(12) SOLICITUD INTERNACIONAL PUBLICADA EN VIRTUD DEL TRATADO DE COOPERACIÓN EN MATERIA DE PATENTES (PCT)

(19) Organización Mundial de la Propiedad Intelectual
Oficina internacional

(43) Fecha de publicación internacional
2 de Noviembre de 2006 (02.11.2006)

PCT

(10) Número de Publicación Internacional
WO 2006/114452 A1

(51) Clasificación Internacional de Patentes:
G07C 13/00 (2006.01)

(21) Número de la solicitud internacional:
PCT/ES2005/000215

(22) Fecha de presentación internacional:
26 de Abril de 2005 (26.04.2005)

(25) Idioma de presentación: español

(26) Idioma de publicación: español

(71) Solicitante *(para todos los Estados designados salvo US)*: **SCYTL SECURE ELECTRONIC VOTING, S.A.** [ES/ES]; Calle Entença, 95, E-08015 Barcelona (ES).

(72) Inventores; e

(75) Inventores/Solicitantes *(para US solamente)*: **DAZA FERNANDEZ, Vanesa** [ES/ES]; c/Camí del Colomer 3-9, pis 2n C, E-08190 Sant Cugat Del Vallès (ES). **PUIG-GALÍ ALLEPUZ, Jorge** [ES/ES]; Rbla. Ribatallada 31, Casa 2, 1-3, E-08190 Sant Cugat Del Vallès (ES). **RIERA JORBA, Andreu** [ES/ES]; P. Església, 5, 3, E-08251 Sant Pedor (ES). **VALLÉS FONTANALS, Pere** [ES/ES]; Mejía Lequerica 34, 2-1, E-08028 Barcelona (ES).

(74) Mandatario: **TORNER LASALLE, Elisabet**; c/Bruc, 21, E-08010 Barcelona (ES).

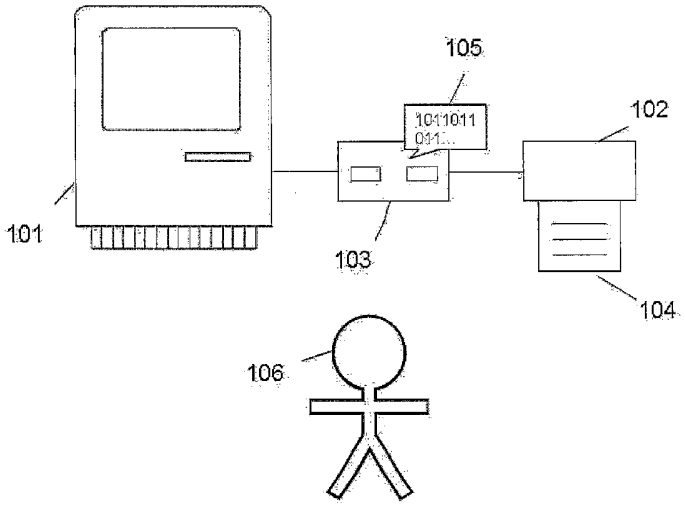
(81) Estados designados *(a menos que se indique otra cosa, para toda clase de protección nacional admisible)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Estados designados *(a menos que se indique otra cosa, para toda clase de protección regional admisible)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), euroasiática (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europea (AT, BE, BG, CH, CY, CZ, DE, DK,

[Continúa en la página siguiente]

(54) Title: AUDITABLE METHOD AND SYSTEM FOR GENERATING A VERIFIABLE RECORD OF VOTES THAT IS SUITABLE FOR ELECTRONIC VOTING

(54) Título: MÉTODO Y SISTEMA AUDITABLES PARA LA GENERACIÓN DE UN REGISTRO VERIFICABLE APLICABLE A VOTACIÓN ELECTRÓNICA



(57) Abstract: The invention relates to an auditable method and system for generating (203) a verifiable record of votes that is suitable for electronic voting. The inventive method is characterised in that a voting module (101), an auditing module (103) and a verification module (102) perform the following steps in which: voting options are selected (201) by the voter (106) in the voting module (101); the voting options are sent (202) from the voting module (101) to the auditing module (103); a record of votes (104) is generated (203) in the verification module (102), which contains the voting options selected by the voters (106) in the voting module (10); the voter (106) confirms (204) that the record of votes (104) contains the voting options that s/he selected in the voting module (101) by direct verification of the record of votes (104); and auditing information is generated (205) in the auditing module (103) in order to secure the electronic vote and/or the associated record of votes (104) which are both generated from the voting options (201) selected and confirmed (204) by the voter (106).

[Continúa en la página siguiente]

WO 2006/114452 A1

EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Para códigos de dos letras y otras abreviaturas, véase la sección "Guidance Notes on Codes and Abbreviations" que aparece al principio de cada número regular de la Gaceta del PCT.

Publicada:

— *con informe de búsqueda internacional*

(57) Resumen: Método y sistema auditables de generación 203 de un registro verificable aplicable a votación electrónica. El método se caracteriza porque un módulo de votación 101, un módulo de auditoría 103 y un módulo de verificación 102 realizan las siguientes etapas: - selección 201 de las opciones de voto por parte del votante 106 en el módulo de votación 101, - envío 202 de las opciones de voto del módulo de votación 101 al módulo de auditoría 103, - generación 203 en el módulo de verificación 102 de un registro de voto 104 que contiene las opciones de voto seleccionadas por el votantes 106 en el módulo de votación 101, - confirmación 204 del votante 106 de que el registro de voto 104 contiene las opciones de voto seleccionadas por el votante 106 en el módulo de votación 101 mediante una verificación directa del registro de voto 104 y, - generación 205 de cierta información de auditoría en el módulo de auditoría 103 para proporcionar seguridad al voto electrónico y/o al registro de voto 104 asociado, generados ambos a partir de las opciones de voto seleccionadas 201 y confirmadas 204 por el votante 106.

METODO Y SISTEMA AUDITABLES PARA LA GENERACIÓN DE UN REGISTRO VERIFICABLE APLICABLE A VOTACION ELECTRONICA

Campo de la invención

La presente invención se enmarca primariamente dentro del campo de la votación electrónica e introduce un método auditable para la generación de un registro de voto verificable por un votante, mediante el uso de protocolos criptográficos. El método proporciona una información de auditoría, que permite garantizar ciertas propiedades necesarias en un proceso de votación como la integridad de dicho registro de voto, su autenticidad o el no-repudio, evitando la adición de votos falsos o la modificación de votos que se han emitido correctamente.

El citado registro de voto se genera, según es conocido en el estado de la técnica en un módulo de verificación, tal como una impresora, a partir de una o más opciones de voto seleccionadas por el votante en un módulo de votación, tal como un DRE. La finalidad de dicho registro de voto es facilitar que el votante verifique directamente que las opciones del registro de voto impreso coinciden con las opciones seleccionadas previamente por el propio votante en el módulo de votación. La generación de un registro de voto para cada voto emitido permite una auditoría paralela del proceso electoral.

La invención también se refiere a un módulo de auditoría fácilmente auditable para la implementación del método propuesto. Este módulo se encuentra intercalado entre el módulo de votación y el módulo de verificación.

Antecedentes de la invención

En un método de votación electrónica, un votante o una pluralidad de ellos emiten sus votos desde un dispositivo electrónico, que suele denominarse terminal de votación. El votante selecciona en dicho terminal de votación la totalidad o parte de las opciones de voto y verifica en el propio terminal de votación que dichas opciones seleccionadas reflejan su intención de voto. Tras confirmar que dichas opciones coinciden con su intención de voto, procederá a

la emisión del voto, que será almacenado electrónicamente para facilitar su posterior recuento. Para garantizar el adecuado desarrollo de una elección, es importante que el voto se almacene correctamente (esto es, tal como ha sido emitido por el votante) y que los procesos de recuento se realicen sobre los votos almacenados. Por lo tanto es importante que los terminales de votación electrónica incorporen medidas que garanticen estas propiedades.

Las primeras máquinas de votación electrónica, conocidas como DRE (del inglés, Direct Recording Electronic), fueron introducidas en los Estados Unidos en los años 70 (US-B1-3.934.793). En ellas el votante procede a la emisión del voto en el terminal de votación donde, tras confirmar si las opciones seleccionadas reflejan sus opciones de voto, los votos emitidos se registran y almacenan electrónicamente en el propio DRE.

El problema principal de estos terminales es que no ofrecen un registro independiente y paralelo de los votos en el que el votante pueda verificar si sus opciones de voto se han registrado correctamente antes de emitir el voto. De este modo se podrían detectar errores en el registro de las opciones de voto seleccionadas, antes de que los votos fueran emitidos. De este modo se podrían evitar la mayoría de las irregularidades detectadas actualmente, como que una urna contenga más votos que votantes. Adicionalmente, este registro paralelo se puede utilizar en caso de problemas para hacer un recuento paralelo.

Otro problema es la falta de medidas de protección de los votos almacenados. En muchos casos las medidas de protección que se utilizan son insuficientes y ponen en riesgo la integridad de los votos y en consecuencia la honestidad de la elección.

Otro problema de este tipo de terminales es la dificultad de su auditoría. La mayoría de los terminales de votación electrónica existentes en el mercado son dispositivos complejos, combinación de una arquitectura hardware y software, y generalmente se encuentran protegidos por derechos de propiedad intelectual o utilizan componentes (p.e. software) que se encuentran sujetos a estos derechos. Todo ello provoca una gran opacidad respecto a cómo se lleva a cabo interiormente el proceso electoral en los terminales de votación y, por consiguiente, hace incrementar la incertidumbre de una posible manipulación de los votos emitidos desde el terminal de votación. Además, los procesos de

auditoría destinados a verificar el cumplimiento de los requisitos necesarios para garantizar la seguridad de una elección y detectar posibles prácticas fraudulentas son, en general, costosos y poco transparentes. De hecho, habitualmente se realizan en laboratorios independientes que deben firmar contratos de confidencialidad muy estrictos. Estos son algunos de los principales motivos por los que todavía existe un gran número de escépticos en relación con el uso de dichos terminales de votación electrónica.

Dicha ausencia de verificación del registro correcto del voto, insuficiencia de medidas de protección de los votos emitidos y dificultad de auditoría han sido puestas de manifiesto en numerosos estudios recientes, como el comúnmente denominado Informe Hopkins (Khono T., Stubblefield A. y Rubin A. *Analysis of an Electronic Voting System.* Johns Hopkins Information Security Institute Technical Report TR-2003-19) publicado en julio de 2003 y en el que se ponía en entredicho la seguridad de los DREs de uno de los mayores fabricantes americanos. A este informe se sumaron otros como el análisis de seguridad de las máquinas de votación electrónica realizado por la comisión de voto electrónico de Irlanda (*First Report of the Comission on Electronic Voting on the Secrecy, Accuracy and Testing of the Chosen Electronic Voting System*) y que corroboraba los problemas de seguridad que comportan el uso de las máquinas de votación electrónica (de tipo DREs) en los procesos electorales de ese país.

Fruto de toda esta incertidumbre, han surgido diferentes propuestas en este campo con el principal objetivo de paliar esta falta de seguridad y auditoría en los procesos electorales que utilizan DREs, permitiendo garantizar en cierta manera que la máquina de votación electrónica registra exactamente aquellos votos emitidos por los votantes , y preserva la integridad y privacidad de dichos votos.

