(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 811 128**

(51) Int. CI.:

G07C 13/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.08.2016 E 16184546 (6)**

(97) Fecha y número de publicación de la concesión europea: **06.05.2020 EP 3136354**

(54) Título: **Método de aseguramiento y de verificabilidad de un voto electrónico**

(30) Prioridad:

28.08.2015 FR 1558047

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.03.2021

(73) Titular/es:

ELECTION-EUROPE (100.0%)
1 place Paul Verlaine
92100 Boulogne Billancourt, FR

(72) Inventor/es:

JAMIN, RÉGIS y
DAHL, CHRISTOPHER

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método de aseguramiento y de verificabilidad de un voto electrónico

La invención tiene por objeto un método de aseguramiento y de verificabilidad de un voto electrónico.

Los sistemas de voto electrónico pueden estar sometidos a problemáticas de seguridad, especialmente en lo que concierne a la integridad y fiabilidad de los datos de voto.

Se conocen sistemas de voto electrónico basados en softwares que utilizan un sistema de cifrado de tipo cifrado RSA por un módulo o un programa inspirado en el lenguaje Java. Sin embargo, con tales sistemas, el cifrado y la transmisión de la papeleta de voto son efectuados únicamente con los medios informáticos utilizados por el votante, por ejemplo con el ordenador del votante. Además, con tales sistemas, se utilizan las mismas claves de cifrado para cada votante. En particular, la papeleta de voto cifrada es enviada directamente a una base de datos de alojamiento, una urna virtual, y no se efectúa control alguno de integridad de los datos y por tanto de fiabilidad de los datos. De esta manera, estos sistemas son potencialmente vulnerables, especialmente a la modificación de los programas o de los módulos inspirados en el lenguaje Java y a una interceptación y manipulación de un componente « html » de la página de internet de la papeleta de voto.

Además, un sistema de voto electrónico debe responder a las exigencias de la Comisión Nacional de la Informática y de las Libertades (CNIL) la cual preconiza especialmente que las papeletas de voto sean cifradas de modo ininterrumpido, lo que necesita la utilización de software embarcado en el navegador de internet, pero también responder a las exigencias de la Agencia Nacional de la Seguridad y de los Sistemas de Información (ANSSI), la cual recomienda evitar la utilización de aplicaciones ligeras tales como las aplicaciones Java en los navegadores de internet para gestionar la seguridad de las transacciones. Un sistema de voto electrónico debe igualmente conformarse al referente de seguridad del OWASP (Open Web Application Security Project) Top Ten 2013.

El documento US2002/077887 A1 describe una arquitectura que permite el voto electrónico anónimo en Internet utilizando tecnologías de clave pública.

El documento US2010/121765 A1 concierne a un procedimiento y a un dispositivo de voto electrónico en redes, que comprenden sistemas informáticos en los cuales se ponen en práctica un sistema de cabina de votación, un sistema validador y un sistema de tabla de resultados.

El documento WO02/056230 A2 concierne a una instalación para escrutinio. Esta instalación hace intervenir una infraestructura pública de clave que se emplea durante la elección.

Debido a esto, hay una necesidad de un sistema de voto electrónico que permita garantizar el anonimato de la papeleta de voto, así como la fiabilidad, la confidencialidad, la integridad y la unicidad del voto electrónico.

A tal efecto, la invención tiene por objeto un método de aseguramiento y de verificabilidad de un voto electrónico, siendo puesto en práctica el método por medios informáticos y que comprende:

- una etapa de recepción de una papeleta de voto temporal, en el transcurso de la cual se recibe de una entidad votante una papeleta de voto temporal, estando la papeleta de voto cifrada por medio de una clave de cifrado pública de voto,

- una etapa de recepción de una papeleta de voto de validación, en el transcurso de la cual se recibe de la citada entidad votante una papeleta de voto de validación, estando la papeleta de voto de validación cifrada por medio de una clave de cifrado pública de validación,

- una etapa de descifrado, en el transcurso de la cual se descifra la papeleta de voto de validación por medio de una clave privada de validación asociada a la citada clave de cifrado pública de validación,

- una etapa de validación, en el transcurro de la cual se envía a la citada entidad votante una petición de validación generada a partir de la papeleta de voto de validación descifrada,

siendo repetidas las etapas precedentes hasta la validación de la petición de validación por la citada entidad votante a continuación de lo cual se registra la papeleta de voto temporal cifrada como papeleta de voto definitiva en espera de su recuento.

