

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 554 535**

51 Int. Cl.:

G07C 13/00

(2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **25.04.2008** **E 08750857 (8)**

97 Fecha y número de publicación de la concesión europea: **02.09.2015** **EP 2147415**

54 Título: **Sistema y procedimiento de votación supervisado**

30 Prioridad:

25.04.2007 GB 0708029

10.12.2007 GB 0723998

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
21.12.2015

73 Titular/es:

EVERYONE COUNTS, INC. (100.0%)

4435 Eastgate Mall, Suite 100

San Diego, CA 92121, US

72 Inventor/es:

BURTON, CRAIG ALEXANDER

74 Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

ES 2 554 535 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Sistema y procedimiento de votación supervisado

La presente invención se refiere a un sistema de votación supervisado y en particular a un sistema de votación electrónico. Se refiere también a un procedimiento de funcionamiento del sistema de votación.

5 Los sistemas de votación pueden ser usados para contar, almacenar y/o registrar el número de votos recibidos por cada votante elegible. Dichos sistemas de votación son útiles en muchos campos diferentes, tales como elecciones locales o de gobierno nacional, votaciones impulsadas por medios de comunicación en respuesta a un programa de televisión, por ejemplo, o para entretenimiento, tal como una encuesta, "consulta electrónica", plebiscito, voto deliberativo, votación de preselección de un partido, no gubernamental, de una organización, elecciones sindicales, referéndums u otros
10 procedimientos democráticos. Se apreciará que la invención descrita en la presente memoria puede ser aplicable en muchos campos, aunque en esta solicitud, la descripción se centrará en sistemas de votación usados para elecciones políticas y similares.

Es común que los votos se realicen sobre una papeleta en un colegio electoral o centro de votación (un edificio particular o una habitación en un edificio). Típicamente, las papeletas se reciben en una caja de seguridad por parte de funcionarios en el colegio electoral supervisado y, una vez expirado el plazo para votar, la caja de seguridad es transportada por
15 funcionarios o policías a un centro de recuento central de manera que los votos puedan ser contados y puedan compilarse los totales con los resultados de otros colegios electorales. Este procedimiento de emisión de voto es bien conocido como voto secreto.

Se conocen sistemas de votación basados en la electrónica y comprenden una terminal de votación independiente que tiene un software cargado en la misma. La terminal está programada de manera que presenta al votante la lista de candidatos para la región, municipio o sala particular en el que se encuentra la terminal, de manera que el votante pueda emitir su voto. Durante el funcionamiento, una persona que desea votar llegaría al colegio electoral y consultaría al oficial del censo electoral, que determinaría si esa persona es o no apta para votar. Dichas estaciones de voto electrónico usan típicamente una versión en papel del censo electoral o un registro electrónico con una base de datos instalada en la
20 terminal que usa el presidente del colegio electoral.

Si el votante es apto para votar, el oficial entrega al votante una tarjeta electrónica u otro elemento que activará una de las terminales de votación. A continuación, el votante puede pasar a la terminal, insertar la tarjeta electrónica o elemento, lo que causará la presentación de una lista de candidatos, y emitirá su voto. La votación se almacena en la terminal de votación o en un medio de almacenamiento extraíble en la terminal de votación. Las terminales autónomas o sus medios de almacenamiento son recogidos del colegio electoral y transportados a un centro de recuento para la compilación de los resultados desde cada terminal. Sin embargo, hay varias desventajas con esta disposición, ya que existe la posibilidad de que las terminales podrían ser reprogramadas para alterar los votos que han sido emitidos. Además, las máquinas autónomas o sus medios de almacenamiento extraíbles (por ejemplo, tarjetas de memoria) podrían ser robados, alterados, perdidos o dañados durante el transporte al centro de recuento descartándose de esta manera todos los votos emitidos en esa máquina/distorsionando los resultados de la elección.
30

También es conocido el voto por Internet. Esta disposición comprende típicamente proporcionar a un votante un identificador, tal como un número PIN secreto único, por correo. A continuación, el votante visita un sitio web de votación que requiere la introducción del número PIN. Tras la verificación del PIN, el usuario puede registrar un voto. La votación a través de Internet puede plantear riesgos de seguridad ya que la terminal del votante puede tener baja seguridad (puede verse comprometida o puede ser observada de manera remota). La confianza pública en el voto por Internet es generalmente baja, debido a la posibilidad de fraudes en Internet perpetrados mediante técnicas tales como "phishing".
40

El documento US2004/0024635 A1 describe un sistema de voto electrónico seguro.

A continuación se proporciona, a modo de ejemplo solamente, una descripción detallada de la presente invención con referencia a los dibujos adjuntos en los que:

45 La Figura 1 muestra una realización del sistema de votación de la invención;

La Figura 2 muestra un ordenador personal usado en el sistema de la Figura 1; y

La Figura 3 muestra un diagrama de flujo que ilustra una realización del procedimiento de funcionamiento del sistema de votación de la Figura 1.

La presente invención se refiere a un sistema de votación electrónico, supervisado, en red, con la funcionalidad para permitir a una persona emitir su voto en cualquier colegio electoral que elija.
50

Los aspectos de la invención se describen en la reivindicación independiente 1.