Un primer grupo de propuestas se basan en la utilización de protocolos criptográficos para la protección de los votos y para facilitar la auditoría de la elección. Estas propuestas, como las descritas en (EP-B1-1 224 767, WO-A3-02/077754, WO-A2-03/071491, WO-A1-03/050771 y la solicitud de patente PCT/ES04/000350), garantizan el correcto desarrollo del proceso electoral mediante la protección criptográfica de los votos digitales emitidos y la generación de un registro de verificación para el votante. Este registro de

verificación está basado en un recibo de voto, generado mediante técnicas criptográficas y que puede utilizar el propio votante una vez finalizada la elección para verificar que su voto se ha tenido en cuenta en el recuento. Este recibo no revela ninguna de las opciones de voto seleccionadas por el votante, evitando así problemas como posibles coacciones o venta de votos. El inconveniente principal de estas propuestas criptográficas es que dicho recibo no puede utilizarse en un recuento paralelo, puesto que no contienen las opciones de voto seleccionadas. Por otro lado, la verificación a partir del recibo de voto de que las opciones de voto registradas por el terminal de votación son las correctas, no es un proceso directo para el votante. En este caso el votante debe confiar en que estos procesos sean seguros.

Existe un segundo grupo de soluciones basadas en la impresión en papel del voto en claro, esto es, imprimiendo las opciones de voto seleccionadas por el votante. De esta manera se proporciona un registro paralelo del voto electrónico generado en el terminal de votación. Este voto en papel permite al votante verificar visualmente el contenido del voto antes de ser emitido. Si el votante confirmar que las opciones de voto impresas corresponden con su intención de voto, el voto impreso permite realizar un recuento paralelo de los votos si fuera necesario, facilitando una auditoría de los resultados finales.

La primera solución basada en la impresión en papel de los votos, fue introducida por la Dr. Mercuri a principio de la década de los 90 (Mercuri, R. *Facts About Voter Verified Paper Ballots*). Esta solución, conocida también como el *método Mercuri*, requiere que el voto impreso, con las selecciones realizadas en el terminal de votación, esté protegido del votante mediante un medio transparente (cristal o visor). La corrección del voto es entonces examinada por el votante a través de este cristal o visor de modo que el votante no pueda manipular de forma accidental o malintencionada el voto impreso. Finalmente, si el votante está de acuerdo, el voto es depositado de manera mecánica en una urna, sin que el votante pueda manipularlo. En caso de que el votante no esté de acuerdo, el voto debería ser destruido o marcado como inválido antes de ser depositado mecánicamente en la urna. Uno de los principales problemas de este método es que no permite la verificación del voto a votantes con discapacidades visuales, puesto que el método requiere intrínsecamente que se realice una

verificación visual del método. Por otro lado, no queda muy claro qué ocurre si por un error del terminal de votación, aunque el votante no esté de acuerdo con las opciones de voto impresas, éste se introduce en la urna como válido. Otro problema es que, aunque la urna protege la integridad del voto impreso contra manipulaciones del votante, ésta no garantiza la integridad posterior del voto en papel una vez haya sido emitido. Es decir, no evita la adición, substitución o eliminación de votos en la urna por parte de terceros con acceso a la urna. Además se trata de una solución costosa y de difícil gestión, puesto que implica la adición de una urna específica por terminal de votación.

Con el fin de agilizar el proceso de recuento, existen otras soluciones basadas en la impresión del voto en papel, que no requieren el uso de medidas para la protección del voto impreso. En este grupo encontramos soluciones como las propuestas en US2003/006282-A1, US 2004/0195323-A1 o la publicación Keller A. M. *et at, A PC-Based Open Source Voting Machine with an Accesible Voter Verifiable Paper Ballot*. A diferencia de la solución Mercuri, estas soluciones utilizan códigos o tintas especiales para proteger la integridad del voto en el momento de la impresión del voto. De este modo se evita el recuento de votos que no hayan sido generados por terminales válidos. En este grupo el voto, una vez confirmado, se guarda electrónicamente y el votante debe poner el voto impreso en la urna física correspondiente. El principal problema de estas soluciones radica en la imposibilidad de garantizar un registro coherente de los votos electrónicos y los votos impresos en papel. Esto es debido principalmente a que no se puede garantizar que el votante deposite el voto en papel en la urna una vez emitido en el terminal de votación. Esta aproximación genera más confianza de los votantes en el voto impreso en papel que en el voto electrónico. Por otro lado, al permitir al votante acceder a los votos impresos en papel que contienen las opciones de voto en claro, se facilitan prácticas fraudulentas como la coacción o la venta de votos. Además, aunque utilizan códigos o tintas especiales para garantizar la integridad o autenticidad del voto, estas marcas no son verificables por los votantes sin medios electrónicos. De este modo un mal funcionamiento o manipulación del terminal de votación podría permitir invalidar votos válidos verificados y emitidos por el votante sin que éste fuera consciente de un tal error.

Existe pues la necesidad de introducir un nuevo método para la generación de un registro de voto verificable por el votante, que facilite la auditoría y recuento manual de dicho registro, que pueda ser utilizado independientemente por personas con discapacidades visuales y que permita garantizar la integridad de dicho registro sin facilitar su invalidación por culpa de errores o manipulaciones.

Breve exposición de la invención

La presente invención describe un método fácilmente auditable para la generación 203 de un registro de voto 104 que contenga de forma explícita las opciones de voto seleccionadas por dicho votante 106 en un módulo de votación 101. Este registro de voto 104 además puede ser utilizado para la realización de un recuento paralelo de los votos emitidos. La invención también se refiere a las características de un módulo de auditoría 103 asociado a un módulo de votación 101 y un módulo de verificación 102, que constituyen un sistema de votación electrónica que permite la implementación de dicho método.

Así, un primer objetivo de la presente invención es definir un método seguro para generar un registro de voto 104 que permita a los votantes 106 la verificación directa de dicho registro de voto 104, tal como va a ser almacenado.

Es también objetivo de la invención permitir al votante 106 invalidar el registro de voto 104 en caso de que éste no refleje la intención de voto del votante 106, sin que una vez invalidado dicho registro pueda ser confundido en ningún caso con un registro válido. Esta invalidación no debe impedir al votante 106 volver a repetir el proceso de selección 201 y confirmación 204 para acabar emitiendo un voto válido.

Otro objetivo de esta invención es permitir que el mismo registro de voto 104 pueda utilizarse directamente en un recuento manual o mecánico, entendiendo por manual un proceso no mecanizado llevado a cabo por personas sin necesidad de conocimientos técnicos.

Con el fin de proteger la integridad, autenticidad y no-repudio de los registros de voto emitidos, es otro objetivo del método generar una marca que permita verificar la integridad del registro de voto 104 una vez confirmado. Esta

marca permitirá verificar que el voto ha sido emitido desde un dispositivo válido y no ha sido alterado una vez confirmado por el votante 106.

Es otro objetivo de esta invención evitar que errores aislados o manipulaciones intencionadas en el módulo de votación 101 y en el módulo de auditoría 103 puedan invalidar registros de voto o votos electrónicos.

Otro objetivo de la presente invención es proporcionar un mecanismo que reduzca el esfuerzo de auditoría de los sistemas de votación electrónica, centrando dicha auditoría en el módulo de auditoría 103.

La presente invención también permite proteger la integridad de los votos electrónicos almacenados en el módulo de votación 101, facilitando la detección de inconsistencias en caso de que el recuento de los registros de voto no coincida con el de dichos votos electrónicos.

Por último, pero no menos importante, la presente invención tiene como objetivo no limitar su campo de aplicación a los entornos de votación electrónica, sino que también contempla la posibilidad de utilizar el método descrito para proporcionar por ejemplo integridad a aquellos registros de documentos electrónicos consideradas de relevada importancia.

El método propuesto se caracteriza por comprender las siguientes etapas básicas: recibir en un módulo de auditoría 103 una información digital que contiene unas opciones de voto seleccionadas en un módulo de votación 101; generar en un módulo de verificación 102 un registro de voto 104 verificable por el votante 106 que contenga las opciones de voto seleccionadas por el votante 106 recibidas por el módulo de auditoría 103; confirmar si el registro de voto 104 contiene las opciones de voto que el votante 106 ha seleccionado en el módulo de votación 101; y generar en el módulo de auditoría 103 una información que permita verificar la validez del registro de voto 104, a partir del resultado de la confirmación.

Asimismo, el método propuesto permite el uso de más de un módulo de verificación 102 adicional para permitir además una verificación alternativa para personas con discapacidades visuales.

En caso de que el votante 106 confirme que el registro de voto 104 no contiene su intención de voto, el método permite invalidar dicho registro de

forma permanente sin que éste pueda ser confundido posteriormente con un registro válido.

También se contempla la posibilidad de que cada voto disponga de un identificador único que puede ser generado de forma colaborativa entre los módulos de votación y de auditoría.

El método propuesto comprende unas etapas adicionales que permiten la generación 205 compartida de un registro de auditoría entre el módulo de votación 101 y el módulo de auditoría 103 para evitar un único punto de fallo que invalide dicho registro de voto 104.

El método propuesto también comprende unas etapas adicionales que permiten mantener sincronizados los registros de voto y los votos electrónicos almacenados en el terminal de votación, facilitando así una posterior auditoría.

Por su parte, el módulo de auditoría 103 utilizado para la implementación del método propuesto comprende, en su versión más básica, los siguientes elementos: unos medios de entrada y salida de datos para recibir y enviar una información digital relacionada con las opciones de voto seleccionadas por el votante 106 en el módulo de votación 101, y unos medios de procesamiento que permiten generar una información digital de auditoría 105 para garantizar la integridad, la autenticidad y el no-repudio de los votos emitidos y detectar posibles fallos (voluntarios o no) en el protocolo que ejecute el módulo de votación 101.

Dicho módulo de auditoría 103 comprende, además, en una variante de ejecución preferida, unos medios de almacenamiento que le permiten almacenar información para la auditoría.

Otras características de la invención, y en concreto, características particulares de las etapas del método y elementos constitutivos del módulo de auditoría 103, serán descritos con mayor detalle a continuación, ilustrados además con unas láminas de dibujos.

Breve descripción de los dibujos

La figura 1 muestra de manera simplificada los principales elementos sobre los que se implementa el método para facilitar la auditoría de procesos

electorales, descrito en la presente invención: un módulo de votación 101 a través del cual el votante 106 realiza una selección 201 de unas opciones de voto; un módulo de verificación 102 que genera un registro de voto 104 que contiene las opciones de voto seleccionadas en el módulo de votación 101 para que sean verificadas por el votante 106; y un módulo de auditoría 103 que recibe las opciones de voto enviadas 202 por el módulo de votación 101, envía dichas opciones de voto al módulo de verificación 102 para que genere el registro de voto 104 y genera, después de una confirmación 204 por acción u omisión del votante 106, una información de auditoría 105 a partir de al menos las opciones de voto seleccionadas por el votante 106 en el módulo de votación 101 para garantizar la validez de al menos el registro de voto 104.

La figura 2 ilustra de forma esquemática las etapas básicas de que se compone el método propuesto en la presente invención. Tras realizar una etapa de selección 201 de unas opciones de voto en el módulo de votación 101, este módulo de votación 101 realiza una etapa de envío 202 de las opciones de voto a un módulo de auditoría 103. El módulo de auditoría 103 envía las opciones de voto al módulo de verificación 102 para realizar una etapa de generación 203 de un registro de voto 104 verificable por el votante 106. Tras una etapa de confirmación 204, por acción u omisión de el votante 106, se realiza una etapa de generación 205 de una información de auditoría 105 implementada por el módulo de auditoría 103 a partir de al menos las opciones de voto.

