógica interna. Éstas máquinas estarán supervisadas por distintos actores humanos, con diferentes intereses en los resultados, por lo que se garantiza que no se creará un complot a gran escala. Además, los códigos con la lógica interna de las máquinas serán hechos públicos. La seguridad del proceso y de los datos estará garantizada aunque los códigos sean públicos por lo que se puede ofrecer un sistema de seguridad robusto a la vez que una lógica de actuación transparente.

Algunas ventajas de estos mecanismos son: i) generación de identidades aleatorias, los datos del usuario nunca se asocian al voto emitido por éste directamente; ii) fragmentación de la información, esto quiere decir que para recuperarla es necesario resolver ciertos algoritmos diferentes repartidos entre varios sistemas: iii) control de acceso mediante claves personales emitidas de forma segura por la Autoridad que gestiona el proceso electoral; iv) restricción del acceso administrativo para garantizar que solo puede acceder físicamente a cada máquina el administrador acreditado; v) registro de prácticamente todas las acciones que realiza el sistema, y solo la autoridad competente podrá, tras el proceso de votación y de forma excepcional, consultarlos en caso de reclamaciones; vi) utilización de certificados digitales, emitidos por Autoridades de Certificación de fe pública, que deben ser ajenas al sistema de votación y proporcionar un servicio con la suficiente profesionalidad, dependiendo de las necesidades de la implementación en cada caso; vii) mecanismos de seguridad informáticos, a parte de los mecanismos de seguridad especificados más arriba existen muchos otros pero que están más relacionados con la informática propiamente dicha que con el presente diseño. Este tipo de mecanismos van desde cortafuegos informáticos, que impiden los ataques externos, hasta el uso de software inmune a virus, que impide ataques de tipo troyano.

Para una mejor comprensión del sistema de votación cuya patente se reivindica, y especialmente con vistas a la explicación que a más abajo se realiza sobre la forma en que en la práctica se lleva a cabo, se acompaña a esta memoria descriptiva dos dibujos ilustrativos: El dibujo de la Figura 1 es un esquema del proceso global de votación, con los ocho elementos principales del sistema y los doce flujos de datos que entre ellos tienen lugar, mientras que la Figura 2 es una recreación del caso práctico de implementación del proceso de votación que se comenta al final de la descripción.

Modo de ejecución

Tomando como referencia el esquema global del proceso de votación telemática ilustrado en la Figura 1, pasamos a continuación a hacer una exposición detallada de su forma de implantación en la vida real.

Para ello es necesario previamente establecer los perfiles de las personas que intervienen en el proceso, al margen de los propios votantes, para luego describir las diferentes fases de la implantación. La exposición se cierra con un caso práctico puesto como ejemplo.

I. *Personas que intervienen en el proceso*

En la puesta en práctica del sistema de votación telemática a través de Internet desarrollado intervienen, como mínimo, los agentes siguientes:

Entidad que solicita las elecciones.- Deberá facilitar un listado de los votantes, así como el peso de voto de cada uno, y acondicionar, en caso de que así se acuerde, las salas necesarias para la instalación y uso de los equipos informáticos. Además se encarga de elegir la Autoridad de Certificación, en función del presupuesto que tenga y las ofertas que reciba, siempre que cumplan los requisitos mínimos: ofrecer un cifrado SSL no inferior a 128 bits e implementar el protocolo SGC (*Server Gated Cryptography*).

Administrador.- Sus funciones o tareas serán: i) verificar que el servidor web cumple los requisitos mínimos; ii) crear y gestionar a los diferentes usuarios y grupos de usuarios del Sistema; iii) configurar de manera correcta el demonio Slapd, donde se especifica las interfaces por donde se escucha, contenidas en la variable, Slapd Services. El protocolo de comunicación que se deberá especificar es el ldaps; iv) configurar de manera correcta los ficheros .ldap .conf, donde está definida la configuración global de los clientes Ldap; v) configuración y gestión correcta del OpenSSL, para los certificados, renovación de claves, etcétera; vi) configurar correctamente el fichero /etc/syslog.conf.

Técnicos informáticos.- Forman parte de la seguridad activa del proceso, su función es controlar que todos los parámetros de seguridad del sistema permanecen estables.

II. *Forma de realización*

Antes de la votación, el sistema ya tiene una base de datos de los votantes (Universo de Votantes), facilitada por la entidad que solicita la votación, con algún dato personal, por ejemplo un email, y con el peso del voto de cada votante, si hubiera diferencias.

El sistema Autoridad de Certificación envía al votante las claves públicas certificando las mismas, este paso se corresponde con el flujo de datos llamado Clave pública-Certificado.

