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

(19) Organización Mundial de la Propiedad Intelectual
Oficina internacional

PCT

(43) Fecha de publicación internacional
4 de Junio de 2009 (04.06.2009)

(10) Número de Publicación Internacional
WO 2009/068697 A1

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

(21) Número de la solicitud internacional:
PCT/ES2007/000681

(22) Fecha de presentación internacional:
26 de Noviembre de 2007 (26.11.2007)

(25) Idioma de presentación: español

(26) Idioma de publicación: español

(71) Solicitante *(para todos los Estados designados salvo US)*: **SCYTL SECURE ELECTRONIC VOTING, SA** [ES/ES]; C/ Tuset, 20 1-7, E-08006 Barcelona (ES).

(72) Inventores; e

(75) Inventores/Solicitantes *(para US solamente)*: **VALLÈS FONTANALS, Pere** [ES/ES]; SCYTL SECURE ELECTRONIC VOTING, SA, c/ Tuset, 20 1-7, E-08006 Barcelona (ES). **PUIGGALÍ ALLEPUZ, Jorge** [ES/ES]; SCYTL SECURE ELECTRONIC VOTING, SA, c/ Tuset, 20 1-7, E-08006 Barcelona (ES). **MORALES ROCHA, Victor Manuel** [ES/ES]; SCYTL SECURE ELECTRONIC VOTING, SA, c/ Tuset, 20 1-7, E-08006 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, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP,

[Continúa en la página siguiente]

(54) Title: METHOD AND SYSTEM FOR THE SECURE AND VERIFIABLE CONSOLIDATION OF THE RESULTS OF ELECTION PROCESSES

(54) Título: MÉTODO Y SISTEMA PARA LA CONSOLIDACIÓN SEGURA Y AUDITABLE DE RESULTADOS DE PROCESOS ELECTORALES

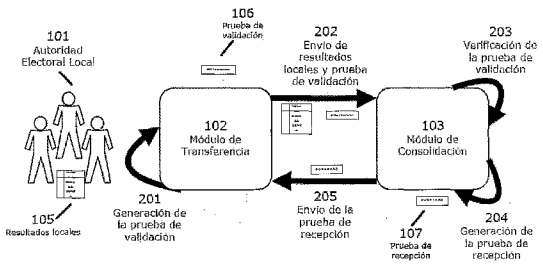

FIGURA 2

101 Local Election Authority
102 Transfer Module
105 Local results
106 Validation test
107 Reception test
201 Generation of validation test
202 Transmission of local results and validation test
203 Verification of validation test
204 Generation of reception test
205 Transmission of reception test

(57) **Abstract:** The invention relates to a method and system for the secure and verifiable consolidation of the results of an election process, in which local election authorities (101) validate local election results by generating a validation test (106). Said validation test is communicated to a consolidation module (103) which verifies that the test (106) has been generated by the correct election authorities. Subsequently a reception test (107) is generated, containing the result of the validation, i.e. the acceptance or non-acceptance of the validation test. Finally the reception test (107) is transmitted to the election authorities in order to provide validation information. The invention also relates to different ways of generating the validation and reception tests for robust verification of the identity of the local election authorities (101) that have participated in the election result validation, verification that the validated local election results are the same as those to be consolidated and preservation of the integrity of the official documents containing the local election results.

(57) **Resumen:** La presente invención describe un método y un sistema para la consolidación segura y auditable de los resultados de un proceso electoral, en el que participan unas autoridades electorales locales (101) para validar, mediante la generación de una prueba de validación (106),

[Continúa en la página siguiente]

WO 2009/068697 A1

KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, 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).

Publicada:

— *con informe de búsqueda internacional*

unos resultados electorales locales. Esta prueba de validación es comunicada a un módulo de consolidación (103), que verificará que dicha prueba de validación (106) haya sido generada por las autoridades electorales correctas. A continuación se generará una prueba de recepción (107) que contendrá el resultado de dicha validación, que podría ser la aceptación o no de dicha prueba de validación. Finalmente la prueba de recepción (107) es enviada a las autoridades electorales para información de dicha validación. La invención también describe distintas formas de generar las pruebas de validación y de recepción, para poder verificar de forma robusta la identidad de las autoridades electorales locales (101) que han participado en la validación de los resultados electorales, para poder verificar si los resultados electorales locales validados son los mismos que se van a consolidar y para preservar la integridad de las actas oficiales de los resultados electorales locales.

Método y sistema para la consolidación segura y auditable de resultados de procesos electorales

Campo de la invención

La presente invención se enfoca principalmente en el campo de los procesos electorales e introduce un método seguro y auditable para la consolidación de resultados. El método proporciona los procesos necesarios para que unas autoridades electorales locales, tales como los miembros de una mesa electoral, comuniquen de forma segura y auditable unos resultados electorales a un centro de consolidación de resultados.

El método es susceptible de ser utilizado en la consolidación de resultados en entornos remotos, tanto en procesos electorales presenciales como remotos.

La invención se refiere también a un sistema para implementar el citado método.

Antecedentes de la invención

La precisión en los resultados es una característica primordial de todo proceso electoral. Tradicionalmente, el recuento de los votos se ha llevado a cabo manualmente, lo cuál tiene como consecuencia un retraso no deseado en la publicación de resultados y sobretodo una alta probabilidad de cometer errores en dicho recuento.

La modernización de los sistemas electorales ha permitido agilizar el recuento de los votos y la precisión en los resultados mediante el uso de dispositivos de voto electrónico (p.Ej., terminales de voto electrónico o máquinas de escaneo de votos). Estos dispositivos permiten generar un registro electrónico de los votos, y por lo tanto la realización de un recuento electrónico más rápido y fiable. También facilitan el envío, tanto de los votos electrónicos como de los resultados locales obtenidos, a un sistema de recuento central que permita la consolidación de los resultados de distintos colegios electorales o canales de voto. Sin embargo, las propuestas actuales sólo contemplan la

protección de la privacidad de los votos o resultados enviados mediante el cifrado. Estas soluciones no incorporan medidas que faciliten auditar la integridad de dichos recuentos locales o identificar si estos resultados han sido avalados por las autoridades encargadas de realizar dicho recuento. De este modo, no es posible verificar de una forma fiable si los recuentos locales recibidos por el centro de consolidación han sido manipulados antes de ser procesados por el centro de consolidación. Adicionalmente, estas propuestas no tienen en cuenta la posibilidad de consolidar resultados que provengan de recuentos manuales, por lo que no son aplicables a entornos de voto tradicional.

Un ejemplo de estas propuestas lo podemos encontrar en la patente US7044375, que describe un sistema en el cuál se lleva a cabo una consolidación central de los resultados de una votación llevada a cabo por medios electrónicos. El sistema tiene un dispositivo de adquisición y comunicación que se encarga de reunir los votos y/o resultados generados en las máquinas de votación y/o recuento locales en los recintos de votación. Esos datos son cifrados y enviados desde cada recinto local hacia un sistema central de consolidación de resultados por medio de un canal de comunicación. El sistema central de consolidación recibe los datos, los descifra y realiza el recuento. El sistema de consolidación envía periódicamente los resultados actualizados a un sistema de publicación de resultados. Tal como se menciona anteriormente, esta solución no incorpora medidas que permitan proteger la integridad de los datos enviados el sistema central. Tampoco incorpora medidas que permitan verificar si los datos enviados han sido verificados por los gestores locales del proceso electoral sino que asume en todo momento que los datos recibidos provienen de una fuente de confianza sin validar ésta.

De forma similar, la patente US20060196939 describe un sistema de votación electrónica que incluye un sistema de recuento de votos centralizado. Los resultados locales de cada precinto electoral son cifrados y enviados a un sistema de recuento centralizado. Dicha transmisión puede ser online o por medio del transporte físico de los dispositivos de almacenamiento de la terminal de recuento local. El dispositivo de almacenamiento local cuenta con una interfaz física que le permite conectarse al sistema de recuento centralizado para efectuar la descarga y descifrado de los resultados locales. El sistema de

recuento centralizado, a través de una red de comunicación, envía los resultados a un sistema de publicación, el cuál se encarga de dar a conocer los resultados.