Las figuras 3a, 3b, 3c, 3d y 3e describen diferentes aproximaciones para la generación 205 de una información de auditoría 105 utilizando técnicas de codificación. Para facilitar una descripción más detallada de los procesos y protocolos criptográficos listados se utilizará la siguiente notación:

- *B*: Información que contiene las opciones de voto seleccionadas por el votante 106 en el módulo de votación 101. También puede contener otra información adicional como un identificador único de voto.
- $COD_{MA}(B)$: Codificación de una información *B* mediante una clave *MA* asociada al módulo de auditoría 103.
- $COD_{MVT}(B)$: Codificación de una información *B* mediante una clave *MVT* asociada al módulo de votación 101.

- $COD_{MA}(COD_{MVT}(B))$: Generación de una codificación mediante una clave *MA* asociada al módulo de auditoría 103, y una codificación de una información *B* mediante una clave *MVT* asociada al módulo de votación 101.
- $COD_{MA}(B, COD_{MVT}(B))$: Generación de una codificación mediante una clave *MA* asociada al módulo de auditoría 103, una información *B*, y una anterior codificación de la información *B* mediante una clave *MVT* asociada al módulo de votación 101.

La figura 3a muestra una aproximación en la que la información de auditoría 105 se genera 205 únicamente mediante el módulo de auditoría 103, mientras que en la figuras 3b, 3c, 3d y 3e esta generación 205 se realiza de forma colaborativa mediante el módulo de auditoría 103 y el módulo de votación 101. Las figuras empiezan con unas etapas comunes de envío 202 de una información *B*, que contiene las opciones de voto seleccionadas por el votante 106, al módulo de auditoría 103 y al módulo de verificación 102. A continuación, después de una etapa de confirmación, cada figura muestra una distinta aproximación de generación 205 de una información de auditoría 105. Finalmente esta información de auditoría 105 se envía al módulo de verificación 102 para que la pueda añadir al registro de voto y, en el caso de que no dispusiera previamente de ella, al módulo de votación para que pueda añadirla a un voto electrónico.

La figura 3a muestra una aproximación en la que la información de auditoría 105 se genera en el módulo de auditoría 103 mediante una codificación de la información *B* con una clave *MA* asignada a dicho módulo de auditoría 103. Las figuras 3b y 3d muestran dos aproximaciones en la que la información de auditoría 105 se genera mediante una segunda codificación de una información previamente codificada de la información *B*. En la figura 3b la primera codificación se realiza en el módulo de votación 101 y la segunda codificación se realiza en el módulo de auditoría 103. En la figura 3d el orden de codificación es inverso, de este modo la primera codificación se realiza en el módulo de auditoría 103 mientras que la segunda se realiza en el módulo de votación 101. Finalmente las figuras 3c y 3e muestran dos aproximaciones similares a las dos

últimas expuestas pero en las que la información de auditoría 105 se genera mediante una segunda codificación a partir de una información *B* y una primera codificación de dicha información *B*. En la aproximación 3c la primera codificación se realiza en el módulo de votación 101 y la segunda en el módulo de auditoría 103, mientras que en la figura 3e la primera codificación se realiza en el módulo de auditoría 103 y la segunda en el módulo de votación.

Por último las figuras 4a y 4b muestran dos posibles implementaciones del método descrito en las que se duplican algunos de sus módulos. La figura 4a muestra una implementación en las que se utilizan dos módulos de auditoría para facilitar una verificación doble, mediante medios visuales y mediante medios audibles. En la implementación 4b se utiliza más de un módulo de auditoría 103 conectados entre sí para generar una información de auditoría 105 de forma colaborativa entre ellos.

Descripción detallada de la invención

La presente invención se refiere a un método y un sistema aplicable a un entorno de votación electrónica para facilitar la auditoría y protección de procesos electorales que utilizan un módulo de votación 101 electrónica, tal como un DRE (del inglés, Direct Recording Electronic) para la selección 201 de los votos y un módulo de verificación 102, tal como una impresora, para la generación 203 de un registro de voto 104 verificable por un votante 106. El ámbito de la invención no cubre tareas como la construcción del censo, el registro de los votantes 106, el recuento de los votos emitidos durante el proceso electoral ni la posible gestión de claves de los votantes 106.

En la presente invención entenderemos por voto, todo aquel registro, ya sea digital o no, vinculado a un votante 106 con derecho a participar en un proceso electoral. En general, un voto consistirá de diferentes preguntas y el votante 106 deberá seleccionar su opción de voto para cada una de las preguntas que se realicen. En la explicación que sigue a partir de este punto asumiremos, sin pérdida de generalidad, que en cada voto se formula una única pregunta. En caso que no sea así, el método puede aplicarse tanto de forma individual como de forma conjunta en el global de las preguntas de las que se

componga el voto. Cabe notar que cuando se menciona en la presente memoria que una información digital o un registro de voto 104 contiene las opciones de voto seleccionadas por el votante 106, se entiende que dicha información o registro contiene una representación en cualquiera de los diferentes posibles formatos que puedan tener dichas opciones de voto.

Para poner en práctica esta invención se propone la utilización de un módulo de auditoría 103, que se encuentra asociado al módulo de votación 101 y al módulo de verificación 102 correspondientes. Aunque los tres módulos son susceptibles de ser agrupados de forma individual o conjunta, en una implementación preferente el módulo de auditoría 103 se encontrará intercalado entre el módulo de votación 101 y el módulo de verificación 102. De entre las principales aportaciones de este módulo de auditoría 103 destacan la generación 205 de una información digital de auditoría 105 que aporta seguridad al proceso de generación 203 del registro de voto 104, así como la simplificación del proceso de auditoría de las votaciones.

El módulo de auditoría 103 recibe del módulo de votación 101 una información que contiene las opciones de voto seleccionadas por el votante 106, y estas opciones de voto recibidas son enviadas por este módulo de auditoría 103 al módulo de verificación 102. A partir de las opciones de voto, el módulo de verificación 102 genera un registro de voto 104 verificable por el votante 106 que debe contener de forma explícita las opciones de voto recibidas. El votante 106, por acción u omisión, deberá confirmar si el registro de voto 104 contempla su intención de voto. Una vez recibida la confirmación, el módulo de auditoría 103 generará una información de auditoría 105 que garantizará algunas propiedades como la integridad, la autenticidad y el no repudio del registro de voto 104 generado por el módulo de verificación 102.

El módulo de auditoría 103, según la presente invención, comprende en una implementación básica los elementos descritos a continuación. Una unidad de entrada y salida que permite la recepción y el envío 202 de una información en formato digital relacionada con las opciones de voto seleccionas por el votante 106 en el módulo de votación 101 asociado. Y unos medios de procesamiento que permiten generar cierta información digital de auditoría 105

que facilite la auditoría del proceso electoral y permita generar registros de voto seguros.

En una implementación preferida, dicho módulo de auditoría 103 también incorpora unos medios de confirmación para permitir al votante 106 confirmar si las opciones de voto registradas en el registro de voto 104 son o no las deseadas.

Se ha previsto también proporcionar unos medios de almacenamiento a dicho módulo de auditoría 103, de manera que disponga de capacidad para almacenar información digital relacionada con las opciones de voto o en el caso de que sea necesario, las claves criptográficas necesarias para ejecutar los protocolos criptográficos que describiremos más adelante. Debido a que los datos almacenados en dicha unidad de almacenamiento pueden ser necesarios durante la elección, esta unidad de almacenamiento debe ser persistente, evitando así la posibilidad de una pérdida de datos generado por ejemplo por un fallo de energía eléctrica. La presente invención también prevé que parte de los medios de procesamiento y de los medios de almacenamiento del módulo de auditoría 103, se encuentren en un dispositivo extraíble que aporte dichas funcionalidades, como sería una tarjeta inteligente criptográfica. De este modo se incrementarían las medidas de seguridad y el correcto funcionamiento de dicho módulo.

Para facilitar la integración con un módulo de votación 101, el módulo de auditoría 103 puede disponer de una fuente de alimentación de energía autónoma. De este modo puede obtener la energía para su funcionamiento de una célula de energía propia o conectándose directamente a la red eléctrica. También se ha previsto que la obtención de dicha energía provenga del módulo de votación 101 al que se encuentra asociado.

La invención supone que el módulo de votación 101 posee esencialmente una interfaz de presentación de las opciones de voto que el votante 106 puede seleccionar, y unos medios para realizar dicha selección con los que interactúa el votante 106 para realizar una etapa de selección 201 de una o más opciones de voto. En la invención se contempla la posibilidad de una implementación en la que el módulo de votación 101 disponga de unos medios de almacenamiento para, tras dicha etapa, almacenar las opciones de voto seleccionadas siendo

éstas facilitadas posteriormente a un sitio de procesado local o remoto para su recuento. Se contempla también la posibilidad de que dichos medios de almacenamiento guarden la información necesaria (tal como por ejemplo claves) para llevar a cabo la implementación de los protocolos criptográficos que detallaremos más adelante. Al igual que hemos descrito en el caso del módulo de auditoría 103, también se contempla la posibilidad de que parte de los medios de procesamiento y de los medios de almacenamiento de que disponga el módulo de votación 101 se encuentren agrupados en un dispositivo extraíble que aporte dichas funcionalidades, como sería una tarjeta inteligente criptográfica.

En referencia al módulo de verificación 102 la invención supone que está formado esencialmente por unos medios de entrada y salida de datos, con los que el módulo de verificación 102 puede conectarse al módulo de auditoría 103. Para facilitar la accesibilidad de los votantes 106 con discapacidades, la presente invención contempla diferentes módulos de verificación que permitirán generar diferentes registros de voto. Con este fin se contempla la posibilidad de que dicho registro de voto 104 pueda ser, por citar un ejemplo, visual o auditivo. Finalmente también se contempla la posibilidad de que exista más de un módulo de verificación 102 conectado a un módulo de auditoría 103 para permitir a los votantes 106 utilizar distintas formas de verificación de las mismas opciones de voto.

Como hemos mencionado anteriormente, en la presente invención presentamos un método fácil de auditar en el que, un módulo de votación 101, un módulo de verificación 102 y un módulo de auditoría 103, proporcionan un registro de voto 104 verificable. El citado método se caracteriza esencialmente porque tras una etapa de selección 201 de las opciones de voto en el módulo de votación 101, comprende los tres módulos que acabamos de mencionar, las siguientes etapas básicas:

- recibir en el módulo de auditoría 103 una información digital enviada 202 por el módulo de votación 101 que contiene las opciones de voto previamente seleccionadas por el votante 106 en dicho módulo de votación 10 1;

- enviar desde el módulo de auditoría 103 al módulo de verificación 102 al menos las opciones de voto recibidas del módulo de votación 1 01 para que el

módulo de verificación 102 un registro de voto 104. Para facilitar que el votante 106 pueda verificar el registro de voto 104, dicho registro de voto 104 contiene de forma explícita al menos las opciones de voto seleccionadas por dicho votante 106 en el módulo de votación 101.

- confirmar, mediante acción u omisión, si el votante 106 está de acuerdo con las opciones de voto mostradas en el registro de voto 104.

- generar mediante el módulo de auditoría 103 una información digital de auditoría 105 relacionada con las opciones de voto seleccionadas por el votante 106 en el módulo de votación 101. Esta información digital permitirá, en una auditoría del proceso electoral, verificar la validez de los votos emitidos.