El votante va a la web oficial de votación, donde se le abre una ventana que le pide ese o esos datos. El usuario los introduce, este paso se corresponde con el flujo de datos llamado Identidad Usuario. El votante en la web oficial de votación puede ver unos enlaces a los distintos candidatos realizados por el *módulo Alta Ideas Candidato* del Sistema de Anonimato. El *módulo Gestión de sesión* del Sistema de Anonimato es el que se encarga de personalizar la presentación de cara al usuario y crear un perfil.

Al Sistema de Anonimato le llega esta información, y verifica en la base de datos Universo de Votantes, a través del *módulo Check Universo de Votantes,* que el usuario que se conecta al sistema pertenece al rango de votantes. Esta consulta se corresponde con el flujo de datos llamado Datos Usuario. En caso afirmativo, se genera una CRS (solicitud de certificado), que debidamente autorizada por la Autoridad de Certificación será enviada junto con una clave personal al votante.

El votante, siguiendo las instrucciones de pantalla, abre su correo donde estará su clave personal y el certificado emitido por la Autoridad de Certificación. Después de descargarlos, ejecuta el auto-instalable de certificación.

El ejecutable le dice al votante la dirección web de la aplicación. Una vez en ella el votante puede ver las páginas de los candidatos (para eso no hace falta identificarse) o identificarse en el sistema con la clave personal. Entonces el votante, para identificarse, introduce su clave personal cifrada con la clave pública del servidor.

El Sistema de Anonimato comprueba la validez de la clave personal. En caso afirmativo se creará la sesión, en otro caso se le denegará el acceso. A partir de este momento las comunicaciones son seguras entre el votante y el sistema.

El Sistema de Anonimato entonces, a través del *módulo Check Status*, comprueba el estado del votante mediante dos verificaciones: primero, si el votante tiene una identidad ya asignada en el sistema, en caso afirmativo se le envía al paso 10 (para mayor anonimato el votante tiene un nombre aleatorio en el sistema a la hora de votar); 2) si ha votado (en caso afirmativo, se le deniega la continuidad en el sistema). Este paso se corresponde con el flujo de datos llamado Cod.Bloq.Voto.

El *módulo Generador de Identidades* del Sistema de Anonimato genera una identidad para el votante, chequeando dicha operación en la base de datos Relación Usuario-Identidad. Esto es esencial para que el *módulo Check Status* pueda realizar de manera satisfactoria la primera verificación. Por otro lado se actualiza la base de datos local, donde se introducen los datos personales y la identidad del sistema de manera fragmentada, es decir, no se relaciona identidad en el sistema con un determinado votante. Este paso se corresponde con el flujo de datos llamado Cod.Bloq.Id-Usuario.

Entonces el *módulo Gestión de Sesión* del Sistema de Voto, recibe la sesión del votante con su identidad en el sistema, comprobando la validez de la misma, y en caso afirmativo se le muestra al votante la solicitud de voto.

El votante ve en su pantalla que seleccione al candidato que desee y presione el botón "Votar". Con este gesto, el votante le da al Sistema de Voto, su voto junto con la identidad sin fragmentar que le proporciona el sistema, este paso se corresponde con el flujo de datos llamado Identidad en el sistema-voto, que lo almacena el *módulo Inserción de voto* en una base de datos diferente a la de autentificación de los usuarios, preservando así el anonimato.

El Sistema de Voto recibe el voto, que será registrado en la BD Urna electrónica y la actualiza con el voto y la identidad en el sistema sin fragmentar. Este paso se corresponde con el flujo de datos llamado Voto id-sistema.

El Sistema de Voto actualiza la BD Relación Usuario-Identidad estableciendo que ese votante ha votado, generando un bloqueo ante un segundo intento de votación por parte del votante. Este paso se corresponde con el flujo de datos llamado Cod.Bloq.Voto.

El Sistema de Voto, mediante el *módulo Generador de informes*, confirma al votante que la votación ha sido registrada, y éste lo ve por pantalla.

Por otro lado, un usuario autorizado por la entidad que convoca las elecciones, accede localmente al Sistema de Recuento, que comprueba que este usuario es el autorizado mediante el *módulo Control de Acceso*.

Una vez activado el recuento, se llamará remotamente al Sistema Verificador, que le atenderá en caso de haber terminado el periodo de votación, de lo contrario rechaza la petición.

El Sistema Verificador accede a las bases de datos Urna electrónica (este paso se corresponde con el flujo de datos llamado Nº de votantes) y Relación Usuario-Identidad.