Una realización de un sistema 1 de votación se muestra en la Figura 1. El sistema 1 de votación comprende varias terminales 2, 3, 4 de votación (VO) y terminales 5, 6 de presidente electoral (PO) que son operadas por uno o más miembros 55 del personal. Las operaciones a realizar con la configuración del equipo y la introducción de contraseñas son realizadas por al menos dos miembros 55 del personal de PO que tienen la tarea de establecer la estación 1 de votación para los votantes. Se muestran tres terminales 2, 3, 4 VO y dos terminales 5, 6 PO, pero se apreciará que pueden usarse más o menos terminales de votación o terminales PO.

Típicamente, cada terminal VO tiene una barrera de privacidad alrededor de la misma para prevenir que la pantalla sea visible para votantes que no sean el usuario asignado. La Figura 2 muestra la terminal 2 VO, configurada para permitir que una persona con discapacidad vote sin ayuda. Esta configuración puede requerir una posición particular en el colegio electoral con respecto a las rampas y el suelo, iluminación y una barrera de privacidad alrededor de la terminal VO. Las terminales 2, 3, 4 VO y las terminales 5, 6 PO están situadas en un colegio electoral representado por el recinto 7.

El sistema de votación comprende además un servidor 8 de censo (Censo) que está dispuesto para procesar la información de votación recibida desde las terminales VO y determinar opciones de votación específicas de votante a ser presentadas a cada votante individual usando una de las cabinas 2, 3, 4 de votación electrónica. Además, el sistema 1 de votación comprende un servidor 9 de planificación (Planif.) que está dispuesto para gestionar la asignación de las terminales VO. Un servidor 10 de aplicaciones (Aplic.) es usado para gestionar los registros de sesión de votación electrónica. Las cabinas 2, 3, 4 de votación, las terminales 5, 6 PO, el servidor 10 de aplicaciones, el servidor 9 de planificación y el servidor 8 de censo se comunican a través de una red de comunicaciones que, en esta realización, incluye la Internet 12 pública. Las comunicaciones hacia y desde Internet pueden ser, en muchas realizaciones, a través de firewalls, conmutadores y otros dispositivos de seguridad estándar. En esta realización, la comunicación es a través del conmutador 11. En otras realizaciones, puede usarse una red privada tal como una LAN o una red superpuesta en Internet, tal como una VPN, para las comunicaciones.

Las terminales 2, 3, 4 VO están compuestas por ordenadores personales de propósito general, Figura 2 (por ejemplo, de sobremesa, portátil, tableta, PDA, notebook o dispositivos similares), que tiene unos medios 18 de visualización que comprenden un monitor CRT o una pantalla LCD, por ejemplo, y medios 20 de entrada que comprenden un teclado, por ejemplo. El teclado 20 puede ser un teclado QWERTY convencional, aunque en esta realización está personalizado con botones que corresponden a la información requerida por un usuario para emitir un voto. Otras realizaciones pueden incluir un ratón o un dispositivo 19 de puntero, o un teclado con codificación braille y auriculares/micrófono 17. Por el contrario/adicionalmente, podrían usarse pantallas táctiles. Las terminales 4, 5, 6 VO incluyen también medios de red, tales como una tarjeta de red inalámbrica Wi-Fi (por ejemplo 80211b o comparable) que, a través de un enrutador inalámbrico o pasarela, proporciona los medios 10 para la comunicación con Internet. O puede proporcionarse una conexión por cable a Internet.

Las terminales 2, 3, 4 VO y las terminales 5, 6 PO están "limpias" en el sentido de que no tienen ningún software precargado en las mismas y, en algunas realizaciones, pueden ser proporcionadas sin ninguna unidad de disco duro interno o dispositivo de almacenamiento masivo interno. De esta manera, las terminales 2, 3, 4 VO y las terminales 5, 6 PO requieren la inserción de un "medio de arranque" en un lector apropiado (no mostrado) para funcionar. Típicamente, el medio de arranque (no mostrado) se proporciona en un formato inmutable, tal como un DVD-R o un CDR, y contiene software para permitir que la terminal se comunique con los servidores de aplicaciones 10, de planificación 9 o de censo 8. De esta manera, en la presente realización, el software incluye sólo un sistema operativo basado en Linux, los controladores necesarios para permitir la comunicación y un navegador web habilitado para Java. Esto es ventajoso, ya que las terminales 2, 3, 4 VO y las terminales 5, 6 PO solo tienen la cantidad mínima de software para permitir que puedan proporcionar el servicio de votación, reduciendo por lo tanto significativamente la posibilidad de que una terminal sea reprogramada o que cualquier software malicioso sea incorporado a la misma, por ejemplo. La provisión de este software en medios inmutables que están almacenados y se distribuyen de manera segura hace que la introducción de software incorrecto o malintencionado en las máquinas VO o PO sea muy difícil, y hace que sea más fácil y más seguro, para un experto comprobar que no haya ningún software malicioso (malware, por ejemplo, caballos de Troya) en los equipos. Esta disposición hace que sea muy fácil reemplazar ordenadores que no funcionan correctamente con hardware de recambio ya que el hardware no requiere una configuración ni una instalación de software previa. El uso de ordenadores de propósito general permite que el sistema aproveche la tecnología actual y permite que las máquinas configuradas para votar desempeñen otros papeles fuera de las elecciones, reduciendo de esta manera la carga económica de la propiedad y el mantenimiento del equipo.