Este método contempla una etapa adicional en la que, una vez confirmado el registro de voto 104, el módulo de votación 101 almacena internamente un voto en formato electrónico con las opciones de voto que el votante 106 ha confirmado. Este voto electrónico puede también contener el resultado de la confirmación 204 del votante que indique si se trata de un voto válido (apto para el recuento) o inválido (no apto para el recuento). Un voto inválido es aquel que no recoge la intención de voto del votante 106, por lo que no puede ser contabilizado. Un voto inválido puede ser debido a un cambio de opinión del votante 106 o un error al realizar la selección 201 de las opciones, que es descubierto al verificar el registro de voto 104. En ese caso, el votante 106 tiene la opción de volver a la etapa de selección 201 de las opciones de voto para modificarlas. Como ya ha sido generado el registro de voto 104 que no contiene intención de voto del votante 106, es importante que el voto electrónico relacionado con dicho registro refleje que no es de un voto válido para evitar que sea contabilizado. Igualmente, en el caso de que el voto electrónico no sea válido, se contempla también la posibilidad de que dicho voto electrónico no sea finalmente almacenado.

El método contempla que el registro de voto 104 verificable por el votante 106 pueda estar en diferentes formatos para facilitar la verificación a votantes 106 con discapacidades. Por ejemplo, si se trata de proporcionar al votante 106 una verificación visual, se prevé su implementación mediante una impresora o si se trata de proporcionar al votante 106 una verificación auditiva, se contempla su implementación mediante un dispositivo de audio, tal como unos auriculares.

También contempla la posibilidad que esta verificación se pueda hacer de forma simultánea, por ejemplo visual y audiblemente, por ejemplo sobre dos módulos de verificación distintos conectados al mismo módulo de auditoría 103.

Para mejorar la seguridad y auditoría del método, también se prevé la posibilidad de que los medios de confirmación se encuentren en el módulo de auditoría 103. En este caso el módulo de auditoría 103 genera una información digital de confirmación, que contiene principalmente la confirmación 204 del votante 106, para comunicar dicha confirmación 204 al módulo de votación 101 y/o al módulo de verificación 102. El método de la presente invención contempla en especial la posibilidad de que la confirmación del votante 106 sea negativa. Esto es que el votante 106 considere las opciones del registro de voto 104 no coinciden con las opciones de voto que previamente ha seleccionado o que realmente quería seleccionar en el módulo de votación 101. En este caso dicha información digital de confirmación puede contener adicionalmente información digital codificada generada a partir de las opciones de voto seleccionadas por el votante 106 en el módulo de votación 101 y/o la confirmación del votante 106. Como medida de auditoría, la información de confirmación también puede ser enviada al módulo de verificación 102 para que la añada al registro de voto 104, dejando así constancia de si el registro de voto 104 ha sido aceptado o no por el votante 106. También se contempla la opción que la información de confirmación pueda ser utilizada por el módulo de auditoría 103 para generar la información de auditoría 105.

Para la etapa de confirmación, el método descrito en la presente invención prevé utilizar unos medios de confirmación que permitan al votante 106 efectuar, en caso de que lo consideren oportuno, dicha confirmación . En la etapa de confirmación 204 puede existir una opción por defecto que se ejecute automáticamente en caso de que se cumplan unas ciertas condiciones. Por ejemplo, la confirmación 204 automática de las opciones de voto al cabo de un tiempo establecido de inactividad tras la generación 203 del registro de voto 104. De este modo se protege la privacidad del votante 106 o se impide que un votante 106 pueda votar más de una vez si el votante 106 anterior se olvidó de confirmar el voto. La implementación más sencilla constaría de únicamente un botón de confirmación, pudiendo ser ampliada a más botones en caso de que se

considere oportuno. Para facilitar la accesibilidad de votantes 106 con discapacidades visuales, una realización alternativa contempla la confirmación respondiendo a un mínimo de dos órdenes audibles, que se ejecutan desde un micrófono accesible al votante 106.

Con el fin de mejorar la auditoría de la elección y proteger el registro de voto 104 generado por el módulo de votación 101, la presente invención contempla diferentes aproximaciones para generar una información de auditoría 105 que permita aumentar el nivel de seguridad del registro de voto 104 resultante y evitar inserciones posteriores de votos falsos o manipulaciones por parte de alguno de los dispositivos que conforman el sistema.

En una primera aproximación, el método contempla una solución en la que el módulo de auditoría 103 genera la información de auditoría 105 sin realizar ninguna codificación o, en caso de realizar alguna codificación, sin utilizar componentes secretos (o privados), tales como claves criptográficas. En ambos casos esta información de auditoría 105 se genera a partir de la información digital que contiene al menos las opciones de voto seleccionadas. Teniendo en cuenta que esta etapa depende de la confirmación 204 del registro de voto 104, también se podría utilizar adicionalmente para esta generación la información de confirmación de dicho registro de voto 104. Para la codificación de la información, se pueden utilizar algoritmos criptográficos como funciones resumen o hash, tales como las funciones SHA1 o SHA256. También se contempla usar una función criptográfica, tal como una función resumen de acumulación (OWA), que permita encadenar de forma conmutativa diferentes informaciones de auditoría generadas. Esta última propuesta, al generar una información de auditoría 105 resultante a partir de la información de auditoría 105 de cada uno de los votos emitidos, independientemente del orden de los votos que se ya seguido, permite realizar una auditoría posterior sin comprometer la privacidad de los votantes 106.

En una segunda aproximación, y conforme a un ejemplo de realización preferido del método propuesto en la presente invención, el módulo de auditoría 103 genera la información de auditoría 105 mediante una codificación en la que utiliza al menos una clave secreta. Como en la aproximación anterior, esta codificación se puede realizar a partir de las opciones de voto seleccionadas,

pudiendo también utilizar la información de confirmación. En una implementación preferida, dicha codificación es una firma digital de al menos las opciones de voto utilizando la clave privada del módulo de auditoría 103. Esta medida permite mejorar la implementación de las medidas de la primera aproximación, ya que protege la integridad, la autenticidad y el no repudio de la información de auditoría 105. Por ejemplo, es posible verificar que la firma digital ha sido efectivamente realizada por el módulo de auditoría 103, utilizando la clave pública del módulo de auditoría 103. También pueden utilizarse una clave simétrica junto con una función resumen con clave (HMAC). En una implementación menos robusta, el método también puede implementarse con una clave simétrica y un algoritmo de cifrado simétrico, tal como el AES.

Para esta segunda aproximación, el método contempla una etapa adicional en la que se envía la información de auditoría 105 al módulo de verificación 102, para que la añada al registro de voto 104 generado anteriormente. Así se dota al registro de voto 104 de las mismas características que se han proporcionado al módulo de auditoría 103, como por ejemplo, integridad, autenticidad y no repudio. Finalmente, otra etapa adicional contemplada consiste en el envío al módulo de votación 101 de la información de auditoría 105 generada por el módulo de auditoría 103. Esta información, permite al módulo de votación 101 verificar que el registro de voto 104 generado es correcto (p.e. verificando que la firma sea coherente con las opciones de voto seleccionadas en dicho módulo). También, si el módulo de votación 101 almacena electrónicamente los votos confirmados, puede añadir la información de auditoría 105 para proporcionar seguridad al voto electrónico almacenado. Esta última medida permite verificar la integridad de los votos, garantizando que no se introducen votos que no hayan sido emitidos correctamente desde el módulo de votación 101 correspondiente.

En una tercera aproximación, también conforme a un ejemplo de realización preferido del método propuesto, el módulo de auditoría 103 genera la información de auditoría 105 mediante una codificación, en la que también interviene el módulo de votación 101. En este caso para la generación conjunta de la información codificada cada módulo dispondrá de al menos una clave secreta propia. Como en la aproximación anterior, esta codificación inicialmente

se puede realizar a partir de al menos las opciones de voto seleccionadas, pudiendo también utilizar la información de confirmación. En esta aproximación, el método contempla dos posibles alternativas para la generación conjunta de la codificación de la información.

En una primera alternativa se introduce una etapa adicional en la que el módulo de auditoría 103 empieza codificando con su clave privada al menos las opciones de voto y envía esta primera información codificada al módulo de votación 101. El módulo de votación 101, verifica que esta primera información codificada recibida es correcta (p.e. verificando la integridad, autenticidad y no repudio de la información codificada) y genera una segunda información codificada a partir de al menos dicha primera información codificada. Una vez el módulo de votación 101 ha generado la segunda información codificada, se contempla una nueva etapa en la que dicha segunda información codificada se envía al módulo de auditoría 103. A continuación, el módulo de auditoría 103 verifica que esta segunda información codificada recibida es correcta. Esta alternativa se recomienda utilizarla cuando la confirmación 204 del registro de voto 104 es negativa, utilizando también como información para generar las codificaciones la información de confirmación.

En una segunda alternativa se introduce una etapa adicional, a continuación de la etapa de confirmación 204, en la que el módulo de votación 101 empieza codificando con su clave privada al menos las opciones de voto y envía esta primera información codificada al módulo de auditoría 103. El módulo de auditoría 103, verifica que esta primera información codificada recibida es correcta y en caso afirmativo genera una segunda información codificada a partir de al menos dicha primera información codificada. Una vez el módulo de auditoría 103 ha generado la segunda información codificada, se contempla una nueva etapa en la que dicha segunda información codificada se envía al módulo de votación 101. A continuación al módulo de votación 101 verifica que esta segunda información codificada recibida es correcta. Esta alternativa se recomienda utilizarla cuando la confirmación 204 del registro de voto 104 es positiva.

En ambas alternativas y en caso de que la verificación de la información codificada sea correcta, el método contempla que el módulo de auditoría 103

utilice la segunda codificación para la generación 205 de la información de auditoría 105. Adicionalmente, si el módulo de votación 101 almacena electrónicamente los votos confirmados, puede añadir esta segunda información codificada al voto electrónico para proporcionar seguridad al voto electrónico. El método también contempla una etapa adicional de envío de la segunda codificación al módulo de verificación 102 para añadirla al registro de voto 104.

En una implementación preferente, se contempla que cada módulo disponga de una clave asimétrica privada propia y distinta. De este modo la codificación realizada en ambos módulos será una firma digital y la verificación de la firma se realizará utilizando la clave pública correspondiente. Por lo tanto la integridad, autenticidad y no repudio de la información de auditoría 105, voto electrónico y/o registro de voto 104, se protegerá mediante una doble firma digital. Esta doble firma digital puede comprender dos firmas independientes de las mismas opciones de voto (y posiblemente la información de confirmación relacionada) concatenadas, o una firma anidada de una firma de las opciones de voto.

En una segunda implementación preferente, el módulo de votación 101 y el módulo de auditoría 103 tienen fragmentos de una clave privada de la elección (o bien asociada a cada par formado por un módulo de votación 101 y un módulo de auditoría 103). Así cada uno de los módulos, en la etapa correspondiente, genera una firma parcial. A partir de estas firmas parciales, y utilizando un protocolo de firma distribuida, es posible generar una firma de la elección equivalente a la que se habría obtenido directamente de la clave privada de la elección. Así, por ejemplo, propiedades como la integridad, la autenticidad y el no repudio de la información de auditoría 105, voto electrónico y/o registro de voto 104, se garantizan mediante una verificación utilizando la clave pública de la elección asociada a la clave privada.