El Sistema Verificador, a través del *módulo Verificación Parcial y Total*, el número de votos es igual o inferior al número de votantes locales, y de que el número de votantes del sistema es igual o menor al número de votantes globales. Por otro lado, a través del *módulo Peso de los Votos*, verifica además de que el peso de los votos es correcto. Este paso se corresponde con el flujo de datos llamado Nº de votos totales-Peso voto.

En el caso de que el Sistema Verificador devuelva un resultado contradictorio, se acabará el recuento informando de los errores. En caso de que el Sistema Verificador devuelva un resultado satisfactorio, el *módulo Envío de Informes* recoge los resultados obtenidos, les da un determinado formato y los envía al Sistema de Recuento. Este paso se corresponde con el flujo de datos llamado Test.

El Sistema de Recuento leer el informe presentado por; el Sistema Verificador y si todo es correcto se conecta a: la base de datos Urna electrónica, y recuenta los votos., Este paso se corresponde con el flujo de datos llamado Nº' de Votos. En otro caso, es decir, no se contabilizarán los votos, pasando directamente al *módulo Generador de Informes Votos-Verificación.*

Por último, el *módulo Generador de Informes Votos-Verificación* del Sistema de Recuento genera un informe de los comicios electorales, los cuales podrán ser publicados y consultados en la web.

III. *Caso práctico*

Sea una empresa que ha contratado los servicios de este sistema de votación telemática pues desea realizar una junta general para votar una ampliación de capital. Esta empresa se divide en mil acciones que, para simplificar la explicación, estarán repartidas entre cien personas a partes iguales. Las posibilidades de voto serán SI, NO y ABSTENCION.

Como la empresa desea tomar una decisión equitativa e imparcial, se ha decidido que el voto será secreto, evitando así la coacción, que solo se emitirá un voto por accionista y que se desea una seguridad total de que el proceso se ha llevado a cabo perfectamente. La duración de la votación será de seis horas.

Como sus accionistas, representados en la Figura 2 como un icono con un sobre, no viven en la ciudad en la que se encuentra la sede de la empresa, también se ha impuesto la premisa de que la votación se pueda realizar desde cualquier parte del mundo y con cualquier tecnología de; acceso Internet disponible.

A la empresa se le dio la opción de que todo el proceso se llevase a cabo remotamente, sin embargo, la empresa prefirió que las máquinas se colocasen en su propio edificio.

Para una implementación sencilla se cuenta con cuatro ordenadores como servidores base, que darían cabida a los sistemas ya especificados anteriormente: anonimato, votación, recuento y verificación.

Además son necesarios otros tres ordenadores donde se instalan las diferentes bases de datos y un equipo de firewall, para aislar los equipos del resto de la Red de Área Local de la empresa.

Para la importante labor de supervisión se utilizan cuatro equipos conectados a los diferentes servidores ampliando así la seguridad con la que se realiza esta tarea.

Por último, son necesarias tres salas vacías, donde dos de ellas serían de baja seguridad, y la otra de alta seguridad, en parte proporcionada por la propia empresa.

La implantación del sistema trataría de hacerse de la manera más limpia y menos perjudicial para las actividades de la empresa. Dado que ésta ha comentado que posee una sala especializada para la colocación de servidores, la colocación de los sistemas y de las bases de datos que contengan el Universo de Votantes y la relación de Identidades y usuarios, se llevaría a cabo en ella (Sala 1 en Figura 2).

El resto de los sistemas y bases de datos se ubicarían en una de las otras dos salas acondicionadas (Sala 2 en Figura 2). En la última sala libre se colocarían los sistemas de supervisión, así como los informáticos encargados de su uso y el coordinador (Sala 3 en Figura 2).

Para la configuración elegida por la empresa se elige un software apropiado, con la configuración mínima para funcionar, evitando complicaciones de uso. Dado que la instalación de las máquinas debe ser rápida, pero limpia y transparente, se ha tomado la decisión de llevar los ordenadores en blanco, y una vez conectados se procedería a la instalación de una imagen mediante la inserción de un CD de datos. Estas imágenes contendrían todas las funcionalidades necesarias para cada sistema, así como scripts de carga previa de bases de datos si fuese necesario.

El personal necesario para este tipo de eventos difiere mucho según la implementación. En este caso se estima que sería necesario un equipo de siete técnicos informáticos (representados en la Figura 2 como un icono con una llave inglesa) durante el día de la votación. Cinco se encargarían de la supervisión del funcionamiento, donde cuatro de ellos llevarían a cabo la propia supervisión y otro realizaría la tarea de coordinador (representados en la Figura 2 como un icono con una llave). Los otros dos informáticos estarían cerca de las salas de los servidores por si se produjese alguna incidencia.