Ventajosamente, el método de aseguramiento y de verificabilidad de un voto electrónico permite responder a los paradigmas de las recomendaciones gubernamentales en materia de seguridad emitidas por la CNIL y la ANSSI, al tiempo que se conforman al referente de seguridad del OWASP Top Ten 2013.

Además, la papeleta de voto es sometida a un doble cifrado y el cifrado de la papeleta de voto se realiza de manera ininterrumpida.

De modo ventajoso, la utilización de una papeleta de voto de validación permite a la entidad votante verificar su voto electrónico antes de que este último sea tenido en cuenta, y así validar si el mismo corresponde a su voto, o invalidarlo si el mismo difiere de su elección.

Además, al método de aseguramiento y de verificabilidad de un voto electrónico permite garantizar la fiabilidad, la confidencialidad, la integridad, la unicidad y el anonimato de la papeleta de voto electrónico.

El método según la invención puede igualmente comprender una o varias de las características siguientes, consideradas individualmente o según cualesquiera combinaciones posibles:

- el método comprende, previamente a las etapas de recepción de una papeleta de voto temporal y de validación, una etapa de envío en el transcurso de la cual se envía a una entidad votante al menos una definición de papeleta de voto, una clave de cifrado pública de voto y una clave de cifrado pública de validación; y/o

- el método comprende, previamente a la etapa de envío, una etapa de selección de al menos una clave de cifrado pública de validación en el transcurso de la cual se selecciona aleatoriamente una clave de cifrado pública de validación entre un conjunto de claves de cifrado públicas de validación, y/o

- la clave de cifrado pública de validación es diferente de la clave de cifrado pública de voto; y/o

- la clave de cifrado privada de voto asociada a la clave de cifrado pública de voto es diferente de la clave de cifrado privada de validación asociada a la clave de cifrado pública de validación; y/o

- el método comprende, previamente a la etapa de validación, una etapa de verificación por el votante en el transcurso de la cual se verifica el contenido de la papeleta de voto de validación; y/o

- en el transcurso de la etapa de validación se suprime la papeleta de voto de validación en cuanto se genera la petición de validación; y/o

- la papeleta de voto temporal no es descifrada; y/o

- previamente a la repetición de las etapas se suprime la papeleta de voto temporal cifrada; y/o

- la clave de cifrado privada de voto asociada a la clave de cifrado pública de la papeleta de voto temporal es accesible únicamente a los asesores de la votación.

La invención se refiere igualmente a un producto de programa informático, tal como un producto de programa de ordenador, que comprende una o varias secuencias de instrucciones almacenadas y accesibles a un procesador, y que, cuando son ejecutadas por el procesador, llevan al procesador a ejecutar las etapas del método según la invención.

La invención concierne igualmente a un soporte de almacenamiento legible por un medio informático, comprendiendo el soporte de almacenamiento al menos un programa, y en el cual el programa lleva al ordenador a ejecutar las etapas del método según la invención.

La invención tiene igualmente por objeto un aparato que comprende un procesador configurado para almacenar una o varias secuencias de instrucciones y para ejecutar al menos una de las etapas del método según la invención.

Salvo indicación en contrario, los términos « calcular », « determinar », « evaluar » o equivalente, se refieren a la acción de un medio informático que manipula y/o transforma datos físicos, como datos electrónicos o cantidades en el seno de los registros y/o de las memorias, en otros datos físicos, como cantidades en el seno de las memorias del sistema informático, de los registros o de otros medios de almacenamiento, de transmisión o de visualización.

Además, los modos de realización de la presente invención no se describen en referencia a un lenguaje de programación particular. Una variedad de lenguajes de programación pueden ser utilizados para poner en práctica el método de la invención.

Otras características y ventajas de la presente invención se pondrán de manifiesto en la lectura de la descripción y de las figuras siguientes:

- la figura 1 ilustra una arquitectura del entorno de la ejecución de un voto electrónico según un modo de realización de la invención, y

- las figuras 2 y 3 representan un organigrama de las etapas del método de aseguramiento y de verificabilidad de un voto electrónico según un modo de realización de la invención.

Debe observarse que estos dibujos solamente tienen el objetivo de ilustrar el texto de la descripción y en modo alguno constituyen una limitación del alcance de la invención.

En las diferentes figuras, los elementos análogos están designados por referencias idénticas.