En algunas realizaciones, se proporcionan medios de arranque para detener todos los servicios periféricos en un ordenador antes de iniciar la instalación del software indicado anteriormente (es decir, el mínimo requerido para implementar la presente invención). Esto pretende convertir el ordenador en un ordenador a prueba de manipulaciones. En una realización, la desactivación del puerto USB y la compatibilidad Plug-and-Play (PnP) previene que la terminal VO

sea conectada a un dispositivo USB, que si no podría ser usado para introducir un software diferente. En otra realización, el software en el medio de arranque deshabilita teclas en el teclado, por ejemplo para prevenir la combinación CTRL-ALT-DEL u otros comandos especiales que proporcionarían acceso a los usuarios al sistema operativo o a los servicios internos de las terminales PO o VO.

- 5 El servidor 9 de planificación está dispuesto para aceptar conexiones desde y autenticar cada terminal 2, 3, 4 VO en el colegio 7 electoral y otros colegios electorales. En una realización, esto se consigue mediante la provisión de una lista de identidades de máquina en cada medio de arranque. El personal de PO arranca una máquina VO, selecciona una identidad para esa máquina (tal como Máquina de votación 1). A continuación, el personal de PO expulsa el medio de arranque, se mueve a la siguiente máquina y repite el procedimiento (pero esta vez selecciona Máquina de votación 2).
- 10 Cuando cada máquina VO inicia su navegador web, la terminal VO solicita la contraseña expedida con un certificado digital que forma cada identidad de máquina separada. El personal de PO introduce esta contraseña.

- 15 En esta realización de la invención, cada colegio electoral recibe su propio medio de arranque, específico para ese colegio electoral. El servidor de planificación detecta cuándo una identidad específica de máquina es usada más de una vez. La preparación de las terminales PO es realizada mediante un procedimiento similar de arranque y selección de las identidades de máquina a partir de una lista de máquinas PO, sin embargo, el servidor de autenticación es el servidor 8 de censo.

- 20 Esta realización de la configuración supervisa el uso de una identidad de máquina en cada caso de máquina de votación y máquina de supervisor. La identidad de máquina asigna un certificado de cliente HTTPS diferente a cada máquina. El contenido de este certificado (por ejemplo, un valor único establecido en la unidad organizativa (Organisational Unit, OU)) forma la base gracias a la cual el servidor 9 de planificación es capaz de diferenciar entre las máquinas y es capaz también de formar una sesión HTTPS cifrada totalmente autenticada. Esta seguridad hace que sea difícil introducir una máquina VO o PO fraudulenta en la red.

- 25 La invención contempla que el medio de arranque participe en una prueba de validación con el servidor de planificación para determinar si el medio de arranque es una copia legítima no dañada del software para una terminal VO o RO. Esto ocurre de la manera siguiente: el medio de arranque arranca la máquina e inicia el navegador web que está incluido en el software de arranque. El navegador VO consulta al servidor de censo y el navegador VO consulta al servidor de planificación. El servidor de planificación o el servidor de censo responden con un número aleatorio. El software de arranque usa este número aleatorio como una semilla para crear una lista de direcciones aleatorias en su propio medio de arranque. A continuación, el VO lee 512KB o bloques similares desde las direcciones en esta lista y procesa estos datos
- 30 leídos para determinar una suma de comprobación MD5. La suma de comprobación es enviada de nuevo al servidor de planificación o de registro. Los servidores de planificación y de registro albergan una pluralidad de los números aleatorios anteriores y las sumas de comprobación MD5 correctas que deberían resultar con el medio de arranque. Si la terminal no devuelve una suma de comprobación MD5 válida, esto resultaría en un mensaje de error y el medio de arranque usado debería ser desechado.

- 35 Una vez arrancadas todas las máquinas y asignadas sus identidades, el personal 55 de PO solicita una terminal 2, 3 o 4 VO para un votante. Esto ocurre mediante una solicitud desde la terminal 5, 6 PO al servidor 9 de planificación. Cada terminal 2, 3 o 4 VO desocupada consulta periódicamente al servidor 9 de planificación para comprobar si hay una solicitud de sesión de votante en espera. La solicitud desde la terminal PO activa una sesión y, a continuación, la primera máquina de votación libre (cualquiera de entre 2, 3, 4) autentica la sesión al servidor de aplicaciones que, a su vez, sirve las papeletas correctas para el votante. El servidor de aplicaciones registra los resultados de los votos emitidos y genera recibos para los votos que se han recibido correctamente. En esta realización, máquinas separadas o grupos de máquinas proporcionan el servicio de censo 8, de planificación 9 y de aplicaciones 10. En algunas realizaciones, estas máquinas pueden estar situadas en ubicaciones físicas separadas o pueden ser proporcionadas por proveedores externos. En algunas realizaciones, el servidor 10 de aplicaciones es un servicio en una sola máquina, junto con el
- 45 servidor 8 de censo y/o el servidor 9 de planificación.