Para la propia seguridad de las salas sería preciso contratar a una empresa de seguridad que enviase tres agentes de seguridad, uno por cada sala a vigilar. En la Figura 2 aparecen representados por un icono con un candado.

Como ejemplo de transparencia y limpieza en las elecciones se precisaría la contratación de un notario, que verificase y firmase los resultados de la votación antes de ser publicados.

Por último, aunque no entra exactamente en la definición de personal, se requeriría la emisión de cien correos físicos certificados para hacer llegar las bases de la votación y las claves de acceso a los votantes.

Todos los equipos se inicializarán seis horas antes del comienzo de la votación y se comprobará su buen funcionamiento mediante una serie de comandos preparados para ello. Inmediatamente después todo el personal abandonará las salas de los servidores, impidiéndose cualquier tipo de entrada no autorizada por el coordinador, y comenzará la monitorización desde la sala remota. La función de los Informáticos será la de controlar que todos los parámetros de seguridad del sistema permanecen estables. Se ha de poner de manifiesto que el seguimiento de los parámetros de seguridad solo será en sentido lectura, impidiendo cualquier tipo de manipulación.

Los servidores comenzarán y finalizarán el proceso de votación a las horas establecidas de forma automática. Si se produjese un cambio de estos parámetros el coordinador sería informado de inmediato, ya que es el único con poder de decisión sobre la actuación del resto del personal, para que se realice lo que se estime más pertinente.

Una vez acabado el proceso de votación se procederá automáticamente a la verificación y recuento de los votos emitidos. Justo después se permitirá el acceso al notario a la sala de recuento, acompañado de un agente de seguridad, que comprobará la veracidad de los resultados y la certificará, procediendo después a la publicación de los mismos en una página web, así como a su envío a todos los participantes mediante correo electrónico.

REIVINDICACIONES

1. Sistema de votación telemática a través de Internet, realizado en un escenario de comunicación en el que intervienen un conjunto de sistemas automáticos que funcionan bajo unos programas predeterminados de sistema operativo, gestores de bases de datos, aplicaciones web y seguridad en Internet, **caracterizado** porque dicho conjunto de sistemas está constituido en su arquitectura básica por una Autoridad de Certificación en Internet, encargada de cifrar las comunicaciones y autentificar tanto al votante como al sistema de votación, un Sistema de Anonimato, encargado de presentar a los candidatos, controlar el acceso, garantizar el anonimato de los votantes y seguimiento de los mismos durante el proceso, un Sistema de Voto, encargado de recibir, gestionar y almacenar los votos emitidos de un determinado departamento, un Sistema de Recuento, encargado de contabilizar el número de votos, un Sistema Verificador, encargado de validar los comicios electorales, una base de datos Relación Usuario-Identidad, encargada de almacenar los datos del usuario, su identidad en el sistema y el estado de los votantes, una base de datos Universo de Votantes, encargada de establecer un rango de votantes del sistema, y una base de datos Urna electrónica, encargada de almacenar los votos emitidos por los votantes.

2. Sistema de votación telemática a través de Internet, según reivindicación 1, en el que la Autoridad de Certificación en Internet es una entidad de fe pública que utilice el cifrado SSL (Secure Socket Layer) de seguridad Web, como puede ser la propia Administración pública.

3. Sistema de votación telemática a través de Internet, según reivindicación 1, en el que el Sistema Anonimato está compuesto por los siguientes módulos: *Gestión de Sesión*, encargado de personalizar la presentación de cara al usuario y crear un perfil volátil del mismo, así como su jerarquización, *Check Status*, encargado de comprobar el estado del votante en el sistema, verificando primero si se le ha otorgado una Identidad, y segundo, si ha votado, *Check Universo de Votantes,* encargado de verificar que el usuario que se conecta al sistema pertenece al rango de votantes, *Generador de Identidades,* encargado de generar Identidades en el sistema en base a números aleatorios (algoritmos) para preservar el anonimato de los Votantes, *Inserción de Identidad*, encargado de registrar en el sistema la asignación de una identidad a cada votante, y *Alta Ideas Candidato*, encargado de recoger la presentación y vínculos personales de los candidatos

4. Sistema de votación telemática a través de Internet, según reivindicación 1, en el que el Sistema de Voto está compuesto por los siguientes módulos: *Gestión de Sesión*, encargado de recibir la sesión del Sistema de Anonimato, *Inserción de voto*, encargado de almacenar el voto emitido por el usuario y la identidad en el sistema que le representa, *Fragmentación del voto*, encargado de fragmentar el voto, *Generador de informes*, encargado de generar informes de confirmación para el votante, e *Inserción de bloqueo de voto*, encargado de validar el voto, reflejándolo en el sistema insertando un "1" donde antes había un "0", en la base de datos Relación Usuario-Identidad Sistema.