La invención se refiere al ámbito del voto electrónico. En particular, un ejemplo de arquitectura del entorno de ejecución de un voto electrónico está ilustrado en la figura 1.

El entorno de un voto electrónico puede comprender actores del sistema de voto electrónico 10, servicios de red 20, servicios de cifrado 30, y servidores de bases de datos 40.

Los actores del sistema de voto electrónico 10 comprenden por ejemplo los electores 11, los miembros de las mesas electorales 12, el Presidente central y los asesores 13 asistidos eventualmente por un ujier o un experto en la materia.

Los servicios de red 20 pueden comprender un sitio de internet 21 del voto electrónico, una interfaz 22 para la administración del voto electrónico y el seguimiento del escrutinio, y un servicio de red de internet 23 para la generación de las claves de cifrado.

Los servicios de cifrado 30 pueden comprender un servicio de red de internet 31 utilizada por el sitio de red de internet 21 de voto electrónico y un servicio de red de internet 32 utilizado por la interfaz 22 de la administración del voto electrónico.

Los servidores de bases de datos 40 comprenden varias bases de datos. Por ejemplo, como está representado en la figura 1, los servidores de bases de datos 40 comprenden una base de datos 41 en la que están almacenadas las claves de cifrado, una base de datos 42 en la que se conservan las definiciones de las papeletas de voto para cada perfil de elector, urnas temporales 43 en las que quedan almacenadas las papeletas de voto en espera de la validación del elector, urnas 44 en las que se conservan las papeletas de voto cifradas validadas correspondientes a cada elección, tablas de resultados 45 completadas después del descifrado de las papeletas de voto, y listas de electores 46.

Los actores del sistema interactúan por ejemplo con los servicios de cifrado 30 de las bases de datos 40 por intermedio de los servicios de red 20.

Ventajosamente, los intercambios entre las diferentes entidades del entorno del voto electrónico se efectúan por una red segura, especialmente una red de internet segura. Por ejemplo, los intercambios pueden efectuarse según el protocolo de transferencia hipertexto seguro (« https »). La conexión segura entre las diferentes entidades del entorno del voto electrónico permite garantizar la confidencialidad y la integridad de las papeletas de voto, garantizando que no se ofrezca ninguna posibilidad a una persona exterior de visualizar la papeleta de voto o de acceder al contenido de la papeleta de voto del elector.

Preferentemente, los tiempos de repuesta de los servicios de red 20, de los servicios de cifrado 30 y de los servidores de datos 40 son optimizados de modo que permitan al elector votar rápidamente y sin limitaciones.

Además, el elector puede votar con plena confidencialidad a partir de cualquier medio informático conectado a la red de internet. En efecto, el elector puede conectarse con el sitio de internet 21 de voto electrónico a través de una conexión segura en modo « https » e identificarse con la ayuda de un identificador y de una contraseña asociada con el fin de efectuar su voto electrónico. No se requiere ninguna telecarga de software, siendo enviadas la definición de las papeletas de voto y las claves de cifrado públicas de voto y de validación al navegador de internet del votante.

Más concretamente, el elector, cuando es registrado en la lista electoral, se asocia a un identificador único que permite asegurarse de la unicidad de voto. A este identificador se asocia una contraseña que permite al elector conectarse al sistema de voto electrónico. Por otra parte, los datos de estado civil correspondientes a un elector se conservan en una base de datos diferente y solo se asocian al mismo cuando sea necesario, por ejemplo para la edición de la lista de electores, para el envío de un acuse de recibo de voto nominativo o para la búsqueda en una lista electoral. De esta manera, a la vista del sistema de voto, un elector queda asociado a un número aleatorio.

Desde su conexión, el sistema establece una transacción, por ejemplo a través de IIS, entre el navegador de internet del elector y el sitio de internet 21 de voto electrónico. A esta transacción se asocia un número aleatorio único por el motor transaccional IIS, el cual se almacenará en una base de datos que representa las acciones de votos electrónicos en curso y cuyo número será asociado al identificador único del elector. A continuación de esta transacción, el elector solo existe por su número de transacción aleatorio asignado por IIS. El número de transacción aleatorio está destinado a durar solo el tiempo del voto electrónico y a borrarse a la confirmación del voto por el elector, o si el elector permanece inactivo demasiado tiempo en el sitio de internet 21 del voto electrónico. El elector por tanto puede intercambiar datos de voto con el sistema con total anonimato de su transacción IIS y a través de una tubería de cifrado SSL/TLS.