- El servidor 8 de censo alberga una base de datos de censo electoral que contiene una lista de votantes aptos y la región en la que viven. El servidor 8 de censo puede consultar también al servidor 10 de aplicaciones para determinar si un votante ha votado y, si es así, los medios mediante los cuales ha votado, por ejemplo, voto electrónico o voto en papel. En esta realización, la base de datos de censo electoral del servidor 8 de censo se mantiene continuamente actualizada. En algunas realizaciones, la información de la base de datos del censo electoral es actualizada hasta el día anterior al inicio de la votación (por ejemplo, el día antes de una elección) o es actualizada hasta cualquier otro momento adecuado.
- 50

- En los procedimientos de censo electoral anteriores, frecuentemente se requiere que la información del censo electoral esté finalizada varias semanas antes de una elección con el fin de permitir la impresión y la distribución de los formularios de voto en papel. De manera ventajosa, el sistema de votación de la presente invención permite el acceso a una información de censo electoral mucho más actualizada y usada durante el procedimiento de votación. Además, la invención proporciona un sistema centralizado que previene la votación duplicada o múltiple por una misma persona en
- 55

tiempo real. Anteriormente, la detección de voto múltiple sólo podía llevarse a cabo mediante la recopilación manual de registros de papel marcado (o electrónicos fuera de línea) para encontrar votantes duplicados. En los países en los que el voto es anónimo, la recopilación a posteriori de marcas de registro es demasiado tarde para prevenir el fraude, ya que las papeletas no tienen marcas para identificar al votante y, de esta manera, no hay medios para extraer los votos fraudulentos encontrados.

En algunas realizaciones de la presente invención, se proporciona al votante la opción de si desea votar electrónicamente o mediante voto en papel. Si elige un voto en papel, el supervisor puede imprimir una lista actualizada de las opciones de voto para el votante una vez verificada la identidad del votante. De esta manera, la presente invención permite usar información actualizada con un sistema de voto en papel que funciona en paralelo. La presente invención permite también que el censo electoral refleje inmediatamente un votante como un votante que ya ha votado a través de cualquier canal (votando en un colegio electoral, o un canal remoto tal como el teléfono o Internet, o mediante un voto en papel en el colegio electoral). El registro electrónico de los votos en papel emitidos puede ser comparado con el número de votos en papel contados a partir de la urna en el colegio electoral.

El funcionamiento de las terminales VO del sistema 1 de votación se describirá ahora con referencia al diagrama de flujo mostrado en la Figura 3 que muestra un procedimiento 30 de votación supervisado. Como parte de la configuración, el personal 55 de PO realiza la etapa 31 de arranque y usa el medio de arranque descrito anteriormente para arrancar las terminales VO y PO. A partir de este momento, las terminales VO realizan la etapa 32 y consultan continuamente (en esta realización, cada 15 segundos) al servidor 9 de planificación. En una etapa 33, un votante proporciona información de identidad al personal 55 de PO en el colegio 7 electoral. En el sistema de la presente invención, el votante puede votar en cualquier colegio electoral que esté conectado a la misma red de comunicaciones que el colegio 7 electoral (es decir, Internet). En esta realización, la información de identidad que el votante proporciona al supervisor 55 es información de nombre y de dirección. Esta información es suficiente para identificar al votante en el censo electoral. En otras realizaciones, la información de identidad comprende el nombre, la dirección, el número de papeleta (por ejemplo, según se muestra en una tarjeta de papeleta enviada al votante por correo), un número PIN (por ejemplo, enviado al votante por correo postal o correo electrónico), algún elemento electrónico, tal como una tarjeta inteligente o dispositivo personal o cualquier combinación de los mismos.

En esta realización (pero no en algunas otras realizaciones), se requiere también que el personal 55 de PO verifique su identidad antes de que la terminal 5, 6 PO sea usada o después de que las terminales PO pasen a modo suspendido debido a la inactividad. Con este fin, se muestra una página de inicio de sesión en la terminal 5 de PO. Se requiere que el PO 55 introduzca una contraseña predeterminada que verifica su identidad como supervisor. La contraseña es transmitida de manera segura (por ejemplo, mediante una conexión SSL) con el servidor 8 de censo que verifica la contraseña. Esta contraseña es proporcionada como complemento a la contraseña de certificado digital requerida en la etapa 31 de arranque.

El votante se acerca al personal 55 de PO que usa la terminal 5 o 6 de PO para introducir el nombre del votante, el número de registro u otra información en la etapa 35. La terminal PO consulta al servidor 8 de censo en la etapa 35, cuyas respuestas enumeran una o más direcciones de votantes proporcionadas en la respuesta desde el servidor de censo. A continuación, el PO solicita una dirección al votante y elige esta dirección posiblemente de entre varias direcciones devueltas desde el servidor de censo. Pueden devolverse varias direcciones para apellidos comunes, por ejemplo. Si el personal 55 de PO teclea un número de registro, por otro lado, se espera que se devuelva una única dirección.

Si el votante confirma la dirección, el sistema de PO es usado para consultar (como parte de la etapa 35) si el votante tiene derecho a votar y no ha votado ya en cualquier otro colegio electoral, de manera remota (a través de Internet o por teléfono según el caso) o en papel. Esta respuesta es devuelta desde el servidor de planificación y el servidor de aplicaciones en la etapa 36. Si el votante no ha votado, el PO puede ofrecer al votante el voto en papel o el voto electrónico. Si el votante elige el papel, el PO lo confirma con la terminal de PO, que registra la emisión de papel. Si el votante solicita una terminal electrónica, el PO la solicita en la etapa 37 y el servidor de censo asigna una terminal disponible a través del servidor de planificación en la etapa 38.