5. Sistema de votación telemática a través de Internet, según reivindicación 4, en el que el módulo Inserción de voto del Sistema de Voto almacena los votos emitidos por los usuarios en una base de datos diferente a la de autentificación de los usuarios.

6. Sistema de votación telemática a través de Internet, según reivindicación 4, en el que el módulo *Inserción de bloqueo de voto* del Sistema de Voto valida los votos emitidos por los usuarios a través de la base de datos Relación Usuario-Identidad, insertando un "1" en el lugar de un "0".

7. Sistema de votación telemática a través de Internet, según reivindicación 1, en el que el Sistema de Recuento está compuesto por los siguientes módulos: *Control de Acceso*, encargado de filtrar el acceso al sistema, dejando libre transito sólo al usuario que esté registrado, *Contador de Votos*, encargado de leer el informe presentado por el Sistema Verificador para dar acceso a la base de datos Urna electrónica y contabilizar el voto, o, si hay irregularidades, pasar directamente al siguiente módulo, *Generador de Informes Votos-Verificación,* encargado de presentar un informe de los comicios electorales.

8. Sistema de votación telemática a través de Internet, según reivindicación 1, en el que el Sistema de Verificación está compuesto por los siguientes módulos: *Verificación Parcial y Total*, encargado de comprobar que no hay más votantes en el Sistema que votantes censados en el universo de votantes, *Peso de los Votos*, encargado de determinar el debido cumplimiento de las reglas preestablecidas, *Envío de Informes*, encargado de recoger los resultados obtenidos, darles un determinado formato y enviárselos al Sistema de Recuento.

9. Sistema de votación telemática a través de Internet, según reivindicación 1, en el que el Sistema Anonimato, Sistema de Voto, Sistema de Recuento y Sistema de Verificación utilizan tecnologías XML (*eXtensible Markup Language*) y XSLT (*Extensible Stylesheet Language Transformations*) para la presentación de la información.

10. Sistema de votación telemática a través de Internet, según reivindicación 1, en el que el Sistema Anonimato, Sistema de Voto, Sistema de Recuento y Sistema de Verificación utilizan tecnologías LDAP (*Lighweight Directory Access Protocol*) y SGBD (*Sistema de Gestión de Base de Datos*) para el acceso y gestión de los datos.

11. Sistema de votación telemática a través de Internet, según reivindicación 1, en el que el sistema de gestión de las bases de datos (SGBD) incluye como medidas lógicas ante un posible ataque por suplantación de un usuario del

sistema por otro fraudulento, un log del SGBD, la restricción del acceso a determinas tablas o columnas atendiendo al usuario suplantado, y un diseño lógico del sistema en el que los usuarios, el voto y lo votado sean números fragmentados en la base de datos que requieren de algoritmos contenidos en los diferentes sistemas para su des fragmentación.

12. Sistema de votación telemática a través de Internet, según reivindicaciones anteriores, **caracterizado** porque entre los elementos que constituyen la arquitectura básica del sistema se producen las siguientes doce interconexiones o flujos de datos: (1) Clave Pública-Certificado, en el que el sistema Autoridad de Certificación envía al votante las claves públicas para su certificación, (2) Identidad Usuario, en el que el votante envía al Sistema de Anonimato los datos personales y la clave asignada para su autentificación, (3) Datos Usuario, en el que el Sistema de Anonimato, a través del módulo *Check Universo de Votantes*, lee de la base de datos Universo de Votantes el número total de votantes y los datos unívocos de cada votante para su autentificación, (4) Identidad en el sistema, en el que el Sistema de Anonimato re-direcciona al Sistema de Voto la identidad del votante en el sistema sin fragmentar, (5) Identidad en el sistema-voto, en el que el votante le da al Sistema de Voto, su voto junto con la identidad sin fragmentar que le proporciona el Sistema de Anonimato, (6) Voto id-sistema, en el que el Sistema de Voto, a través del módulo *Inserción de Voto*, envía estos datos a la base de datos Urna electrónica, (7) Nº de votos totales-Peso Voto, en el que el Sistema Verificador consulta a la base de datos Urna electrónica, bien a través del módulo *Verificación Parcial y Total*, para contabilizar el total de los votos, o bien a través del módulo *Peso de los Votos*, para saber, en su caso, el peso cuantitativo de cada voto, (8) Nº de votantes, en el que el Sistema Verificador, a través del módulo *Verificación Parcial y Total*, consulta la base de datos Relación Usuario-Identidad, donde aparece el número de votantes parciales que han hecho uso del sistema y el de votantes totales censados, (9) Cod.bloq.Id-usuario (bidireccional), en el que el Sistema de Anonimato, por un lado, a través del módulo *Check Status*, comprueba en la base de datos Relación Usuario-Identidad que el votante se ha autentificado, y por otro lado, a través del módulo *Inserción de Identidad*, actualiza la base de datos local, en donde se introducen los datos personales y la identidad del votante en el sistema (fragmentada), (10) Cod.Bloq.voto, en el que el Sistema de Voto, a través del módulo *Inserción de Bloqueo Voto*, valida el voto del votante en la base de datos Relación Usuario-Identidad generando un bloqueo para que no vote una segunda vez, y en el que el Sistema de Anonimato, a través del módulo *Check Status*, consulta en esta base de datos que el votante ha votado, (11) Test, en el que el Sistema Verificador, a través del módulo *Envío de Informes*, envía al módulo Contador de votos del Sistema de Recuento, el informe de verificación de los comicios electorales, y (12) Nº de Votos, en el que el Sistema de Recuento, a través del módulo *Contador de votos*, accederá a la base de datos Urna electrónica y contabilizará los votos almacenados mediante un algoritmo de desfragmentación de votos.