La invención concierne a un método de aseguramiento y de verificabilidad de un voto electrónico, especialmente en el entorno de ejecución de un voto electrónico tal como el descrito anteriormente.

El método según la invención es puesto en práctica por medios informáticos, por ejemplo por ordenadores, tabletas conectadas, teléfonos móviles o cualquier medio informático que tenga acceso a una red de internet.

Un modo de realización preferido del método según la invención está representado en la figura 2. El método de aseguramiento y de verificabilidad de un voto electrónico comprende:

- una etapa S10 de recepción de una papeleta de voto temporal,

- una etapa S20 de recepción de una papeleta de voto de validación,

- una etapa S30 de descifrado, y

- una etapa S40 de validación.

Durante la etapa S10 de recepción de una papeleta de voto temporal, se recibe de una entidad votante una papeleta de voto temporal. Una entidad votante corresponde a una entidad que efectúa el voto electrónico, por ejemplo un elector. La papeleta de voto temporal está destinada a ser registrada como papeleta de voto definitiva tras la validación de la entidad votante.

La papeleta de voto de temporal es cifrada por medio de una clave de cifrado pública de voto. La clave de cifrado pública de voto está asociada a una clave de cifrado privada de voto. Más concretamente, un par de claves de cifrado de voto está asociado a una papeleta de voto temporal, después a una papeleta de voto definitiva cuando la papeleta de voto temporal es registrada como papeleta de voto definitiva.

Ventajosamente, el cifrado utilizado es un cifrado asimétrico, de tipo cifrado RSA. Por ejemplo, la clave de cifrado pública de voto permite cifrar la papeleta de voto temporal y la clave de cifrado privada de voto permite descifrar la papeleta de voto definitiva.

La clave de cifrado pública de voto está almacenada en una base de datos 40, por ejemplo la base de datos 41 de almacenamiento de las claves de cifrado. La clave de cifrado pública de voto es generada por el servicio de red de internet 23 para la generación de las claves de cifrado, y después transmitida a la base de datos 41 a través del servicio de red de internet 32 utilizado por la interfaz 22 de la administración del voto electrónico.

La clave de cifrado privada es conservada en un dispositivo de salvaguarda, fuera de la red de internet. Por ejemplo, la clave de cifrado privada de voto puede ser escrita en un dispositivo de salvaguarda, de tipo USB, destinado a ser conservado por el Presidente central y/o los asesores 13 en una caja fuerte. De modo ventajoso, al clave de cifrado privada de voto asociada a la clave de cifrado pública de la papeleta de voto temporal es accesible únicamente a los asesores del voto y cuando el voto haya terminado.

La papeleta de voto temporal cifrada por la entidad votante es recibida por los servicios de red 20, por ejemplo por el sitio de internet 21 del voto electrónico, y después transmitida a un servicio de cifrado 30, especialmente al servicio de red de internet 31.

La papeleta de voto temporal cifrada es almacenada en una base de datos, tal como la urna temporal 43.

En el transcurso de la etapa S20 de recepción de una papeleta de voto de validación, se recibe dela entidad votante una papeleta de voto de validación.

De modo ventajoso, la papeleta de voto temporal y la papeleta de voto de validación son recibidas conjuntamente de la entidad votante.

La papeleta de voto de validación es cifrada por medio de una clave de cifrado pública de validación, asociada a una clave de cifrado privada de validación. Dicho de otro modo, un par de claves de cifrado de validación está asociado a una papeleta de voto de validación.

Ventajosamente, el cifrado de validación es un cifrado asimétrico, de tipo cifrado RSA.

La clave de cifrado privada de validación y la clave de cifrado pública de validación son almacenadas en una base de datos, por ejemplo la base de datos 41 de almacenamiento de las claves de cifrado.

El par de claves de cifrado de validación es generado por el servicio de red de internet 23 para la generación de las claves de cifrado, y después transmitido a la base de datos 41 a través del servicio de red de internet 32.

Ventajosamente, la clave de cifrado pública de validación es diferente de la clave de cifrado pública de voto. Asimismo, la clave de cifrado privada de voto asociada a la clave de cifrado pública de voto es ventajosamente diferente de la clave de cifrado privada de validación asociada a la clave de cifrado pública de validación.