El servidor de aplicaciones determina algunas opciones de voto específicas del votante que deberían presentarse al votante en la etapa 40. En esta realización, las opciones de voto comprenden una lista de posibles candidatos a los que puede votar el votante. En diferentes circunscripciones habrá diferentes candidatos electorales y, de esta manera, un votante de una circunscripción podrá votar por un conjunto diferente de candidatos en comparación con un votante de una circunscripción diferente. De esta manera, las opciones de voto son específicas del votante. El procedimiento y el sistema de la presente invención permiten a un votante entrar en un colegio electoral fuera de su propia circunscripción, pero que todavía se le presenten opciones de voto correspondientes a su propia circunscripción. En algunas realizaciones, al votante se le presentan opciones de voto correspondientes sólo a su propia circunscripción. Junto con esto, el sistema de votación de la presente invención es supervisado por el personal 55 de PO que proporciona seguridad adicional y reduce

la probabilidad de que alguien intente realizar un fraude electoral (ya que el votante sabe que están siendo supervisados y que esta supervisión previene la coacción de votantes, entre otras prácticas). Esto es considerablemente diferente al voto a través de Internet desde una terminal no supervisada (por ejemplo, en casa) donde un estafador puede sentirse más confiado al intentar cometer un fraude sin ser observado, sin limitaciones de tiempo y sin riesgo de intervención física. La votación supervisada también hace que la venta de votos sea muy difícil ya que no hay ninguna evidencia que el votante pueda proporcionar después de los hechos para garantizar que ha votado a las preferencias de voto del comprador.

En una etapa 39 siguiente, una, y sólo una, de las terminales 2, 3, 4 de VO desocupadas es seleccionada por el planificador para su uso por el votante. El personal 55 de RO retransmite al votante qué terminal de VO usar. En una realización de la invención, el servidor de planificación asigna al votante la primera máquina 2, 3, 4 de votación disponible por su número específico. A continuación, el administrador de votación aconseja al votante que camine a la máquina de votación, que está claramente etiquetada. Si no hay ninguna máquina disponible, el procesador de votos solicita al administrador de votación que espere. En otra realización de la invención, el servidor 9 de planificación es capaz de comprobar cuál de las cabinas no está siendo usada ya que es capaz de recibir la información de estado desde cada cabina 2, 3, 4. En otras realizaciones, el supervisor 55 prescribe una cabina de votación electrónica para el votante comprobando cuál de las cabinas no está siendo usada (por ejemplo, comprobando si hay alguien en las mismas), y enviando esta información al servidor de planificación. En otra realización de la invención, una máquina VO particular (terminal VO dos en esta realización) está colocada sobre un escritorio alto para acomodar una silla de ruedas y esta terminal específica puede ser asignada manualmente por el personal de PO, si es necesario.

En una etapa 40 siguiente, se activa la terminal de VO de la cabina de votación. Como ejemplo, supóngase que se selecciona la cabina 3 de votación. La cabina 3 de votación mostrará las opciones de voto al votante en su pantalla 18. Al prescribir una cabina de votación para que el votante la use, se proporciona una medida de seguridad adicional ya que el votante no es capaz de elegir una cabina particular y, de esta manera, no tiene conocimiento de qué cabina usará antes de que se asigne el número de cabina. Además, en esta realización sólo se prescribe una de las cabinas 2, 3, 4. Por lo tanto, las opciones de voto específicas del votante sólo necesitan ser activadas en una de las cabinas. No se permite hacer cola en las cabinas como es el caso de la votación en papel.

En la etapa 40, la cabina 3 de votación muestra las opciones de voto al votante. En algunas realizaciones, las opciones de voto se presentan en más de un idioma. En algunas realizaciones, se solicita al votante que elija el idioma preferido, idioma en el que se muestra la información posterior al votante. A continuación, las opciones de voto correctas para ese votante se muestran en el idioma elegido.

En esta realización, las opciones de voto comprenden una lista de candidatos a los que puede votar el votante. En algunas realizaciones, el votante puede tener la opción de leer, ver, escuchar, (o cualquier combinación de estas acciones), la información relativa a uno o más de los candidatos. En otras realizaciones, puede solicitarse al votante que lea/vea/escuche esa información, relacionada al menos con el candidato que está votando antes de finalizar su voto.