En ninguno de los dos casos mencionados arriba se proponen acciones que ayuden a preservar la integridad de los resultados. Si bien es cierto que en ambos casos los resultados locales son cifrados antes de ser enviados al servidor central, lo cual los protege durante la transmisión, no se plantean técnicas que garanticen la integridad de los resultados locales antes de ser enviados ni tampoco que puedan garantizar la integridad del resultado final.

Debido a la posibilidad de manipulación de los resultados, existen métodos que pretenden verificar (o auditar) la precisión en el resultado de una elección mediante registros paralelos en diferentes soportes de almacenamiento. Un ejemplo de esto son los sistemas que imprimen cada voto de forma paralela al registro del mismo en un medio electrónico.

El problema principal con los sistemas de registro paralelo de votos es que si uno de los registros es manipulado esto puede ser detectado solamente mediante una auditoría. En caso de detección de una discrepancia en el recuento de ambos registros no es posible saber cuál de ellos ha sido manipulado y por lo tanto no se tiene la certeza de cuál es el resultado correcto.

La presente invención describe un método de consolidación de resultados de un proceso electoral de una manera segura. Dicho método permite la consolidación de resultados locales que se generan en diferentes recintos locales o incluso en diferentes plataformas o canales de votación electrónica. Otro objetivo de la presente invención es proteger la integridad de los resultados locales de la elección, así como comprobar la autoría del oficial o de los oficiales de la elección que envía dichos resultados locales. Además, se pretende con la presente invención generar registros físicos de los resultados locales y proteger su integridad, así como comprobar la autoría de los mismos.

Breve exposición de la invención

La presente invención describe un método para la consolidación de resultados de procesos electorales que permite a unas autoridades electorales,

proteger la seguridad y auditabilidad de los resultados locales de la unidad electoral a la que han sido asignadas esas autoridades. La presente invención describe como parte del método, la generación por parte de uno o más miembros de las autoridades electorales locales de una prueba de validación de los resultados electorales, que permite al menos identificar los miembros de la autoridad electoral que han participado en la validación de los resultados electorales locales. El método también describe la generación de una prueba de validación que además quede vinculada con los resultados electorales locales validados por los miembros de la autoridad electoral local que hayan participado en este proceso de validación. Esta prueba de validación se utilizará para verificar si unos resultados electorales locales a consolidar han sido previamente validados por las autoridades electorales locales asignadas. El método también contempla la comunicación a las autoridades electorales del resultado de dicha verificación.

En una implementación básica, el método comprende las siguientes etapas:

a) Validación por parte de las autoridades electorales locales de una información del resultado electoral local, mediante la generación de una prueba de validación que permita verificar la participación de al menos una parte de dichas autoridades electorales locales en dicha validación;

b) Comunicación de dicha prueba de validación a un modulo de consolidación;

c) Verificación en dicho módulo de consolidación de que la prueba de validación de los resultados locales comunicada ha sido generada por las autoridades locales correctas;

d) Generación en el módulo de consolidación de resultados de una prueba de recepción de al menos dicha prueba de validación y que represente al menos el resultado de la verificación; y

e) Comunicación a las autoridades electorales locales, de la aceptación o no de los resultados locales a partir de la prueba de recepción.

De forma opcional el método contempla que las etapas a) y b) se realicen mediante un módulo de transferencia de información.

En relación a la etapa de generación de la prueba de validación, la invención introduce distintas alternativas para generar dicha prueba de manera que ésta permita identificar la identidad de las autoridades que han participado en la validación de los resultados locales. También propone distintas alternativas, mediante el uso de técnicas criptográficas y/o biométricas, para la generación de la prueba de validación de forma que permita además vincular dicha prueba con los resultados electorales locales validados.

En relación a la etapa de verificación, la invención describe distintas alternativas de verificación de la prueba de validación y acciones soportadas a partir del resultado de dicha validación, como proceder a la aceptación o no de los resultados locales para su consolidación.

La invención también describe distintas alternativas de generación de una prueba de recepción, entre las que se encuentran la de incluir una prueba de integridad generada a partir de los resultados electorales locales aceptados, tal como una firma digital.

Finalmente la invención describe, de forma opcional, cómo se podría utilizar la información de la prueba de recepción para proteger las actas electorales oficiales de los resultados electorales locales. También describe como se podría proteger la privacidad de las pruebas de validación y/o resultados electorales comunicados, mediante el uso de técnicas criptográficas.

Breve descripción de los dibujos

En la figura 1 se muestran un ejemplo de implementación con los principales componentes y procesos de la presente invención. Se muestra cómo unas autoridades electorales locales 101 validan una información de resultados locales 105 comunicada a un módulo de consolidación 103, mediante las siguientes etapas:

- Generación 201 de una prueba de validación 106 a partir de la información de resultados locales 105.

- Comunicación 202 de los resultados locales 105 y de la prueba de validación 106 al módulo de consolidación 103.
- Verificación 203 de la prueba de validación 106 por parte del módulo de consolidación 103.
- Generación 204 de la prueba de recepción a partir del resultado del proceso de verificación.
- Envío 205 de la prueba de recepción 107 a las autoridades electorales locales 105.

La Figura 2 muestra una implementación alternativa del método descrito en la presente invención. En dicha implementación, se utiliza un módulo adicional de transferencia 102 para llevar a cabo la generación 201 de la prueba de validación 106 y para realizar el envío 202 de los resultados locales 105 y de la prueba de validación 106 hacia el módulo de consolidación 103.

La figura 3 muestra dos ejemplos de aplicación de la presente invención. En el ejemplo de la figura 3-a se utiliza una línea telefónica 108 como medio de transmisión para comunicar la información de resultados locales 105. El módulo de transferencia 102 cuenta con una central de llamadas 109 para recibir la información transmitida. El ejemplo de la figura 3-b utiliza como interficie 108 un ordenador para llevar a cabo la introducción de la información de resultados locales 105.

La figura 4 muestra otra implementación alternativa de la presente invención, en la cuál se cuenta con módulos intermedios de consolidación 110. Se muestra un conjunto de autoridades electorales locales 101 en donde cada conjunto representa a las autoridades electorales a cargo de una unidad de gestión electoral. Se muestra en la figura cómo diferentes autoridades electorales locales 101 llevan a cabo el envío 202 de la información de resultados locales 105 y pruebas de validación 106 a diferentes módulos intermedios de consolidación 110. Dichos módulos intermedios de consolidación 110 envían a su vez la información de resultados locales 105 al módulo de

consolidación principal 103 una vez que dicha información de resultados locales 105 ha sido validada y aceptada.

Descripción detallada de la invención

La presente invención se refiere a un método que facilita la consolidación segura de resultados de un proceso electoral, aplicable tanto a entornos de voto presencial como remoto. La consolidación de resultados se lleva a cabo mediante el uso de técnicas y procedimientos que permiten proteger la integridad y auditoría de los resultados electorales.

En esta invención se entenderá por proceso electoral cualquier consulta o solicitud de información de forma pública o privada y a un conjunto de personas limitado o abierto, a partir de la que se realizará posteriormente un resultado acumulativo o cualitativo global o parcial. Ejemplos de procesos electorales, sin ánimo de limitar su definición a ellos, serían votaciones, consultas, encuestas, exámenes o pruebas de evaluación.