13. Sistema de votación telemática a través de Internet, según reivindicación 12, **caracterizado** porque para asegurar la comunicación entre el votante y el Sistema en términos de confidencialidad, integridad y accesibilidad, se utilizan certificados autenticados, a través de la Autoridad de Certificación, basados en el estándar X.509, por parte del Servidor y del cliente, y Protocolo SSL (*Secure Socket Layer*).

14. Sistema de votación telemática a través de Internet, según reivindicación 12, **caracterizado** porque para asegurar la comunicación entre los distintos elementos del sistema y el acceso a los diferentes recursos de información web, se utilizan protocolos Ldap (*Lightweight Directory Access Protocol*), que para la primera finalidad es LDAPv3 y, para la segunda, OpenLdap.

15. Sistema de votación telemática a través de Internet, según reivindicación 12, **caracterizado** porque para asegurar el acceso a los servidores web del Sistema, éstos contarán con los siguientes parámetros mínimos de configuración: ServerType, en valor Inetd, ServerRoot, TimeOut, Port, ServerAdmin, ServerName y DocumenRoot.

16. Sistema de votación telemática a través de Internet, según reivindicación 12, **caracterizado** porque para asegurar la gestión de los Logs del Sistema se introduce una modalidad de Logs distribuidos en la que la configuración del fichero /etc/syslog.conf es realizada conjuntamente por tres Administradores asociados a cada sistema principal del Sistema VT: sistema de anonimato, de Voto, de recuento y de verificación, quienes monitorizan los ficheros de log en tres computadoras diferentes aisladas del entorno (sin conexión a Internet u otro tipo de red de comunicación) para cada uno de esos cuatro elementos principales.