En una etapa 41 siguiente, el votante introduce la información de voto usando los medios 17, 19 o 20 de entrada en la cabina 3 de votación. En una etapa 41 adicional, la cabina de votación envía la información de voto al servidor 7 de aplicaciones. En esta realización, esta etapa 41 se lleva a cabo inmediatamente después de que el votante ha votado, es decir, la información de votación de un votante adicional no es obtenida antes de enviar esta información de votación. Como resultado, la cabina 3 de votación nunca tiene información de votación para más de un votante en un momento determinado, y sólo mientras está encendida. Esto minimiza la posibilidad de fraude ya que no se mantiene información de votación histórica en la cabina de votación. Además, si la casilla de votación resulta dañada o es destruida, entonces no se perderá la información de votación histórica. Si alguna máquina de votación de entre las máquinas 2, 3, 4 deja de funcionar, simplemente se apaga y se reemplaza. Si el votante no ha enviado su voto, puede acercarse al supervisor de nuevo y se le puede asignar otra máquina. Si el votante ha terminado de votar, la máquina de reemplazo está preparada inmediatamente para su asignación al siguiente votante. Si un votante abandona su máquina, el tiempo de la sesión de votación del votante expira y la terminal de VO se convierte de nuevo en disponible para los votantes posteriores. Una sesión abandonada puede ser reanudada en un momento posterior dentro del periodo de votación.

Al almacenar la información de voto de manera remota, e inmediatamente, puede hacerse una copia de seguridad de la información inmediatamente. En comparación con los sistemas de votación electrónicos anteriores en los que los votos electrónicos se almacenaban en una cabina electrónica hasta el final del proceso electoral antes de mover los datos desde la cabina de votación electrónica, este sistema es mucho más seguro contra daños en la cabina de votación o los datos durante la elección. Además, la suma central de votos directamente desde los votantes permite una fuerte confirmación de la inclusión del votante en el recuento electoral, permite la colocación de una seguridad perimetral más fuerte alrededor de los votos recogidos y permite el escrutinio directo sobre la llegada de todos los votos en lugar del escrutinio distribuido requerido para los votos que entran en una pluralidad de urnas o máquinas individuales que pueden estar geográficamente muy separadas.

El elemento en red de la solución proporciona también una forma segura, instantánea, de transporte en comparación con

el transporte físico de los cartuchos de memoria de la máquina de votación.

En algunas realizaciones, en los casos en los que es obligatorio votar en una elección (por ejemplo, es obligatorio votar en las elecciones de Australia y las de otros 28 países), los registros electrónicos mantenidos mediante el planificador 9 pueden ser usados como una guía de quién ha votado y quién no ha votado. Si es necesario, pueden adoptarse acciones dirigidas al grupo que no ha votado (por ejemplo, enviándoles una notificación de multa) o al grupo que ha votado (por ejemplo, enviándoles la confirmación de que han votado exitosamente) o ambos.

En una etapa 42 siguiente, el procedimiento 30 de esta realización comprende emitir un recibo al votante. El recibo tiene la forma de un código (en esta realización, un código alfa-numérico de 12 dígitos). El recibo no contiene la identidad del votante, ni las opciones de voto que tomó el votante. En esta realización, el recibo puede ser usado posteriormente (cuando los votos han sido descifrados) para verificar que un votante ha votado con éxito en la etapa 50. En esta realización, esto se consigue haciendo que el votante inicie sesión en un sitio web de comprobación de recibos e introduzca una "palabra clave" creada como una parte de la emisión de su recibo de votación. Esta "palabra clave" no es una contraseña, sino una palabra solicitada al votante durante la votación, que puede recordar fácilmente. La palabra clave es usada para vincular el recibo con un votante específico. El sitio web de comprobación de recibos muestra un código de recibo actual para el votante (este debería coincidir con el código de recibo del votante en la etapa 51 que se proporcionó en el momento de la votación). El recibo es generado a partir de la palabra clave y la información contenida sólo en el voto cifrado. Si coincide, entonces el voto ha sido entregado a las autoridades que descifran los votos con éxito y sin alteración, pérdida o daño. Si no coincide, entonces el votante tiene la capacidad de informar acerca de esta circunstancia. Debido a que el votante es la única persona que conoce la "palabra clave", el votante es la única persona que puede saber si su recibo coincide y, de esta manera, no hay ninguna posibilidad de que este servicio de comprobación de recibos sea reemplazado en el servidor con una versión troyana que intenta proporcionar recibos.

Pueden realizarse varias modificaciones a la presente invención sin apartarse de su alcance. Por ejemplo, en algunas realizaciones, el personal de PO puede no estar presente en persona, sino a través de medios remotos, tal como puede ser posible con una terminal de PO más unos medios de automatización o de detección adecuados (por ejemplo, una cámara).

En otra realización, el gobierno ha enviado al votante un número de identificación de votante (por ejemplo, por correo postal), un VIN (Voter Identification Number, número de identificación de votante). Es posible que el votante tenga que proporcionar ese VIN al personal de PO para tener permiso para votar. O puede solicitarse al votante que teclee su VIN en la cabina de votación para ser autenticado.