Para llevar a la práctica la presente invención se considera la existencia de unas autoridades electorales locales pertenecientes a un colegio electoral o a cualquier otra unidad de gestión electoral (p.Ej., distrito, recinto, municipio, etc.). Estas autoridades electorales podrían estar formadas por un comité electoral (p.Ej., una mesa electoral), uno o más administradores electorales locales, o una combinación de ellos. La función principal de estas autoridades electorales locales es la validación, al menos de una parte de ellas, de los resultados locales de su unidad de gestión electoral. De forma opcional estas autoridades electorales locales o parte de ellas, podrían también haber participado en la obtención del recuento local y/o comunicación de dichos resultados. También estas autoridades electorales locales o parte de ellas, podrían ser las encargadas de generar y/o validar (p.Ej., mediante una firma manuscrita) una acta oficial en papel de los resultados electorales locales de su unidad de gestión electoral. Habitualmente esta acta se adjunta a los votos físicos o electrónicos que han sido utilizados para el recuento local y enviados a las autoridades electorales centrales para su recuento central o auditoría.

Adicionalmente, para la implementación de esta invención, se contempla la existencia de un módulo de consolidación dónde normalmente se comunican

los resultados locales validados. Este módulo verifica que dichos resultados locales comunicados hayan sido validados por las autoridades electorales locales correspondientes, y comunica el resultado de esa verificación a dichas autoridades. Para ello, se contempla que este módulo de consolidación disponga de unos medios de entrada y salida de datos y unos medios de procesamiento, para recibir y verificar una información relacionada a unos resultados locales. Una información relacionada con el resultado de la verificación es comunicada a al menos las autoridades electorales locales. Opcionalmente, dependiendo del resultado de la verificación, este módulo puede almacenar los resultados para su consolidación, por lo que podría disponer de unos medios de almacenamiento. Para facilitar la comunicación remota de los resultados locales y del resultado de la verificación, este módulo podría estar conectado a una red de comunicaciones y recibir los resultados locales y/o la información para la verificación mediante esta red de comunicaciones. Por lo tanto al menos parte de dichos medios de entrada y salida de datos podrían tratarse de una interficie de comunicación analógica o digital.

De forma opcional, para facilitar una comunicación remota de los resultados locales y/o la generación de información de validación, también se contempla la existencia de un módulo de transferencia de información, a través del cual se comunicarán los resultados locales a un módulo de consolidación. Para este fin se contempla que dicho módulo disponga de una interficie de entrada y salida de datos que permita la introducción de dichos resultados y su comunicación hacia el módulo de consolidación. Junto con los resultados locales se puede también comunicar otra información adicional de validación que pueda ser requerida por el módulo de consolidación para verificar si dichos resultados locales han sido previamente validados por la autoridad electoral local pertinente. Esta información de validación puede ser generada en dicho módulo a partir de una información obtenida de al menos parte de las autoridades electorales locales. Para ello, dicho modulo dispondrá de unos medios de procesamiento además de la interficie de entrada y salida de datos.

En una implementación preferente, la invención se iniciará mediante una primera fase de validación por parte de las autoridades electorales locales de una información de un resultado electoral local. Por simplicidad, se asume que

los resultados locales solo pueden ser validados por las autoridades electorales locales asignadas durante la configuración de la elección, aunque podrían participar en este proceso otras entidades (p.Ej., observadores) si el proceso electoral lo permite. Esta validación consistirá en la generación de una prueba de validación de la información de resultado electoral local, que contenga información que permita verificar la identidad de las autoridades que han participado en dicho proceso de validación. Para ello esta prueba de validación deberá contener al menos una información de la identidad de al menos parte de las autoridades que han participado en la generación de la prueba de validación. Esta información de identidad podría generarse a partir de unas credenciales de identificación, tal como una clave de acceso, un registro biométrico o cualquier otra prueba de identidad que pueda permita identificar a las autoridades electorales de forma única. El conjunto o combinación de estas pruebas de identidad formaría la prueba de validación (PV).

$$PV= (Id_1, Id_2 \ldots Id_n) \quad Id_i \text{ prueba de identidad de la autoridad i}$$

Opcionalmente, dicha información de identidad también se podría generar mediante mecanismos que permitan vincular dicha prueba de identidad con la información de los resultados locales. De este modo la prueba de validación, además de identificar a las autoridades que han participado en la validación, también protegería la integridad de la información de resultados locales (i.e., cualquier modificación posterior de la información de resultados locales validados invalidaría la prueba de validez).

En una implementación preferente, esta información de identidad se generará utilizando algoritmos criptográficos, tales como una firma digital o una MAC, aplicados a al menos la información del resultado local utilizando al menos una clave. La clave o claves utilizadas para la implementación de esta firma o MAC estarían en posesión de uno o varios miembros de las autoridades electorales locales que participan en la generación de la prueba de validación. En este sentido, una única clave podría estar en posesión de un único miembro (p.Ej., un administrador de la elección) o custodiada por al menos un subconjunto de las autoridades electorales, mediante la utilización de un

esquema de compartición de secreto o un método equivalente. En una implementación preferente basada en la existencia de una única clave, esta clave se utilizará para generar una firma o MAC sobre la información del resultado local (IRL) o sobre la concatenación de dicha información del resultado electoral con unas pruebas de identidad de las autoridades que también participen en el proceso de validación, y que no dispongan de acceso a la clave. Las pruebas de identidad, tal como se ha mencionado anteriormente, podrían tratarse de cualquier credencial que identifique de forma única a un miembro de la autoridad electoral. Finalmente, la prueba de validación estaría formada por al menos dicha firma digital o MAC obtenida, o la concatenación de esta firma o MAC con las pruebas de identidad utilizadas para su generación. Por ejemplo:

$$PV = S(IRL)$$

$$PV = S(IRL \mid (Id_1, Id_2 \ldots Id_n))$$

$$PV = S(IRL \mid (Id_1, Id_2 \ldots Id_n)) \mid (Id_1, Id_2 \ldots Id_n)$$

$$PV = S(IRL) \mid (Id_1, Id_2 \ldots Id_n)$$

En otra implementación alternativa, se podrían utilizar más de una clave criptográfica para generar la información de identidad. En este caso las firmas digitales o MAC se podrían generar de forma anidada (p.Ej., realizar una firma digital a partir de otra firma digital previa) o se podrían concatenar o combinar entre ellas. En cualquiera de los casos, una o varias de estas firmas se realizarían de al menos la información de resultado electoral local. Al igual que en la anterior implementación basada en una clave única, además de la información de resultado local, también se contempla utilizar en alguna de las firmas las pruebas de identidad de autoridades que participen en la validación de la información de resultado local. En cualquiera de los casos, la prueba de validación contendría al menos la información de identidad y opcionalmente las pruebas de identidad de autoridades que hayan participado en la validación.

Finalmente, como alternativa al uso de algoritmos criptográficos, también se contempla la generación de la información de identidad a partir de uno o más registros biométricos de las autoridades electorales que participen en la validación. Estos registros deberían contener al menos una información

relacionada con la información de resultados locales. Esta información relacionada podría tratarse de la totalidad, parte o una prueba de integridad de los resultados locales. La prueba de integridad de los resultados podría obtenerse mediante la aplicación de una función criptográfica resumen (p.Ej., MD5, SHA1 u otras equivalentes) o una función de compresión (p.Ej., GZIP, RAR o equivalentes), sobre la información de resultado electoral local. Un ejemplo de prueba biométrica relacionada con la información de resultados locales, sin limitar el método únicamente a su uso, podría ser un registro de voz de una o varias autoridades electorales locales mencionando parte del valor de un hash de la información de resultado electoral local. En este sentido la prueba de validación contendría una información de identidad formada de un conjunto de uno o más registros biométricos de autoridades electorales que contengan la información de resultado local. De forma opcional, los registros biométricos podrían haber sido previamente cifrados por una clave simétrica o asimétrica para preservar la privacidad de sus contenidos (p.Ej., un password o una huella dactilar). De este modo los datos no serían accesibles públicamente y sólo el propietario de la clave de descifrado podría acceder a estos datos (p.Ej., autoridades electorales centrales).