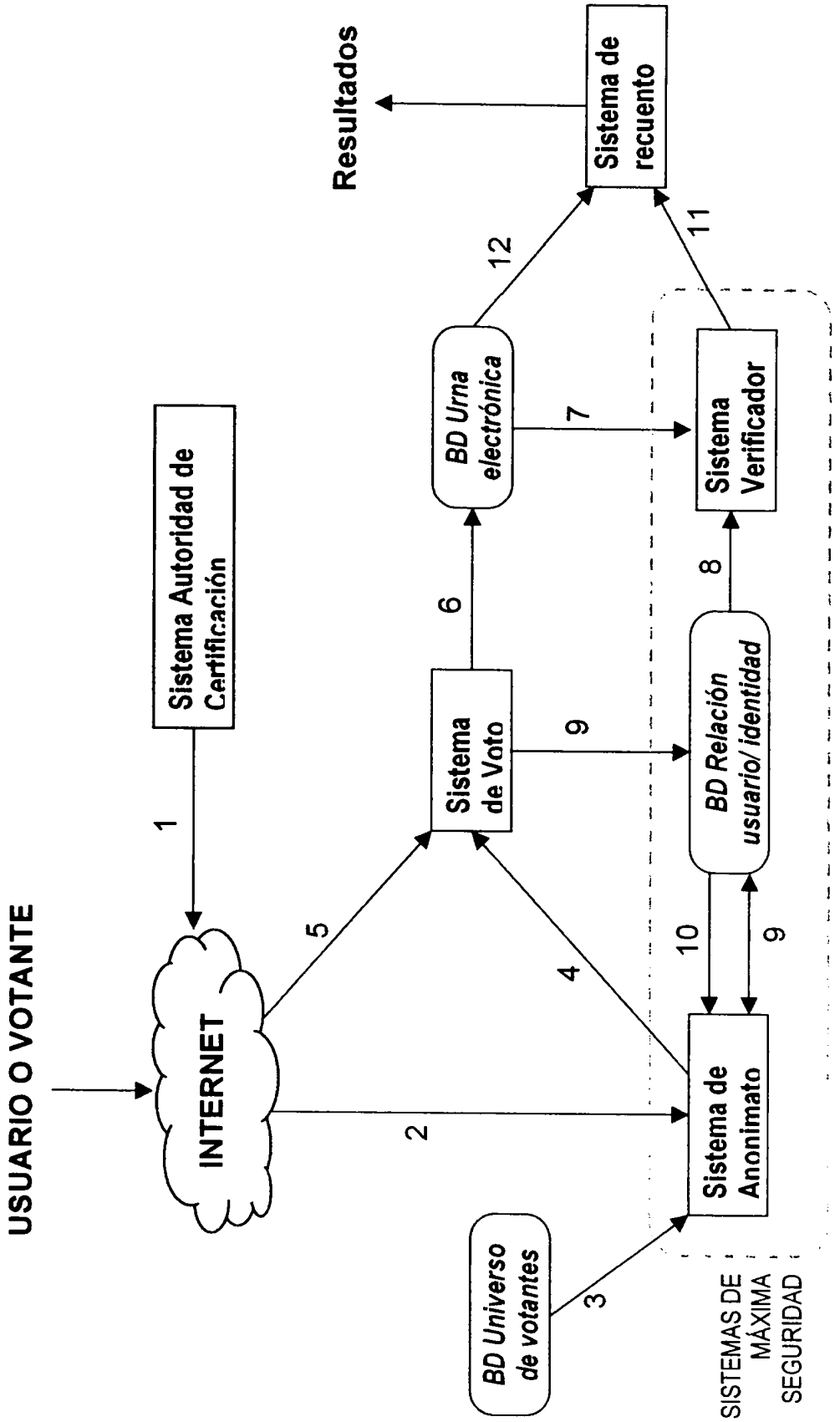
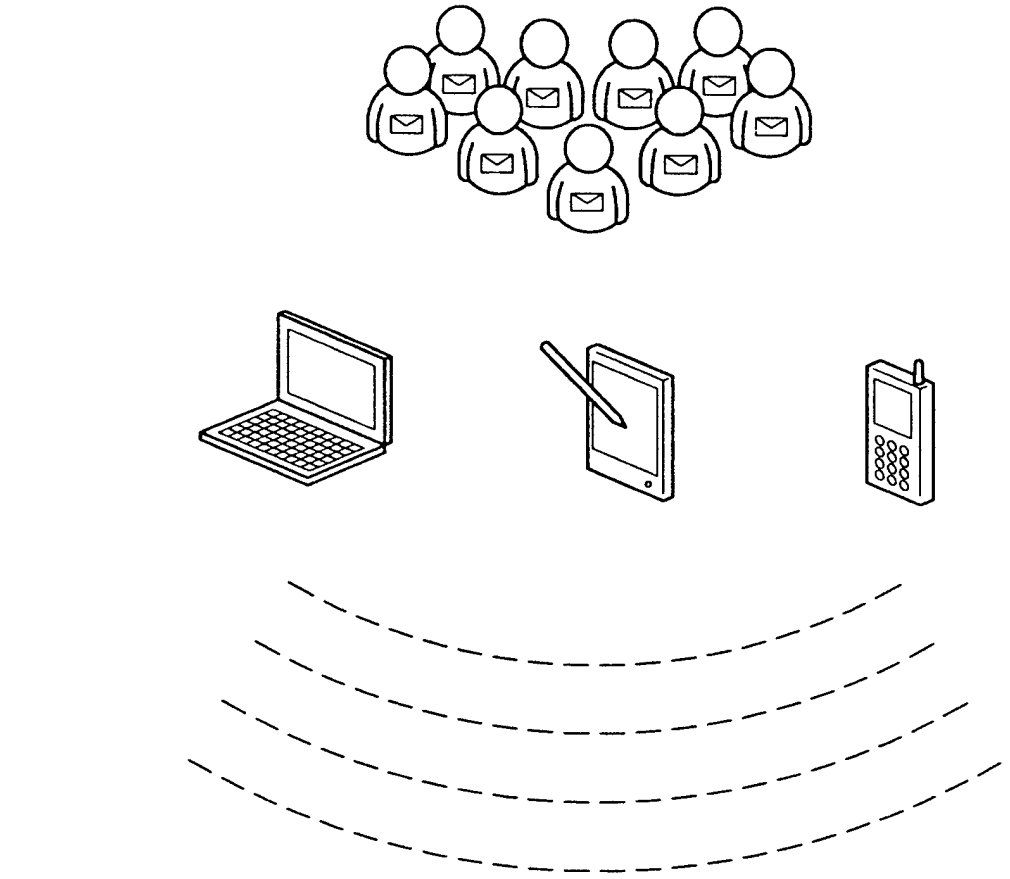