Tal como se ha descrito anteriormente en las distintas aproximaciones y alternativas de generación 205 de la información de auditoría 105 descrita, el método propuesto en la presente invención permite a los módulos de votación y auditoría verificar que los registros de voto se están generando correctamente. Esta cualidad permite detectar errores que sin la existencia del módulo de auditoría 103 pasaban desapercibidos. Un ejemplo es la invalidación de votos

que habían sido confirmados como válidos por los votantes 106, por culpa de un error al generar la firma digital del voto.

La adición de más módulos de auditoría intercalados entre sí y el módulo de votación 101 podría ser posible en el método propuesto. Esta solución implicaría que las codificaciones se harían de forma secuencial entre un módulo y el siguiente, permitiendo que cada módulo verifique la codificación de los anteriores. También sería posible realizar estas codificaciones de forma paralela, utilizando alguno de los protocolos de firma distribuida entre el conjunto de módulos de auditoría y el módulo de votación 101.

El método contempla que en todos los casos en los que se envía una información codificada para dotar de las correspondientes condiciones de seguridad al registro de voto 104, esta información se adapta al formato de este registro de voto 104. Así, en el caso de que dicho registro de voto 104 sea visual (p.e. impreso) la información codificada podrá ser enviada en un formato gráfico (p.e. código de barras). De este modo, en el caso de los registros de voto se procesen de forma automática, esta información codificada podrá ser interpretada por el mismo método de captación de datos (p.e. escaneo óptico). El método también contempla que en el caso de que exista más de un módulo de verificación 102 conectado a un mismo módulo de auditoría 103, se pueda enviar únicamente la información codificada a uno de los módulos.

La presente invención también contempla la posibilidad de incorporar un identificador único de voto en el registro de voto 104. Este identificador de voto único puede ser proporcionado por el módulo de auditoría 103 o puede ser proporcionado por el módulo de votación 101. Para incrementar la seguridad del método en una implementación preferente se contempla una etapa adicional de generación del identificador único de forma colaborativa entre el módulo de votación 101 y el módulo de auditoría 103. El método también contempla de forma preferencial el uso de identificadores únicos de voto para la generación 205 de la información de auditoría 105. En el caso de que la implementación contemple la posibilidad de guardar votos electrónicos en el módulo de votación 101 (tal y como hemos descrito anteriormente), la utilización de un identificador único de voto en el voto electrónico y el registro de voto 104 permite mejorar sustancialmente la detección de pérdida o eliminación de votos mediante la

auditoría de la elección. De este modo, en el caso de inconsistencias en recuentos de los registros de voto y los votos electrónicos, el identificador único de voto puede permitir encontrar la causa de la consistencia.

REIVINDICACIONES

1. Método auditable para la generación (203) de un registro verificable, tal como un registro de voto (104) verificable por un votante (106), en el que se utilizan un módulo de votación (101), un módulo de verificación (102) destinado a la generación (203) de un registro de voto (104) y un módulo de auditoría (103), susceptibles de diversos grados de dispersión y/o agrupación, y unos protocolos criptográficos que permiten la generación (203) de dicho registro de voto (104), para que se garanticen una serie de requisitos de seguridad preestablecidos para un proceso electoral, comprendiendo dicho método para cada voto, una vez seleccionada/s (201) por el votante (106) una/s opción/es de voto en dicho módulo de votación (101) las siguientes etapas:
   a) El envío (202) desde dicho módulo de votación (101) a dicho módulo de auditoría (103), de una información digital que contiene al menos dicha/s opción/es de voto seleccionada/s;
   b) El envío desde dicho módulo de auditoría (103) a dicho módulo de verificación (102) de al menos dicha/s opción/es de voto contenidas en dicha información digital recibida en la etapa a) por dicho módulo de auditoría (103), para la generación (203) por dicho módulo de verificación (102) de dicho registro de voto (104), que es verificable por el votante (106) y que contiene al menos dicha/s opción/es de voto;
   c) La confirmación (204), por acción u omisión, de la coincidencia o no de la intención de voto del votante (106) con dicha/s opción/es de voto contenidas en dicho registro de voto (104) verificable; y
   d) La generación (205) de al menos una información digital de auditoría (105) por al menos dicho módulo de auditoría (103) para garantizar la validez de los votos emitidos en una auditoría posterior.

2. Método según la reivindicación 1 caracterizado por proporcionar una verificación de dicho registro de voto (104) por medios visuales mediante dicho módulo de verificación (102).
3. Método según la reivindicación 1 ó 2 caracterizado por proporcionar una verificación de dicho registro de voto (104) por medios audibles mediante dicho módulo de verificación (102).
4. Método según la reivindicación 1 caracterizado por proporcionar una verificación de dicho registro de voto (104) por medios visuales y/o audibles mediante dicho módulo de verificación (102) y un segundo módulo de verificación (102) adicional.
5. Método según la reivindicación 1 caracterizado porque dicha confirmación (204) especificada en la etapa c) es realizada por el votante (106).
6. Método según la reivindicación 1 ó 5 caracterizado por realizar dicha confirmación (204) en dicho módulo de auditoría (103).
7. Método según la reivindicación 1 caracterizado porque se genera además mediante dicho módulo de auditoría (103) una información digital de confirmación que contiene al menos el resultado de dicha confirmación (204), y dicha información digital de confirmación es transmitida de dicho módulo de auditoría (103) a dicho módulo de votación (101).
8. Método, según la reivindicación 1 caracterizado porque, en caso de que dicha confirmación (204) indique la no coincidencia de la intención del votante (106) con dicha/s opción/es de voto contenidas en dicho registro de voto (104) verificable, dicho módulo de auditoría (103) envía a dicho módulo de verificación (102) una información digital que contiene al menos una indicación de dicha no coincidencia.
9. Método, según la reivindicación 1 caracterizado porque, en caso de que dicha confirmación (204) indique la no coincidencia de la intención del votante (106) con dicha/s opción/es de voto contenidas en dicho registro de voto (104) verificable, el módulo de verificación (102) añade en dicho registro de voto (104) verificable generado en la etapa b) un registro que indica dicha no coincidencia.

10. Método según la reivindicación 1 caracterizado porque el módulo de votación (101) asocia adicionalmente a cada voto un identificador de voto único.

11. Método según la reivindicación 1 caracterizado porque el módulo de auditoría (103) asocia adicionalmente a la información digital que contiene las opciones de voto recibida en la etapa a) un identificador de voto único.

12. Método según la reivindicación 1 caracterizado porque se asocia adicionalmente a cada voto un identificador de voto único generado colaborativamente entre el módulo de votación (101) y el módulo de auditoría (103).

13. Método según la reivindicación 1 caracterizado porque el módulo de auditoría (103) genera dicha información digital de auditoría (105) especificada en la etapa d) a partir de al menos dicha/s opción/es de voto.

14. Método según la reivindicación 13 caracterizado porque para generar dicha información digital de auditoría (105) se realiza al menos una codificación para la cual se provee a dicho módulo de auditoría (103) de al menos una clave.

15. Método según la reivindicación 14 caracterizado porque dicha clave corresponde al menos a la componente privada de un par de claves criptográficas asimétricas.

16. Método según la reivindicación 14 caracterizado por una etapa adicional de envío a dicho módulo de votación (101) de al menos parte de dicha codificación realizada por dicho módulo de auditoría (103).

17. Método según la reivindicación 16 caracterizado porque dicho módulo de votación (101) almacena electrónicamente una copia de al menos parte de dicha información digital de la etapa a) y/o parte de dicha codificación recibida de dicho módulo de auditoría (103).

18. Método según la reivindicación 14 caracterizado porque dicho módulo de auditoría (103) almacena electrónicamente una copia de al menos parte de dicha información digital de la etapa a) y/o parte de dicha codificación realizada por dicho módulo de auditoría (103).

19. Método según la reivindicación 14 caracterizado por una etapa adicional de envío a dicho módulo de verificación (102) de al menos parte de dicha codificación realizada por dicho módulo de auditoría (103).

20. Método según la reivindicación 19 caracterizado porque dicho módulo de verificación (102) añade en dicho registro de voto (104) verificable generado en la etapa b) un registro que contiene al menos parte de dicha codificación recibida de dicho módulo de auditoría (103).

21. Método según la reivindicación 1 caracterizado porque dicho módulo de votación (101) realiza una codificación a partir de al menos dicha/s opción/es de voto.

22. Método según la reivindicación 21 caracterizado porque para realizar dicha codificación se provee a dicho módulo de votación (101) de al menos una clave.

23. Método según la reivindicación 22 caracterizado porque dicha clave corresponde al menos a la componente privada de un par de claves criptográficas asimétricas.

24. Método según la reivindicación 21 caracterizado por una etapa adicional de envío desde dicho módulo de votación (101) a dicho módulo de auditoría (103) de al menos parte de dicha codificación.

25. Método según la reivindicación 24 caracterizado por una etapa adicional de realización mediante dicho módulo de auditoría (103) de una segunda codificación a partir de al menos dicha/s opción/es de voto y/o al menos dicha codificación recibida de dicho módulo de votación (101).

26. Método según la reivindicación 25 caracterizado porque dicha información digital de auditoría (105) de la etapa d) se genera al menos a partir de dicha codificación recibida de dicho módulo de votación (101) y/o dicha segunda codificación.

27. Método según la reivindicación 25 caracterizado porque se provee a dicho módulo de votación (101) y dicho módulo de auditoría (103) de al menos unas respectivas claves para realizar dichas codificaciones correspondientes.

28. Método según la reivindicación 27 caracterizado porque dichas claves corresponden a unos fragmentos de una misma componente privada de un par de claves criptográficas asimétricas.

29. Método según la reivindicación 27 caracterizado porque dichas claves son al menos las componentes privadas de al menos dos pares distintos de claves criptográficas asimétricas, una para dicho módulo de votación (101) y otra para dicho módulo de auditoría (103).

30. Método según la reivindicación 25 caracterizado por una etapa adicional de envío a dicho módulo de votación (101) de al menos parte de dicha segunda codificación realizada por dicho módulo de auditoría (103).

31. Método según la reivindicación 30 caracterizado porque dicho módulo de votación (101) almacena electrónicamente una copia de al menos parte de dicha información digital de la etapa a) y/o parte de dicha segunda codificación recibida de dicho módulo de auditoría (103).

32. Método según la reivindicación 25 caracterizado porque dicho módulo de auditoría (103) almacena electrónicamente una copia de al menos parte de dicha información digital de la etapa a) y/o parte de dicha segunda codificación realizada por dicho módulo de auditoría (103).

33. Método según la reivindicación 17 ó 32 caracterizado porque dicha copia electrónica se almacena en una posición dentro de una zona de almacenamiento que no permita correlacionar el orden de la emisión de los votos con el orden de almacenamiento.

34. Método según la reivindicación 25 caracterizado por una etapa adicional de envío a dicho módulo de verificación (102) de al menos parte de dicha segunda codificación realizada por dicho módulo de auditoría (103).

35. Método según la reivindicación 34 caracterizado porque dicho módulo de verificación (102) añade en dicho registro de voto (104) verificable generado en la etapa b) un registro que comprende al menos parte de dicha segunda codificación recibida de dicho módulo de auditoría (103).