REIVINDICACIONES

1. Procedimiento de votación supervisado para permitir que un votante vote bajo la supervisión de un supervisor (55) en una cabina de votación que incluye una terminal (2, 3, 4) de votación en la que el votante puede votar, en el que la terminal (2, 3, 4) de votación está dispuesta para comunicarse de manera segura con un sistema (1) de votación electrónico, en el que la terminal (2, 3, 4) de votación comprende un sistema de ordenador capaz de leer un medio inmutable, en el que el procedimiento comprende que:
 - el votante proporcione información de identidad al supervisor (55);
 - el supervisor (55) verifique la identidad del votante y envíe la información de identidad desde una terminal (5, 6) de presidente a un servicio (8, 9, 10) de administrador de votación remoto, que determina las opciones de voto específicas del votante que se presentarán a ese votante;
 - el servicio (8, 9, 10) de administrador de votación envíe detalles de las opciones de voto específicas del votante a la terminal (2, 3, 4) de votación;
 - la terminal (2, 3, 4) de votación muestre las opciones de voto al votante;
 - la terminal (2, 3, 4) de votación reciba la información de votación desde el votante; y
 - la terminal (2, 3, 4) de votación envíe la información de votación a un procesador (8, 9, 10) de votos; en el que el procedimiento comprende además que:
 - la terminal (2, 3, 4) de votación reciba un número desde el servicio (8, 9, 10) de administrador de votación;
 - la terminal (2, 3, 4) de votación lea los datos desde el medio inmutable en las direcciones creadas con el número;
 - la terminal (2, 3, 4) de votación genere una suma de comprobación de los datos leídos desde el medio inmutable;
 - la terminal (2, 3, 4) de votación envíe la suma de comprobación al servicio (8, 9, 10) de administrador de votación; y
 - el servicio (8, 9, 10) de administrador de votación autentique la terminal (2, 3, 4) de votación, usando la suma de comprobación.
2. Procedimiento según la reivindicación 1, que comprende además procesar la información de votación en el procesador (8, 9, 10) de votos.
3. Procedimiento según la reivindicación 1 o la reivindicación 2, en el que la terminal (2, 3, 4) de votación envía la información de votación al procesador (8, 9, 10) de votos antes de recibir un votante subsiguiente.
4. Procedimiento según cualquiera de las reivindicaciones 1 a 3, en el que la terminal (2, 3, 4) de votación está conectada a una red de comunicaciones a través de la cual recibe información desde el administrador de votación; o envía información al procesador de votos; o ambos.
5. Procedimiento según cualquiera de las reivindicaciones anteriores, para su uso cuando se proporcionan una pluralidad de cabinas de votación, en el que el procedimiento comprende enviar detalles de las opciones de voto específicas del votante a la terminal (2, 3, 4) de votación de sólo una de las cabinas, en el que el procedimiento comprende además indicar al votante qué cabina puede usar el votante.
6. Procedimiento según la reivindicación 2 o cualquier reivindicación anterior que dependa directamente o indirectamente de la reivindicación 2, en el que el procesamiento de la información de votación en el procesador de votos se realiza sobre la marcha, una vez termina la votación, periódicamente o en cualquier otro momento adecuado.
7. Procedimiento según la reivindicación 2 o cualquier reivindicación anterior que dependa directa o indirectamente de la reivindicación 2, en el que el procesamiento de la información de votación comprende un recuento de votos.
8. Procedimiento según cualquiera de las reivindicaciones anteriores, en el que el administrador de votación remoto determina las opciones de voto específicas del votante correlacionando la identidad del votante con una lista de posibles opciones de voto para diferentes votantes.

9. Procedimiento según la reivindicación 8, en el que el administrador de votación es capaz de acceder o consultar un censo electoral electrónico, que se actualiza continuamente, hasta el día anterior al comienzo de la votación, o cualquier otro momento adecuado.
- 5 10. Procedimiento según la reivindicación 9, cuando depende de la reivindicación 4 o cualquier reivindicación anterior que dependa directa o indirectamente de la reivindicación 4, en el que la red de comunicaciones se usa para la comunicación entre la cabina de votación y un servidor remoto en el que está almacenado el censo electoral electrónico.
11. Procedimiento según cualquiera de las reivindicaciones anteriores, en el que las opciones de voto comprenden una lista de candidatos electorales.
- 10 12. Procedimiento según cualquiera de las reivindicaciones anteriores, que comprende además proporcionar al votante un recibo indicativo de o derivado de la información de votación.
13. Procedimiento según la reivindicación 12, que comprende que el votante verifique que su voto no ha sido cambiado, después de salir de la cabina de votación, usando su recibo.
- 15 14. Procedimiento según cualquiera de las reivindicaciones anteriores, que comprende además verificar la presencia del supervisor antes de que el supervisor verifique la identidad del votante.
15. Procedimiento según cualquiera de las reivindicaciones anteriores, en el que el administrador de votación comprende el procesador de votos.
- 20 16. Procedimiento según cualquiera de las reivindicaciones anteriores, que comprende además proporcionar a la cabina de votación sólo el software necesario para mostrar las opciones de voto al votante, recibir información de votación desde el votante y enviar la información de votación al procesador de votos, y ningún software adicional.
17. Procedimiento según la reivindicación 16, que comprende además comprobar el software instalado en la cabina de votación para garantizar que no se ha instalado software adicional en la misma.
18. Procedimiento según la reivindicación 12 o 13, que comprende además que la terminal de votación reciba una palabra clave desde el votante, en el que el recibo es derivado también a partir de la palabra clave.
- 25 19. Procedimiento según cualquiera de las reivindicaciones anteriores, en el que el procedimiento comprende además que la terminal (2, 3, 4) de votación use las instrucciones de arranque en un medio inmutable; y que la terminal (2, 3, 4) de votación ejecute las instrucciones en el medio inmutable para detener los servicios periféricos que permitirían la introducción de software malicioso a la terminal (2, 3, 4) de votación.
- 30 20. Procedimiento según cualquiera de las reivindicaciones 1-17, en el que al menos un servidor "back-end" proporciona el servicio de administrador de votación y el procesador de votos y en el que el medio inmutable almacena un sistema operativo y software para facilitar la provisión de un cliente "front-end" para la comunicación con al menos uno de los servidores "back-end".