USUARIO O VOTANTE
INTERNET
Sistema Autoridad de Certificación
Sistema de Voto
BD Urna electrónica
Sistema de recuento
Resultados
BD Relación usuario/ identidad
Sistema Verificador
Sistema de Anonimato
BD Universo de votantes
SISTEMAS DE MÁXIMA SEGURIDAD
1
2
3
4
5
6
7
8
9
10
11
12

Figura 1



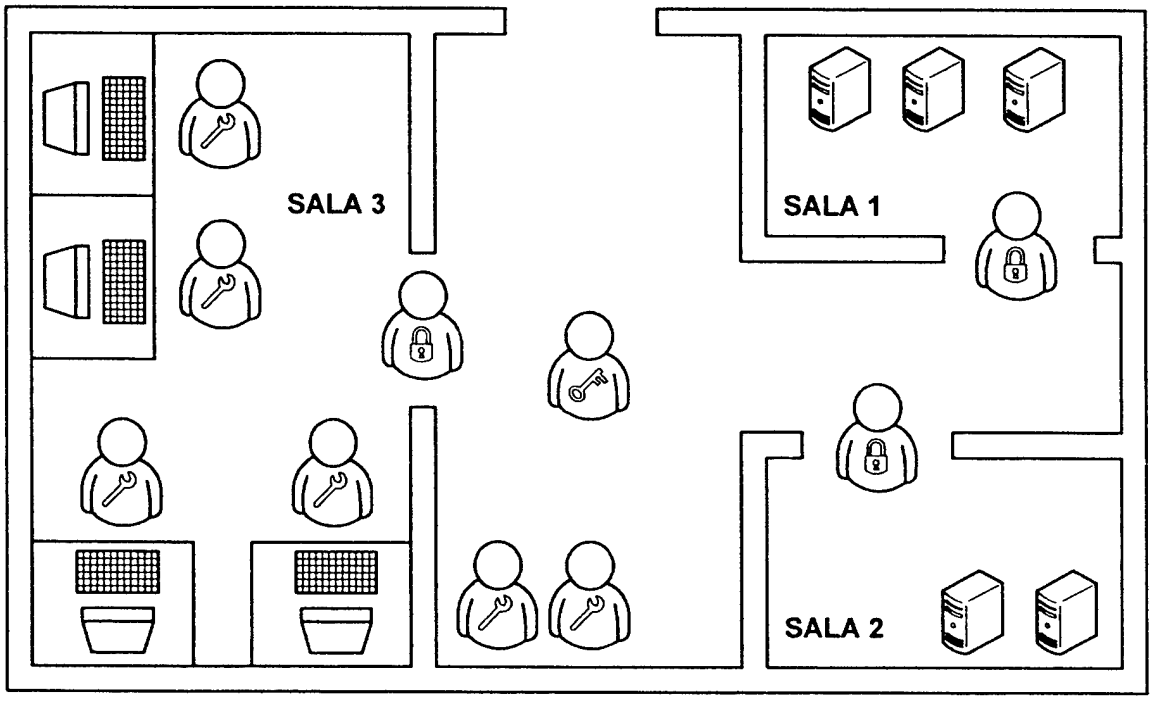


Figura 2

OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) ES 2 283 205

(21) Nº de solicitud: 200503260

(22) Fecha de presentación de la solicitud: **30.12.2005**

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TÉCNICA

(51) **Int. Cl.:** ***G07C 13/00*** (2006.01)
H04L 9/32 (2006.01)

DOCUMENTOS RELEVANTES

Categoría	Documentos citados	Reivindicaciones afectadas
A	WO 03050771 A1 (SCYTL ON LINE WORLD SECURITY) 19.06.2003	
A	US 2002077887 A1 (LONDO SHRADER, T. J.) 20.06.2002	
A	WO 02077929 A2 (VOTEHERE, INC.) 03.10.2002	
A	WO 03062961 A2 (AMERASIA INTERNATIONAL TECHNOLOGY) 31.07.2003	
A	US 2002019767 A1 (BABBIT, V. L. et al.) 14.02.2002	
A	DE 10325491 A1 (SC-INFO+INNO GMBH) 30.12.2004	

Categoría de los documentos citados

X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	Examinador	Página
17.09.2007	A. López Alonso	1/1