36. Sistema de votación electrónica auditable que genera un registro de voto (104) verificable por un votante (106) para implementar el método descrito en las reivindicaciones 1 a 35, del tipo que comprende:

a) un módulo de votación (101) configurado para mostrar unas opciones de voto y registrar una/s selección/es de dicha/s opción/es de voto, que comprende:

i. unos medios de procesamiento;

ii. unos medios de presentación de al menos una/s opción/es de voto;

iii. unos medios de introducción de datos que permitan al votante (106) seleccionar (201) una/s opción/es de voto; y

iv. unos medios de entrada y salida de datos para transmitir al menos una información digital que contiene al menos dicha/s opción/es de voto seleccionada/s; y

b) un módulo de verificación (102) que integra al menos unos medios de entrada y salida de datos para recibir al menos dicha/s opción/es de voto seleccionada/s y generar un registro de voto (104) de al menos dicha/s opción/es de voto recibida/s, siendo dicho registro verificable por el votante (106).

Caracterizado por comprender además un módulo de auditoría (103) intercalado entre dicho módulo de votación (101) y dicho módulo de verificación (102), y adaptado para recibir una información digital de al menos dicho módulo de votación (101), y generar una información digital de auditoría (105) que comprende:

i. unos medios de procesamiento; y

ii. unos medios de entrada y salida de datos para recibir al menos dicha información digital de dicho módulo de votación (101).

37. Sistema según la reivindicación 36 caracterizado porque dicho módulo de verificación (102) es una impresora.

38. Sistema según la reivindicación 36 caracterizado porque dicho módulo de verificación (102) es un dispositivo de audio, elegido del grupo que comprende al menos unos auriculares o unos altavoces.

39. Sistema según la reivindicación 36 caracterizado porque dicho módulo de auditoría (103) y dicho módulo de verificación (102), que es al menos uno, comparten dichos medios de entrada y salida de datos de dicho módulo de auditoría (103).

40. Sistema según la reivindicación 36 caracterizado porque dicho módulo de votación (101) comprende también unos medios de almacenamiento de al menos dicha/s opción/es de voto seleccionada/s.

41. Sistema según la reivindicación 36 caracterizado porque dicho módulo de auditoría (103) comprende también unos medios de almacenamiento de al menos una clave para la generación de una información codificada a partir de al menos parte de dicha información digital recibida por los medios de entrada y salida.

42. Sistema según la reivindicación 41 caracterizado porque parte de dichos medios de procesamiento de dicho módulo de auditoría (103) y parte de dichos medios de almacenamiento de dicho módulo de auditoría (103) se encuentran en un dispositivo extraíble tal como una tarjeta inteligente.

43. Sistema según la reivindicación 41 caracterizado porque dichos medios de almacenamiento están adaptados además para registrar al menos parte de dicha información digital codificada por dichos medios de procesamiento de dicho módulo de auditoría (103).

44. Sistema según la reivindicación 36 caracterizado porque dicho módulo de votación (101) comprende también unos medios de almacenamiento de al menos una clave para la generación de una información codificada a partir de al menos parte de una información introducida mediante dichos medios de introducción de datos y/o al menos parte de dicha información digital recibida por dichos medios de entrada y salida.

45. Sistema según la reivindicación 44 caracterizado porque parte de dichos medios de procesamiento de dicho módulo de votación (101) y parte de dichos medios de almacenamiento de dicho módulo de votación (101) se encuentran en un dispositivo extraíble tal como una tarjeta inteligente.

46. Sistema según la reivindicación 44 caracterizado porque dichos medios de almacenamiento están adaptados además para registrar al menos parte de dicha información digital codificada por dichos medios de procesamiento de dicho módulo de votación (101).

47. Sistema según la reivindicación 36 caracterizado porque dicho módulo de votación (101) está conectado únicamente a dicho módulo de auditoría (103).

48. Sistema según la reivindicación 36 caracterizado porque dicho módulo de auditoría (103) comprende unos medios de confirmación.

49. Sistema según la reivindicación 48 caracterizado porque dichos medios de confirmación son al menos un botón.

50. Sistema según la reivindicación 36 caracterizado porque dicho módulo de auditoría (103) y dicho módulo de votación (101) están conectados bidireccionalmente mediante dichos medios de entrada y salida de datos.

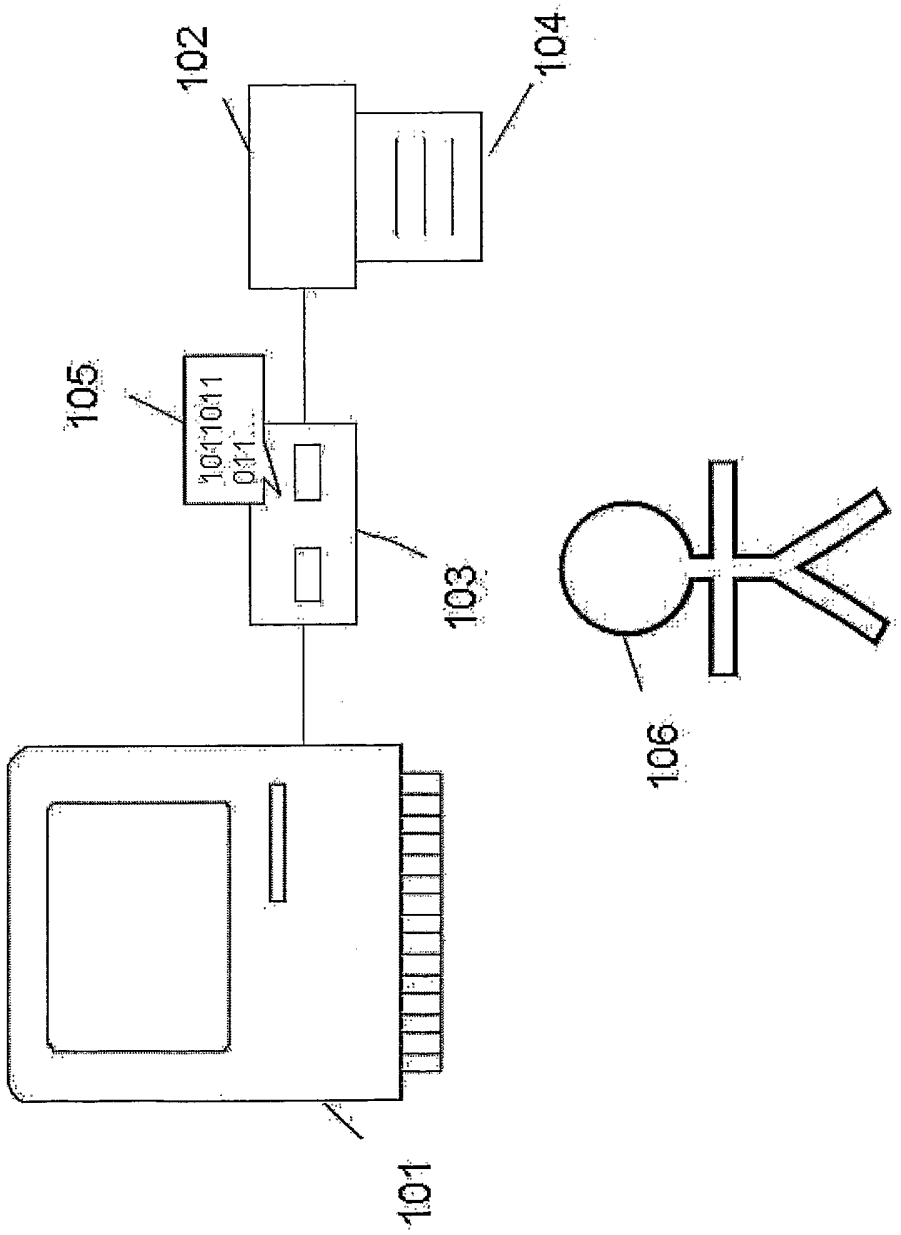


FIGURA 1

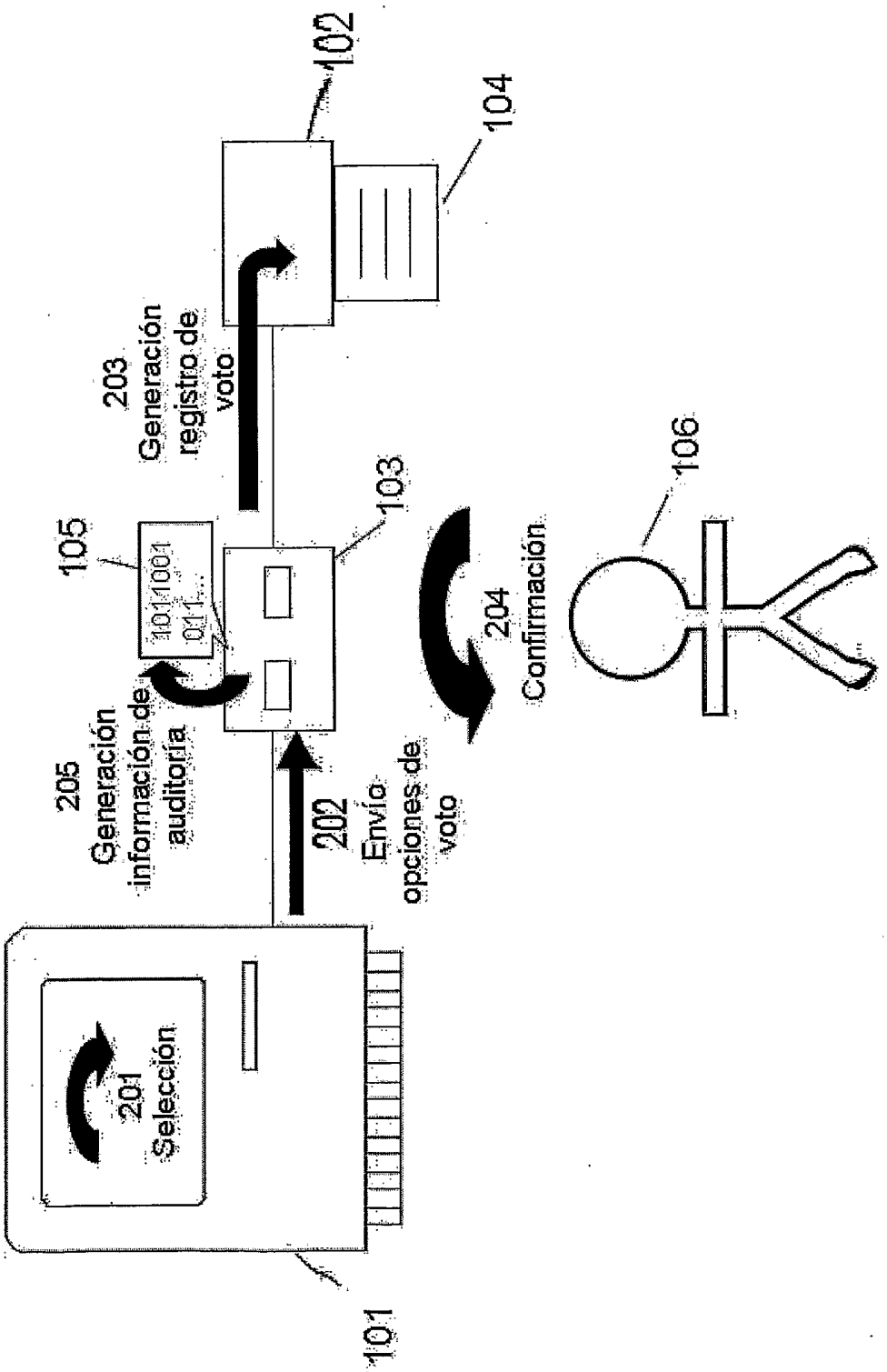

101
201
Selección
202
Envío
opciones de
voto
205
Generación
información de
auditoría
105
101101
011...
103
203
Generación
registro de
voto
102
104
204
Confirmación
106