Una vez generada la prueba de validación, el método contempla una segunda etapa de comunicación a un módulo de consolidación, de al menos dicha prueba de validación. Opcionalmente, en el caso de que el módulo de consolidación no dispusiera de los resultados locales, éstos podrían ser comunicados junto con la información de recuento local. También de forma opcional, tanto los resultados locales como la prueba de validación podrían ser cifrados total o parcialmente (P.Ej., sólo las partes que se considere importante mantener en secreto, como las credenciales o registros biométricos) antes de ser comunicados. Este cifrado permitirá garantizar la privacidad de los resultados locales y/o de la prueba de validación en los casos que así se requiera. El cifrado se podría llevar a cabo mediante un sistema simétrico o asimétrico indistintamente, siempre que la clave de descifrado esté en posesión de la autoridad a cargo del módulo de consolidación.

En una tercera etapa del método, el módulo de consolidación de resultados verificará si la prueba de validación comunicada ha sido generada por

las autoridades electorales locales correctas. Para ello se procederá a verificar si entre las credenciales, pruebas biométricas, firmas digitales y/o cualquier prueba de identidad contenida en la prueba de validación, se encuentran las identidades de las autoridades locales responsables de realizar esa validación. En este sentido la prueba de validación podría contener, aparte de las identidades requeridas por este proceso de verificación, las identidades de otras autoridades electorales que podrían utilizarse en otros procesos posteriores de auditoría de los resultados. En una implementación básica, el proceso de validación tendría en cuenta todas las identidades contenidas en la prueba de validación. En una implementación alternativa, el proceso de verificación sólo verificaría algunas de las identidades contenidas en la prueba de validación. Por ejemplo, la prueba de identificación podría estar formada por la firma digital (P.Ej., generada por un administrador electoral) de las pruebas de identidad de los miembros de la mesa electoral, pudiendo estar estas últimas cifradas. En este caso, la validación se podría realizar únicamente sobre la identidad de la autoridad electoral que ha realizado la firma y no se tendrían en cuenta el resto de pruebas de identidad. De este modo, si estas últimas estaban cifradas, no sería necesario descifrarlas. Este tipo de verificación es útil en el caso de que la prueba de validación se quiera utilizar en procesos posteriores de verificación o auditoría. Por ejemplo, la validación del resto de pruebas de identidad se podría realizar en un segundo módulo de consolidación que se encontrara en un entorno más seguro.

En el caso de que la prueba de validación se haya generado mediante mecanismos que permitan vincular dicha prueba de identidad con la información de los resultados locales (descritos anteriormente), durante esta etapa de verificación se podría también verificar la correspondencia de la prueba de validación con los resultados locales. Si el mecanismo es una firma digital o un MAC, se procedería a verificar que este MAC o firma digital se corresponda a la información del resultado local comunicado. Si el mecanismo utilizado se basa en técnicas biométricas, se verificará que el registro biométrico contenga la información de resultado local, parte de ella o una prueba de integridad de ella (dependiendo del proceso utilizado en la etapa de validación para generar la prueba de validación).

Una vez verificada la prueba de validación, se procederá a una cuarta etapa de generación de una prueba de recepción, que contendrá al menos el resultado de la verificación. Este resultado de la verificación contenido en la prueba de recepción puede ser un valor numérico, alfanumérico, un texto o la combinación de estos. Por ejemplo, se podría utilizar un 1 para representar que la verificación ha sido correcta o un 0 en el caso de que sea incorrecta. También se puede establecer un valor o texto para uno de los casos (P.Ej., 1) y dejar el otro abierto a cualquier otro valor distinto del anterior (P.Ej., cualquier texto o valor distinto de 1). En una implementación alternativa, en el caso de que la verificación sea positiva, la prueba de recepción podría contener una prueba de aceptación generada a partir de al menos parte de la información de resultado local de la prueba de validación verificada. Esta prueba de aceptación podría ser una firma digital o MAC aplicada sobre al menos parte de la información del resultado local o un identificador único de estos resultados locales. De este modo se podría verificar, a partir de la prueba de aceptación contenida en la prueba de recepción, si los resultados electorales locales verificados de la anterior etapa se corresponden con los validados por las autoridades electorales locales.

De forma alternativa, la prueba de aceptación podría contener un subconjunto de información de esta firma, un resumen (P.Ej., criptográfico) de la firma o un subconjunto de la información del hash de esta firma. El objetivo sería generar una prueba de aceptación que tuviera un tamaño susceptible de ser utilizado para una representación visual o audible de esta prueba de aceptación.

En el caso de que verificación sea positiva el módulo de consolidación podría almacenar la información de resultado local si fuera necesario. En este mismo caso y también opcionalmente, el módulo de consolidación podría almacenar también la prueba de validación junto con la información de resultado o de forma independiente. Tanto la información de resultado de la elección como la prueba de validación se podrían almacenar en el mismo módulo que ha realizado la verificación o en un módulo de consolidación adicional.

Finalmente, en su implementación básica, el método contempla una última etapa de comunicación de la prueba de recepción a al menos las autoridades electorales locales que generaron la prueba de validación. De este

modo estas autoridades son informadas de si la prueba de validación y los resultados electorales locales han sido aceptados o no.

Opcionalmente, en el caso de que la prueba de recepción contenga una prueba de aceptación, dicha prueba de aceptación podría utilizarse para verificar que los resultados electorales locales verificados son los mismos validados anteriormente. Por ejemplo, se podría verificar si la firma contenida en la prueba de aceptación se corresponde a los resultados electorales locales validados por las autoridades electorales locales. También de forma opcional, esta prueba de aceptación podría incluirse en las actas oficiales de los resultados electorales que generan las autoridades locales. Por ejemplo, la prueba de aceptación podría imprimirse o escribirse en las actas oficiales de los resultados presenciales de un precinto o colegio electoral. De este modo, se podría verificar si los resultados contenidos en el acta han sido comunicados y aceptados por el módulo de consolidación, verificando la existencia de la prueba de aceptación en la acta. Si además la prueba de aceptación se generó a partir de una firma digital de la información de resultado local, también se podría verificar la integridad del acta comprobando que los resultados reportados en ella se corresponden a los de la firma contenida en la prueba de aceptación.

Llegados a este punto de la invención, ya se podría proceder a la consolidación de resultados (o recuento global de la elección) a partir del conjunto de resultados electorales locales aceptados por el módulo de consolidación. Estos resultados electorales locales podrían haber sido almacenados por el mismo módulo de consolidación tal como se describe anteriormente o haber sido almacenados mediante otros procesos independientes a las etapas mencionadas en la invención. En el caso en que la información de resultado local estuviera parcial o totalmente cifrada por las autoridades electorales locales, se llevará a cabo una etapa adicional de descifrado de dicha información antes de consolidar los resultados. Este proceso de descifrado podría realizarse en un módulo de consolidación. El descifrado se realizaría utilizando la clave privada en posesión de un único miembro de la autoridad electoral central. De manera alternativa, la clave privada podría estar custodiada por un conjunto de miembros de autoridades electorales centrales. Esto sería posible mediante un esquema de compartición de secreto, en el cuál

cada autoridad electoral posee una parte de la clave privada. Para llevar a cabo el descifrado, el total o un subconjunto predefinido de las autoridades electorales deben colaborar para reconstruir la clave y entonces llevar a cabo el descifrado.

Adicionalmente, antes de proceder a la consolidación de los resultados, se podría realizar un segundo paso de validación de las identidades de la prueba de validación que no hubieran sido verificadas anteriormente. Si las pruebas de identidad están cifradas, se procedería a su descifrado utilizando un procedimiento parecido al descifrado de la información de resultado local descrito anteriormente. En el caso de que estas identidades no se correspondieran con las asignadas durante el proceso de configuración de la elección, se podría aislar las informaciones de los resultados locales relacionados con las pruebas de validación rechazadas. De este modo, estas informaciones de resultado local no se utilizarían en la consolidación final. Por ejemplo, partiendo del anterior ejemplo en el que la prueba de validación contenía las pruebas de identidad cifradas de los miembros de la mesa electoral firmadas por una autoridad electoral, la validación de las identidades de los miembros de la mesa electoral se realizaría en esta etapa.