Figura 1

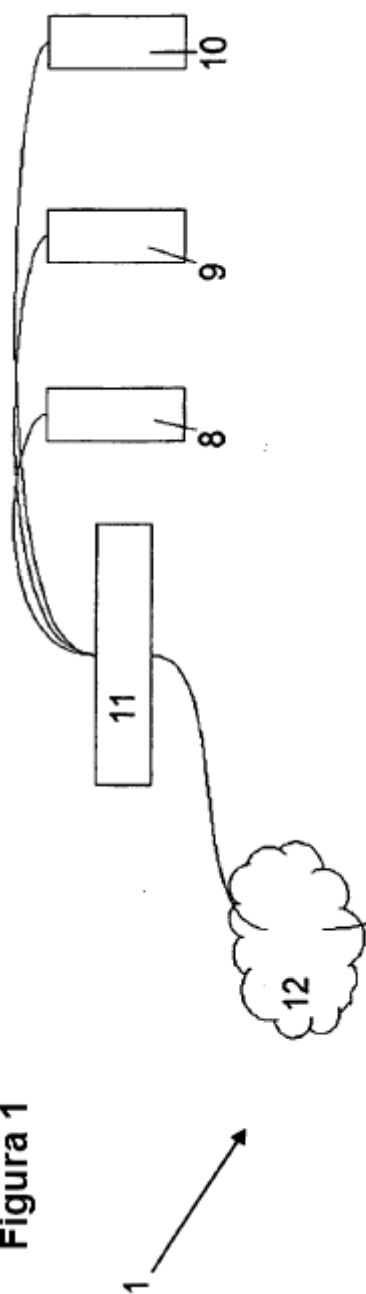


Figura 2

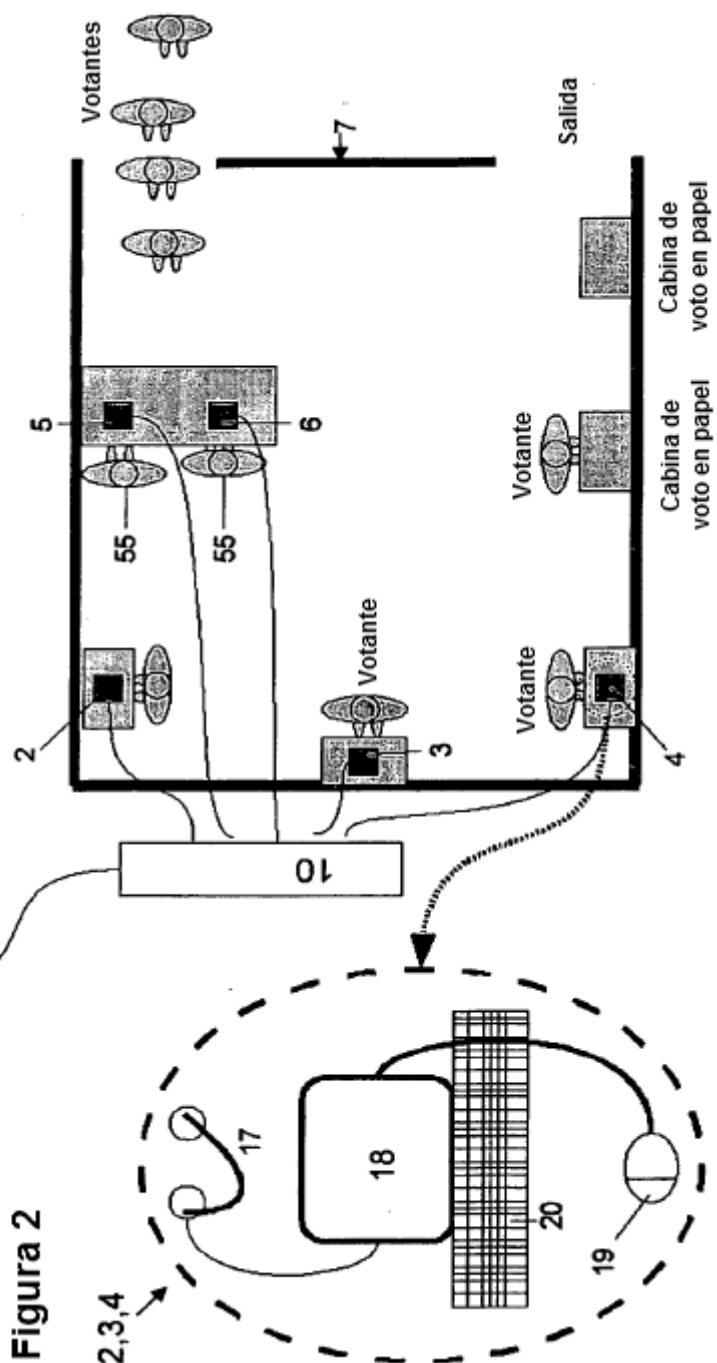


Figura 3