FIGURA 2

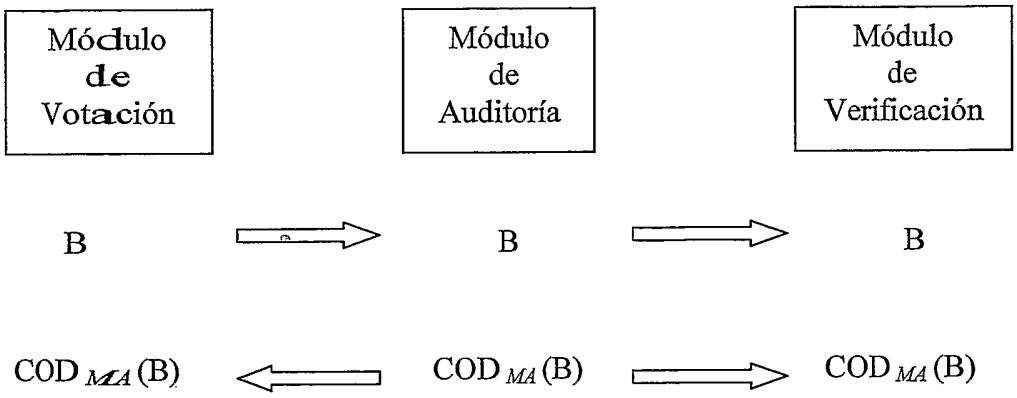

Módulo de Votación
Módulo de Auditoría
Módulo de Verificación
B
B
B
COD MA (B)
COD MA (B)
COD MA (B)

Figura 3a

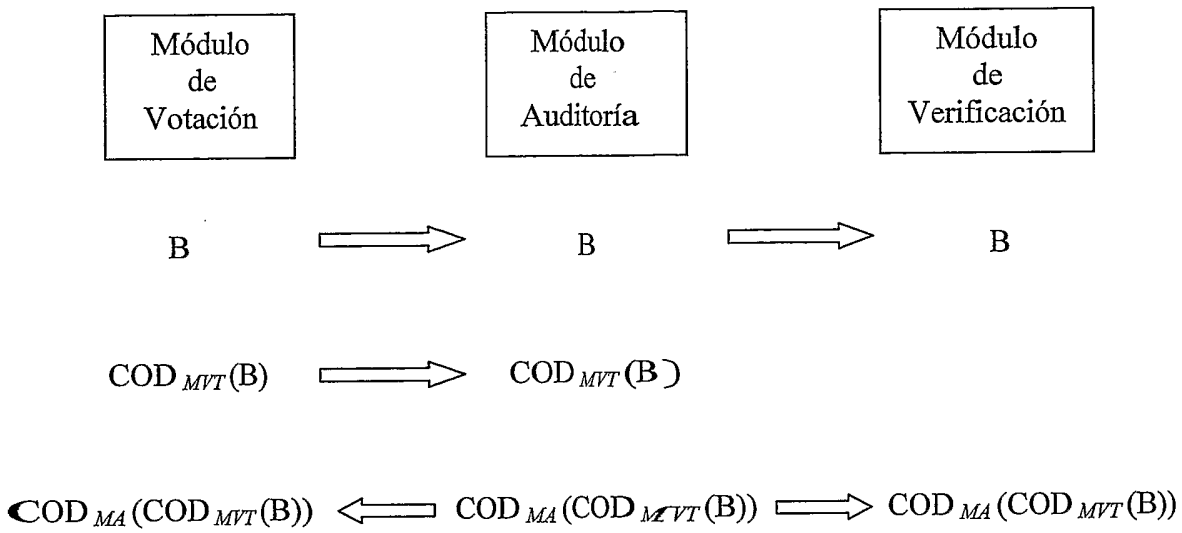

Módulo de Votación
Módulo de Auditoría
Módulo de Verificación
B
B
B
$COD_{MVT}(B)$
$COD_{MVT}(B)$
$COD_{MA}(COD_{MVT}(B))$
$COD_{MA}(COD_{MVT}(B))$
$COD_{MA}(COD_{MVT}(B))$

Figura 3b

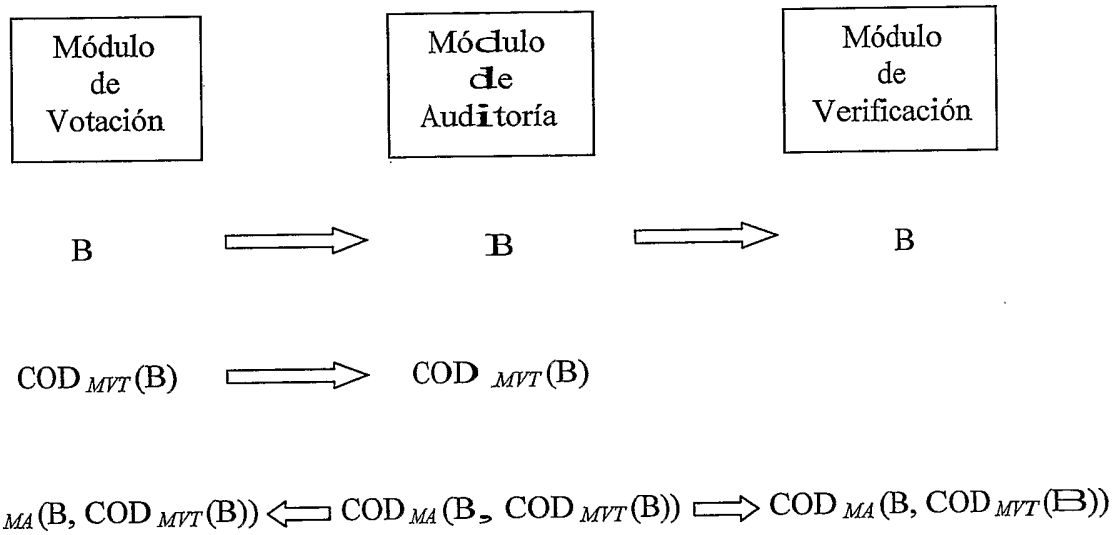

Módulo de Votación
Módulo de Auditoría
Módulo de Verificación
B
B
B
COD MVT (B)
COD MVT (B)
COD MA (B, COD MVT (B))
COD MA (B, COD MVT (B))
COD MA (B, COD MVT (B))

Figura 3c

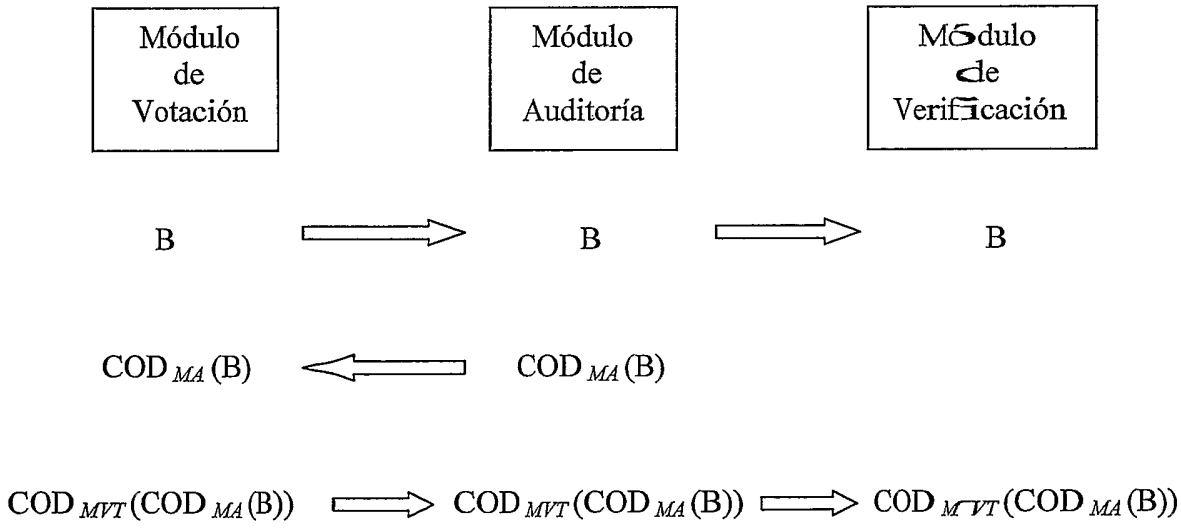

Módulo de Votación
Módulo de Auditoría
Módulo de Verificación
B
B
B
COD MA (B)
COD MA (B)
COD MVT (COD MA (B))
COD MVT (COD MA (B))
COD MVT (COD MA (B))

Figura 3d

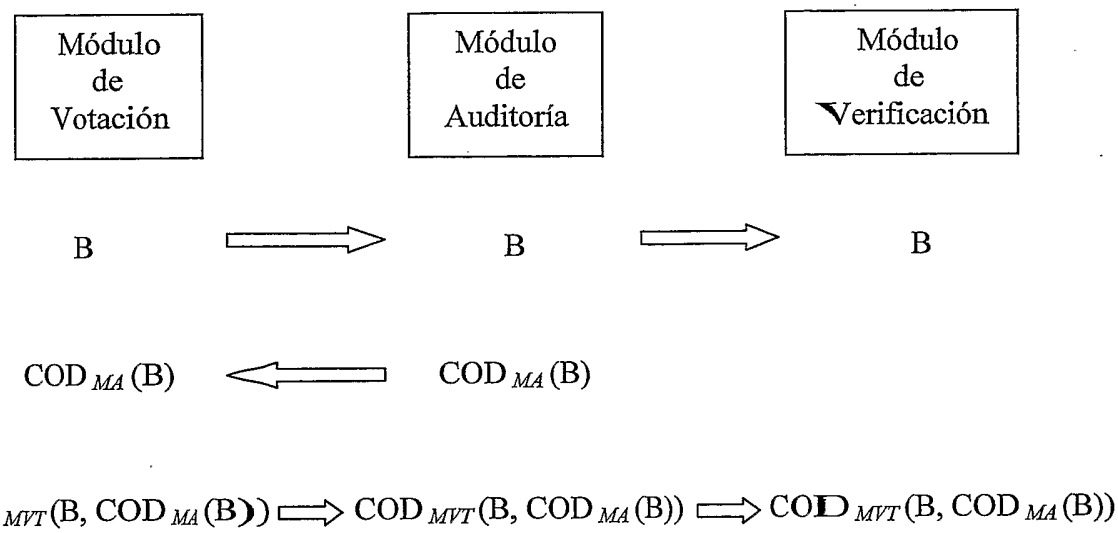

Módulo de Votación
Módulo de Auditoría
Módulo de Verificación
B
B
B
COD MA (B)
COD MA (B)
COD MVT (B, COD MA (B))
COD MVT (B, COD MA (B))
COD MVT (B, COD MA (B))