Para concluir el proceso, el módulo de consolidación podría realizar también el proceso de recuento final de resultados.

En un ejemplo de implementación práctica de este método, el módulo de consolidación podría estar totalmente aislado, es decir, sin ninguna conexión de red. En este caso, la comunicación de los resultados locales y/o prueba de validación podría llevarse a cabo a través de medios de almacenamiento extraíbles. En dichos medios de almacenamiento habrían sido previamente almacenados los resultados locales validados por las autoridades electorales locales, junto con las pruebas de validación. El medio de almacenamiento extraíble será conectado en el módulo de consolidación para que la información contenida pueda ser leída y posteriormente procesada.

En otra implementación práctica de la presente invención se podrá contar con uno o más módulos de consolidación intermedios. Cada uno de esos módulos intermedios recibirá los resultados locales de unidades de gestión electoral previamente asignadas. Cada módulo de consolidación intermedio llevará a cabo los procesos ya descritos de verificación de la prueba de

validación, generación de la prueba de recepción y envío de la misma. Una vez que los módulos de consolidación intermedios hayan recibido y validado la información de todas las unidades de gestión electoral asignadas se reenviará al módulo de consolidación principal al menos la información de resultados locales. Alternativamente, cada módulo de consolidación intermedio realizará un recuento de los resultados locales recibidos, en cuyo caso podrá enviar ese recuento parcial al módulo de consolidación principal.

En otra implementación práctica alternativa de la presente invención, se puede llevar a cabo la consolidación de resultados generados de dos o más canales de votación distintos de manera simultánea. Entre estos se pueden considerar por ejemplo los ya mencionados sistemas de votación electrónica presencial, sistemas de votación por Internet, votación mediante telefonía móvil, votación telefónica (IVR), votación por correo postal y cualquier otro sistema de votación conocido. En esta implementación, el centro de recepción y conteo de votos para cada canal de votación actuaría como una unidad de gestión electoral, representada por unas autoridades electorales. Por lo tanto, los procesos llevados a cabo para la consolidación de los resultados serían iguales a los ya descritos en la implementación preferente.

REIVINDICACIONES

1. Método para la consolidación segura y auditable de resultados de un proceso electoral a partir de unos resultados locales, en el que participan al menos unas autoridades electorales locales, formada por al menos un miembro, para la protección de dichos resultados locales, comprendiendo dicho método para cada resultado local las siguientes etapas:
   a) Validación por parte de las autoridades electorales locales de una información del resultado electoral local, mediante la generación de una prueba de validación que permita verificar la participación de al menos una parte de dichas autoridades electorales locales en dicha validación;
   b) Comunicación de dicha prueba de validación a un modulo de consolidación;
   c) Verificación en dicho módulo de consolidación de que la prueba de validación de los resultados locales comunicada ha sido generada por las autoridades locales correctas;
   d) Generación en el módulo de consolidación de resultados de una prueba de recepción de al menos dicha prueba de validación y que represente al menos el resultado de la verificación; y
   e) Comunicación a las autoridades electorales locales de la aceptación o no de la prueba de recepción, a partir de la prueba de recepción.
2. Método según la reivindicación 2 caracterizado por comunicar adicionalmente en la etapa b) el resultado electoral local validado en la etapa a).
3. Método según la reivindicación 1 ó 2 caracterizado por utilizar un módulo de transferencia de información para la comunicación del la prueba de validación y/o resultado electoral local de la etapa b).

4. Método según la reivindicación 3 caracterizado por utilizar dicho módulo de transferencia de información para generar la prueba de validación de la etapa a).
5. Método según la reivindicación 1 caracterizado por generar la prueba de validación de la etapa a) a partir de al menos una prueba de identidad de al menos una parte de las autoridades electorales locales que han participado en la validación del resultado electoral local.
6. Método según reivindicación 5 caracterizado porque la prueba de identidad se obtiene a partir de unas credenciales de identificación del grupo que comprende una clave de acceso, un registro biométrico o cualquier otra prueba de identidad única.
7. Método según la reivindicación 1 ó 6 caracterizado porque la prueba de identidad se obtiene a partir de un mecanismo que permita vincular dicha prueba de identidad con la información de resultados locales.
8. Método según la reivindicación 7 caracterizado porque el mecanismo utilizado es un algoritmo criptográfico, del grupo que comprende una firma digital o una función MAC, aplicado sobre al menos parte de la información de resultado electoral local y/o al menos una prueba de identidad, utilizando una clave criptográfica.
9. Método según la reivindicación 7 caracterizado porque el mecanismo utilizado es un registro biométrico de al menos una de las autoridades electorales locales y que contenga parte, un resumen o una compresión de la información de los resultados locales.
10. Método según la reivindicación 9 caracterizado por utilizar como registro biométrico un registro audible o escrito de una o varias autoridades locales.
11. Método según la reivindicación 1 ó 2 caracterizado por comprender una etapa previa a la etapa b) que consiste en cifrar de manera parcial o total la prueba de validación y/o la información de resultados locales mediante un sistema de cifrado simétrico o asimétrico.
12. Método según la reivindicación 1 caracterizado por realizar en la verificación de la prueba de validación de la etapa c) una comprobación de que las pruebas de identidad, que son al menos

una, contenidas en la prueba de validación corresponden a unas mínimas autorizadas para realizar la validación de los resultados electorales locales.

13. Método según la reivindicación 2 caracterizado por realizar en la verificación de la prueba de validación de la etapa c) una comprobación de que las pruebas de identidad, que son al menos una, contenidas en la prueba de validación corresponden a unas mínimas autorizadas para realizar la validación de los resultados electorales locales.

14. Método según la reivindicación 2 ó 13 caracterizado por realizar en la verificación de la prueba de validación de la etapa c) una comprobación de que la prueba de validación se corresponda con los resultados electorales locales.

15. Método según la reivindicación 14 caracterizado porque esta comprobación consiste en verificar si las firmas digitales contenidas en la prueba de validación se corresponden con la información firmada y que al menos una de ellas se haya realizado utilizando los resultados electorales locales.

16. Método según la reivindicación 1 caracterizado porque la prueba de recepción de los resultados locales de la etapa d) contenga al menos el resultado de la verificación como una representación numérica, alfanumérico, un texto o la combinación de ellas.

17. Método según la reivindicación 16 caracterizado porque la prueba de recepción de los resultados electorales locales contiene una prueba de aceptación generada a partir de al menos la información de resultado local de la prueba de validación verificada.

18. Método según la reivindicación 17 caracterizado porque dicha prueba de aceptación contiene al menos parte o un resumen de una firma digital o una función MAC aplicada sobre al menos la información de resultado local de la prueba de validación verificada.

19. Método según la reivindicación 16 caracterizado porque las autoridades electorales locales utilizan dicha prueba de aceptación

contenida en la prueba de recepción para verificar que los resultados locales aceptados son correctos.

20. Método según la reivindicación 16 caracterizado por incluir dicha prueba de aceptación de manera escrita o impresa en una acta oficial de resultados locales generada por las autoridades electorales locales.

21. Método según la reivindicación 1 caracterizado por almacenar en el módulo de consolidación los resultados electorales locales y/o dicha prueba de validación.

22. Método según la reivindicación 11 caracterizado por comprender en el módulo de consolidación una etapa adicional de descifrado de los resultados electorales locales y/o prueba de validación.

23. Método según la reivindicación 22 caracterizado porque la clave utilizada para descifrar se encuentra repartida entre un conjunto de autoridades electorales mediante un esquema de compartición de secreto.

24. Sistema para la consolidación segura de los resultados de un proceso electoral a partir de la recolección de resultados locales, para implementar el método descrito en las reivindicaciones 1 a 23, caracterizado por comprender un módulo de consolidación configurado para recibir la información de resultados locales y pruebas de validación, que comprende al menos:

   i. unos medios de entrada/salida de datos que permitan recibir al menos la prueba de validación y devolver una prueba de recepción de dichos resultados locales; y

   ii. unos medios de procesamiento que permitan la verificación de la prueba de validación y la generación de una prueba de recepción.

25. Sistema según la reivindicación 24 caracterizado por utilizar un módulo adicional de transferencia por medio del cuál se envía la prueba de validación y/o información de resultados locales hacia el módulo de consolidación, que comprende al menos:

i. unos medios de entrada/salida de datos que permitan introducir y enviar la prueba de validación y/o información de resultados locales, recibir una prueba de recepción y mostrar el resultado de la verificación contenido en la prueba de recepción.

ii. unos medios de procesamiento que permitan generar una prueba de validación de la información de resultados locales.

26. Sistema según la reivindicación 24 caracterizado porque al menos parte de los medios de entrada/salida están conectados a una red de comunicación del grupo que comprende una red local, global o punto a punto.

27. Sistema según la reivindicación 24 caracterizado porque dicho módulo de consolidación dispone de unos medios de almacenamiento para almacenar la prueba de validación, la información de resultado electoral local y/o una clave criptográfica.

28. Sistema según la reivindicación 25 caracterizado porque al menos parte de los medios de entrada/salida de datos de dicho módulo de transferencia son un dispositivo de captación de información biométrica del grupo que comprende un scanner de huellas dactilares, un dispositivo de registro de voz, una tableta digitalizadora o un scanner de documentos.

29. Sistema según la reivindicación 25 caracterizado porque al menos parte de los medios de entrada/salida de dicho módulo de transferencia están conectados a una red de comunicación digital del grupo que comprende una red local, global o punto a punto, una red de comunicación analógica del grupo que comprende una red de telefonía o una red de video, o una impresora.

30. Sistema según la reivindicación 24 caracterizado porque dicho módulo de consolidación es un ordenador personal, un servidor conectado o no a una red de comunicación, o un servidor de IVR conectado al menos a una red de telefonía.

31. Sistema según la reivindicación 25 caracterizado porque dicho módulo de transferencia es un dispositivo con capacidad de cómputo del grupo que comprende un ordenador personal, una PDA o un teléfono móvil conectado a una red de comunicación.