Figura 3e

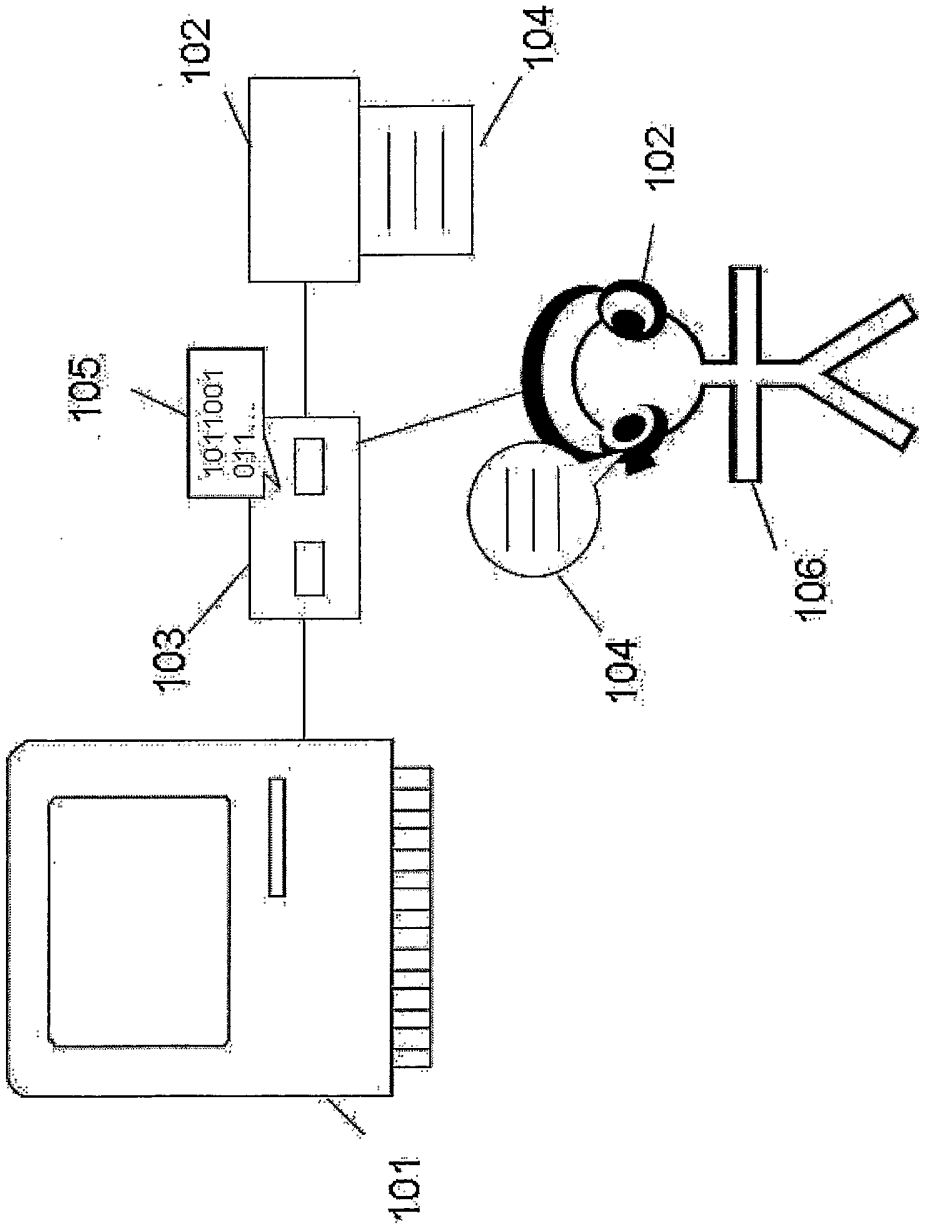


FIGURA 4a

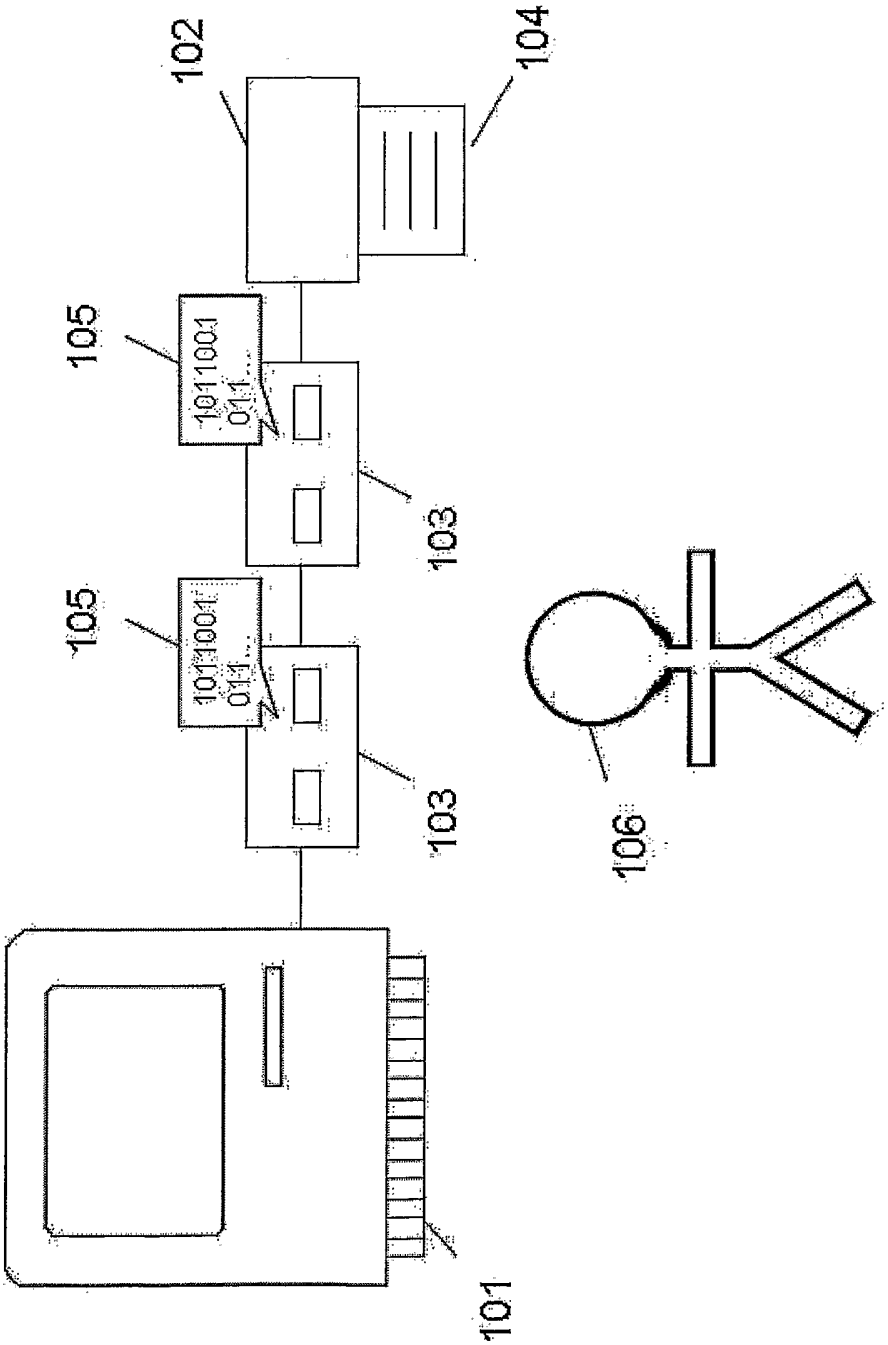


FIGURA 4b

INTERNATIONAL SEARCH REPORT

International application No.
PCT/ ES 2005/000215

A. CLASSIFICATION OF SUBJECT MATTER

G07C 13/00 (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G07C, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CIBEPAT,EPODOC,WPI, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO02056230 A2 (VOTE-HERE) 18.07.2002,the whole document	1 - 50
A	US2002161628 Al (LANE POOR5Jr. et al.) 31.10.2002, the whole document	1 - 50
A	US 2004195323 Al (VADURA et al.) 07.10.2004, the whole document	1 - 50

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 January 2006 (18.01.2006)	26 January 2006 (26.01.2006)
Name and mailing address of the ISA/ SPTO Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/ ES 2005/000215

WO 02056230 A	18.07.2002	US 2002078358 A	20.06.2002
US2002161628A A	31.10.2002	NONE	----------
US 2004195323 A	07.10.2004	US 2003006282 A US 2003178484 A	09.01.2003 25.09.2003

INFORME DE BÚSQUEDA INTERNACIONAL

Solicitud internacional nº

PCT/ ES 2005/000215

A. CLASIFICACIÓN DEL OBJETO DE LA SOLICITUD

G07C 13/00 (2006.01)

De acuerdo con la Clasificación Internacional de Patentes (CIP) o según la clasificación nacional y la CIP.

B. SECTORES COMPRENDIDOS POR LA BÚSQUEDA

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

G07C, G06F

Otra documentación consultada, además de la documentación mínima, en la medida en que tales documentos formen parte de los sectores comprendidos por la búsqueda

Bases de datos electrónicas consultadas durante la búsqueda internacional (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

CIBEPAT,EPODOC,WPI, INSPEC

C. DOCUMENTOS CONSIDERADOS RELEVANTES

Categoría*	Documentos citados, con indicación, si procede, de las partes relevantes	Relevante para las reivindicaciones nº
A	WO02056230 A2 (VOTE-HERE) 18.07.2002, todo el documento	1 - 50
A	US2002161628 A1 (LANE POOR,Jr. et al.) 31.10.2002, todo el documento	1 - 50
A	US 2004195323 A1 (VADURA et al.) 07.10.2004, todo el documento	1 - 50

☐ En la continuación del recuadro C se relacionan otros documentos ☒ Los documentos de familias de patentes se indican en el anexo

* Categorías especiales de documentos citados:

"A" documento que define el estado general de la técnica no considerado como particularmente relevante.

"E" solicitud de patente o patente anterior pero publicada en la fecha de presentación internacional o en fecha posterior.

"L" documento que puede plantear dudas sobre una reivindicación de prioridad o que se cita para determinar la fecha de publicación de otra cita o por una razón especial (como la indicada).

"O" documento que se refiere a una divulgación oral, a una utilización, a una exposición o a cualquier otro medio.

"P" documento publicado antes de la fecha de presentación internacional pero con posterioridad a la fecha de prioridad reivindicada.

"T" documento ulterior publicado con posterioridad a la fecha de presentación internacional o de prioridad que no pertenece al estado de la técnica pertinente pero que se cita por permitir la comprensión del principio o teoría que constituye la base de la invención.

"X" documento particularmente relevante; la invención reivindicada no puede considerarse nueva o que implique una actividad inventiva por referencia al documento aisladamente considerado.

"Y" documento particularmente relevante; la invención reivindicada no puede considerarse que implique una actividad inventiva cuando el documento se asocia a otro u otros documentos de la misma naturaleza, cuya combinación resulta evidente para un experto en la materia.

"&" documento que forma parte de la misma familia de patentes.

Fecha en que se ha concluido efectivamente la búsqueda internacional.	Fecha de expedición del informe de búsqueda internacional
18.Enero.2006 (18.01.2006)	26-01-2006 26 ENERO 2006
Nombre y dirección postal de la Administración encargada de la búsqueda internacional O.E.P.M. C/Panamá 1, 28071 Madrid, España. Nº de fax 34 91 3495304	Funcionario autorizado M. Alvarez Moreno Nº de teléfono + 34 91 3495495

INFORME DE BÚSQUEDA INTERNACIONAL

Información relativa a miembros de familias de patentes

Solicitud internacional nº

PCT/ ES 2005/000215

Documento de patente citado en el informe de búsqueda	Fecha de publicación	Miembro(s) de la familia de patentes	Fecha de publicación
WO 02056230 A	18.07.2002	US 2002078358 A	20.06.2002
US2002161628A A	31.10.2002	NINGUNO	----------
US 2004195323 A	07.10.2004	US 2003006282 A US 2003178484 A	09.01.2003 25.09.2003