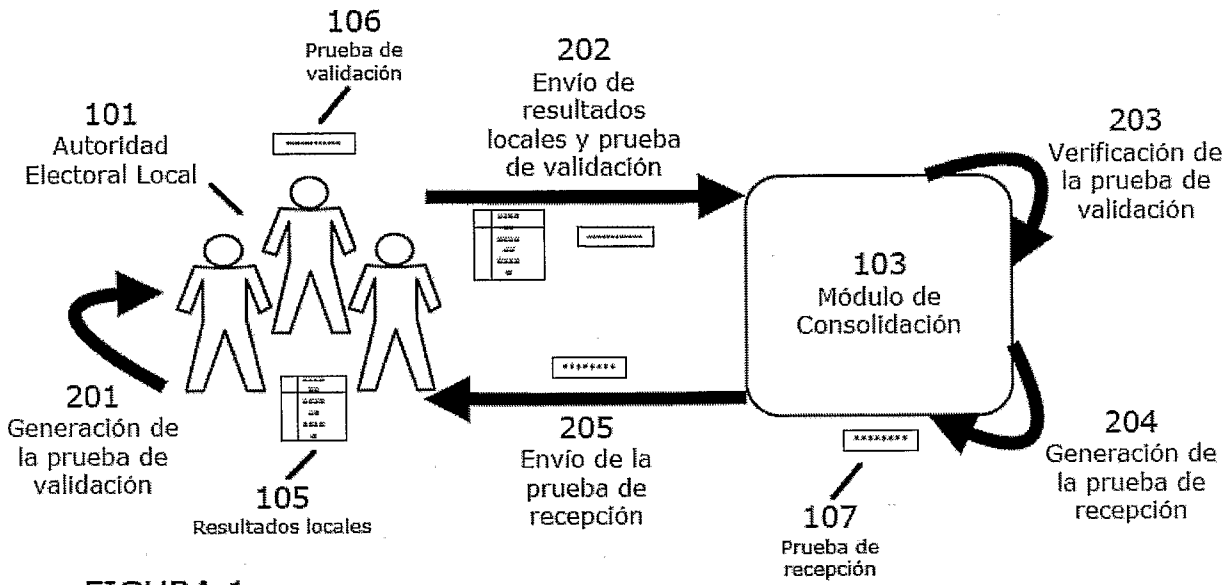

FIGURA 1

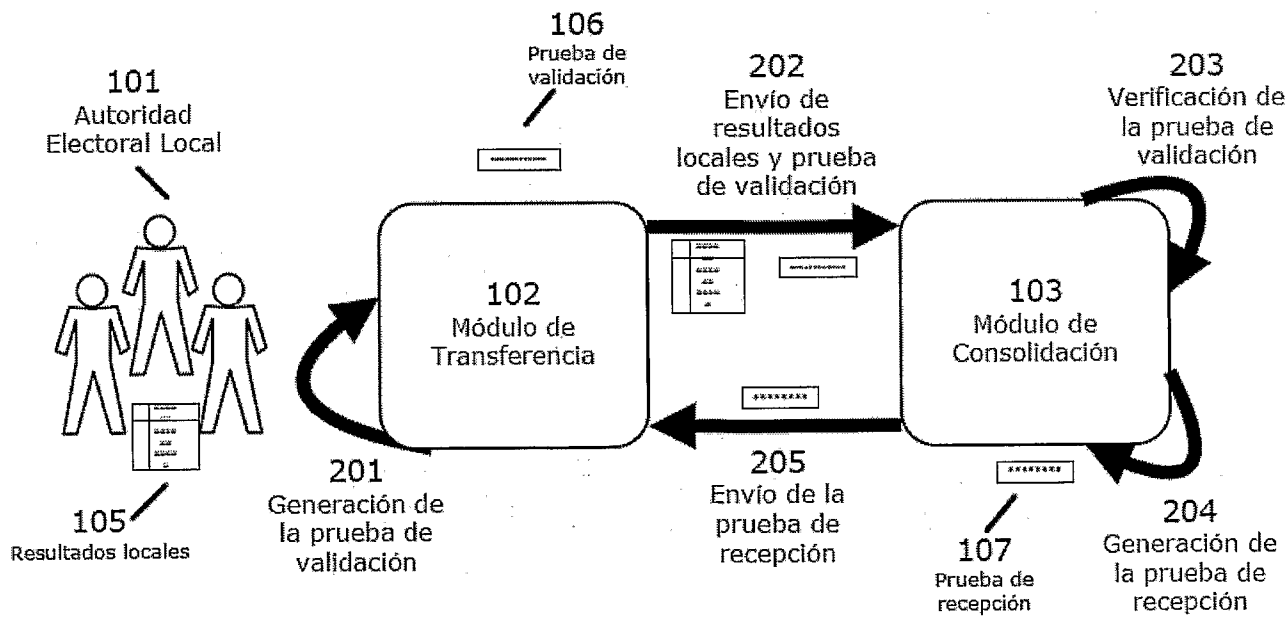

FIGURA 2

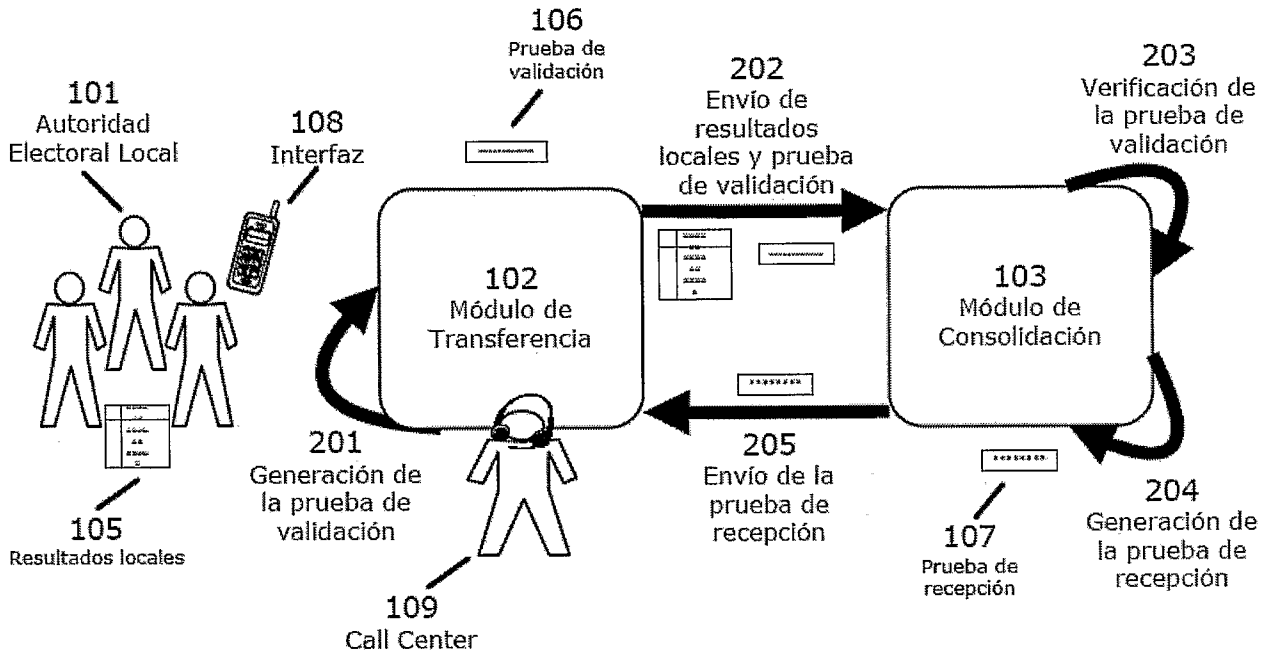

Figura 3-a

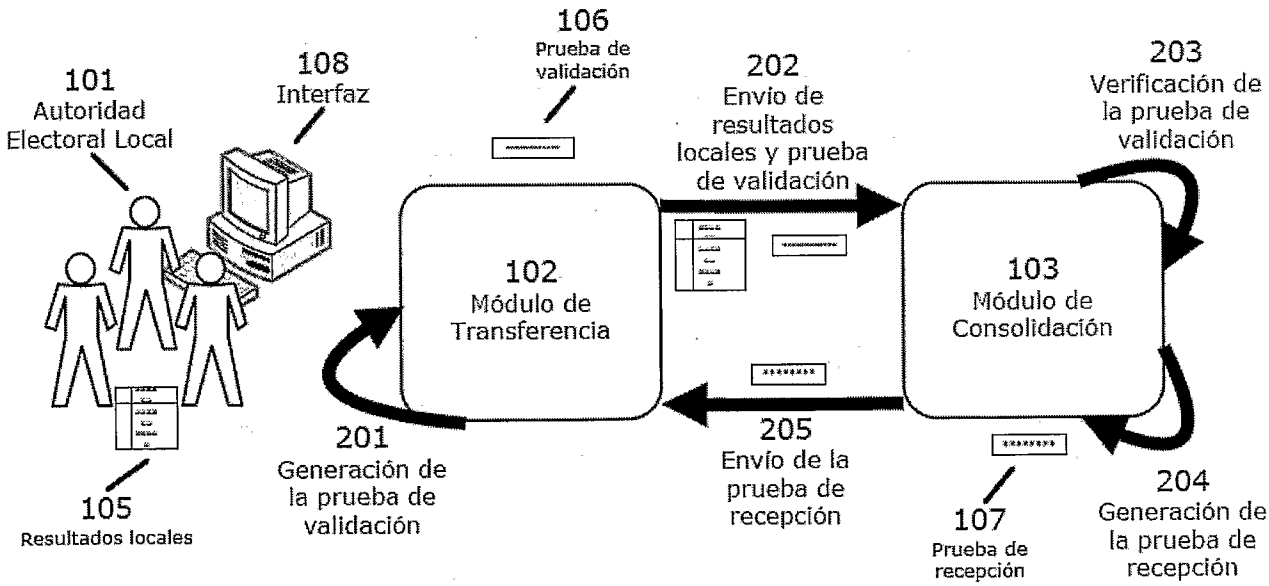

Figura 3-b

FIGURA 3

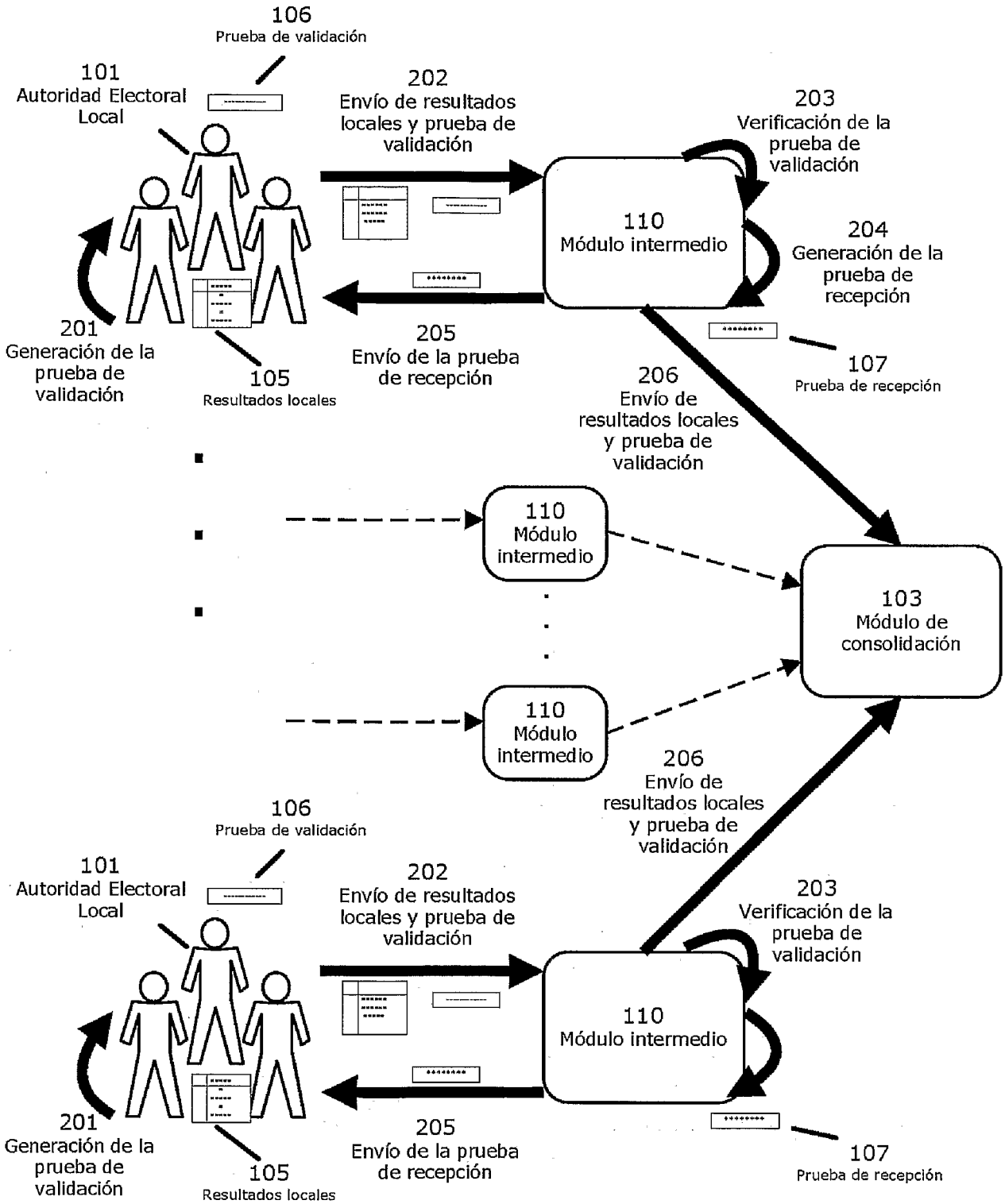
106
Prueba de validación
101
Autoridad Electoral Local
202
Envío de resultados locales y prueba de validación
203
Verificación de la prueba de validación
110
Módulo intermedio
204
Generación de la prueba de recepción
201
Generación de la prueba de validación
205
Envío de la prueba de recepción
105
Resultados locales
107
Prueba de recepción
206
Envío de resultados locales y prueba de validación
110
Módulo intermedio
103
Módulo de consolidación
110
Módulo intermedio
206
Envío de resultados locales y prueba de validación
106
Prueba de validación
101
Autoridad Electoral Local
202
Envío de resultados locales y prueba de validación
203
Verificación de la prueba de validación
110
Módulo intermedio
201
Generación de la prueba de validación
205
Envío de la prueba de recepción
105
Resultados locales
107
Prueba de recepción

FIGURA 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/ ES 2007/000681

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, H04L

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)

INVENES,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	US 2004117244 A1 (SCOTT) 17.06.2004, paragraphs [0003-0004];	1-31
A	US 2006202031 A1 (CHUNG ET AL) 14.09.2006, paragraphs [0069-0071];	1-31
A	US 2004169077 A1 (PETERSEN ET AL) 02.09.2004, paragraphs [0233-0235]; paragraphs [0363-0366];	1-31
A	WO 0211025 A2 (RPOST INTERNATIONAL) 07.02.2002, page 22, line 15 - page 23, line 30;	1-31

☐ 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 document 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 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
31 July 2008 (31.07.2008)	(05-08-2008)
Name and mailing address of the ISA/ O.E.P.M. Paseo de la Castellana, 75 28071 Madrid, España. Facsimile No. 34 91 3495304	Authorized officer M. Alvarez Moreno Telephone No. +34 91 349 54 95

Form PCT/ISA/210 (second sheet) (July 2008)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/ ES 2007/000681

Patent document cited in the search report	Publication date	Patent family member(s)	Publication date
US 2004117244 A	17.06.2004	US 7044375 B	16.05.2006
			16.05.2006
			16.05.2006
US 2006202031 A	14.09.2006	US 2003006878 A	09.01.2003
		US 6961000 B	01.11.2005
		US 2003026462 A	06.02.2003
		US 7197167 B	27.03.2007
		WO 03012595 A	13.02.2003
		CA 2456098 A	13.02.2003
		US 2003052788 A	20.03.2003
		US 7158030 B	02.01.2007
		US 2003062411 A	03.04.2003
		US 6892944 B	17.05.2005
		US 2003136835 A	24.07.2003
		US 6973581 B	06.12.2005
		WO 03062961 A	31.07.2003
		AU 2003207671 A	02.09.2003
		US 2003173404 A	18.09.2003
		US 7077313 B	18.07.2006
		EP 1421459 A	26.05.2004
		EP 20020761211	01.08.2002
		US 2005092835 A	05.05.2005
		US 2005110640 A	26.05.2005
		US 7382255 B	03.06.2008
		US 2006255145 A	16.11.2006
		US 2007170253 A	26.07.2007
US 2004169077 A	02.09.2004	US 6951303 B	04.10.2005
			04.10.2005
			04.10.2005
WO 0211025 A	07.02.2002	CA 2417531 A	07.02.2002
		AU 7802501 A	13.02.2002
		US 2003172120 A	11.09.2003
		US 2006112165 A	25.05.2006
		EP 1410278 A	21.04.2004
		EP 20010955979	25.07.2001
		BR 0112960 A	08.06.2004
		JP 2004521404 T	15.07.2004
		CN 1653458 A	10.08.2005
		MXPA 03000807 A	16.08.2005
		US 2007174402 A	26.07.2007

INFORME DE BÚSQUEDA INTERNACIONAL

Solicitud internacional Nº

PCT/ ES 2007/000681

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 CIP.

B. SECTORES COMPRENDIDOS POR LA BÚSQUEDA

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

G07C, H04L

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)

INVENES,EPODOC,WPI,INSPEC

C. DOCUMENTOS CONSIDERADOS RELEVANTES

Categoría*	Documentos citados, con indicación, si procede, de las partes relevantes	Relevante para las reivindicaciones Nº
A	US 2004117244 A1 (SCOTT) 17.06.2004, párrafos [0003-0004];	1-31
A	US 2006202031 A1 (CHUNG ET AL) 14.09.2006, párrafos [0069-0071];	1-31
A	US 2004169077 A1 (PETERSEN ET AL) 02.09.2004, párrafos [0233-0235]; párrafos [0363-0366];	1-31
A	WO 0211025 A2 (RPOST INTERNATIONAL) 07.02.2002, página 22, línea 15 - página 23, línea 30;	1-31

☐ 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
31 Julio 2008 (31.07.2008)	05-AGOSTO-2008 (05-08-2008)
Nombre y dirección postal de la Administración encargada de la búsqueda internacional O.E.P.M. Paseo de la Castellana, 75 28071 Madrid, España. Nº de fax 34 91 3495304	Funcionario autorizado M. Alvarez Moreno Nº de teléfono +34 91 349 54 95

INFORME DE BÚSQUEDA INTERNACIONAL

Información relativa a miembros de familias de patentes

Solicitud internacional Nº

PCT/ES 2007/000681

Documento de patente citado en el informe de búsqueda	Fecha de Publicación	Miembro(s) de la familia de patentes	Fecha de Publicación
US 2004117244 A	17.06.2004	US 7044375 B	16.05.2006
			16.05.2006
			16.05.2006
US 2006202031 A	14.09.2006	US 2003006878 A	09.01.2003
		US 6961000 B	01.11.2005
		US 2003026462 A	06.02.2003
		US 7197167 B	27.03.2007
		WO 03012595 A	13.02.2003
		CA 2456098 A	13.02.2003
		US 2003052788 A	20.03.2003
		US 7158030 B	02.01.2007
		US 2003062411 A	03.04.2003
		US 6892944 B	17.05.2005
		US 2003136835 A	24.07.2003
		US 6973581 B	06.12.2005
		WO 03062961 A	31.07.2003
		AU 2003207671 A	02.09.2003
		US 2003173404 A	18.09.2003
		US 7077313 B	18.07.2006
		EP 1421459 A	26.05.2004
		EP 20020761211	01.08.2002
		US 2005092835 A	05.05.2005
		US 2005110640 A	26.05.2005
		US 7382255 B	03.06.2008
		US 2006255145 A	16.11.2006
		US 2007170253 A	26.07.2007
US 2004169077 A	02.09.2004	US 6951303 B	04.10.2005
			04.10.2005
			04.10.2005
WO 0211025 A	07.02.2002	CA 2417531 A	07.02.2002
		AU 7802501 A	13.02.2002
		US 2003172120 A	11.09.2003
		US 2006112165 A	25.05.2006
		EP 1410278 A	21.04.2004
		EP 20010955979	25.07.2001
		BR 0112960 A	08.06.2004
		JP 2004521404 T	15.07.2004
		CN 1653458 A	10.08.2005
		MXPA 03000807 A	16.08.2005
		US 2007174402 A	26.07.2007