La papeleta de voto de validación cifrada es recibida por los servicios de red 20, por ejemplo por el sitio de internet 21 del voto electrónico, y después transmitida a un servicio de cifrado 30, especialmente a un servicio de red de internet 31 utilizado por el sitio de internet 21 de voto electrónico.

Durante la etapa S30 de descifrado, la papeleta de voto de validación es descifrada por medio de una clave de cifrado privada de validación asociada a la citada clave de cifrado pública de validación.

La clave de cifrado privada de validación es extraída previamente de la base de datos en la cual está almacenada con el fin de poder descifrar la papeleta de voto de validación.

En el trascurso de la etapa S40 de validación, se envía a la entidad votante una petición de validación generada a partir de la papeleta de voto de validación descifrada.

Ventajosamente, la definición de la papeleta de voto es extraída igualmente de la base de datos en la cual está almacenada, por ejemplo la base de datos 42. La definición de una papeleta de voto corresponde al perfil de un elector y los datos que se derivan de él, como por ejemplo los nombres de las listas o de los candidatos que se presentan a la elección. La papeleta de voto de validación descifrada puede ser comparada con la definición de la papeleta de voto antes de que la petición de validación sea enviada a la entidad votante.

Durante la espera de la validación de la petición de validación, la papeleta de voto de validación no es conservada en una base de datos, sino que es almacenada en una memoria del servicio de cifrado 30 que da un carácter efímero a la papeleta de voto de validación.

Después de la recepción de la petición de validación, la entidad votante puede validar o invalidar la petición de validación. Dicho de otro modo, el votante puede validar su voto si el mismo está conforme con su elección, o invalidarlo si no corresponde a su elección.

Las etapas S10 a S40 son repetidas hasta la validación de la petición de validación por la entidad votante.

Cuando la petición de validación es validada por la entidad votante, la papeleta de voto temporal cifrada es registrada como papeleta de voto definitiva en espera de su recuento, y la papeleta de voto de validación es suprimida de la memoria de servicio de cifrado 30.

De modo ventajoso, previamente a la repetición de las etapas, se suprime la papeleta de voto temporal cifrada.

La papeleta de voto temporal no es descifrada.

Después de la validación de la petición de validación, la papeleta de voto temporal es transferida de la base de datos temporal en la cual estaba almacenada hacia una nueva base de datos. Por ejemplo, la papeleta de voto temporal puede ser desplazada de la urna temporal 43 hacia la urna 44 en la que se conservan las papeletas de voto cifradas validadas.

Dicho de otro modo, después de la validación de la petición de validación, se efectúa la validación de la transacción IIS, conocida de otro modo con el término anglófono « commit », y la papeleta de voto temporal es transferida de la base de datos de las papeletas de voto en espera de confirmación a la base de datos de las papeletas de voto definitivas.

Durante el registro de la papeleta de voto definitiva, se registra una indicación de que la citada entidad votante ha votado. Dicho de otro modo, cuando la papeleta de voto temporal cifrada es registrada como papeleta de voto definitiva, se rellena automáticamente la lista de electores y la entidad votante recibe una confirmación de voto.

La validación de la transacción permite activar el registro del elector en la lista de votantes porque la transacción IIS ha terminado.

Preferentemente, no existe ninguna relación entre la base de datos de las papeletas de voto y la base de datos de la lista de electores, de este modo se garantiza el anonimato de los datos intercambiados en la transacción de voto IIS, habiéndose rota la relación entre el nombre del votante y el contenido de su papeleta desde la conexión establecida por el elector, es decir desde su identificación en el sitio de internet 21 de voto electrónico.

El número aleatorio único de la transacción IIS asociado al identificador del elector permite hacer la correspondencia con el elector. El registro automático inmediato permite prevenir cualquier intento de doble voto, y garantizar la unicidad del voto electrónico.

Preferentemente, en el transcurso de la etapa S40 de validación, en cuanto se genera la petición de validación, se suprime la papeleta de voto de validación. Más concretamente, la papeleta de voto de validación, cifrada o descifrada, no es conservada en una base de datos o en un disco duro. La papeleta de voto de validación está destinada a ser almacenada en una memoria viva del servicio de cifrado 30, antes de ser suprimida. La papeleta de voto de validación descifrada puede existir únicamente en el navegador de la entidad votante y en la memoria de un servicio de cifrado, tal como el servicio de red de internet 31 utilizado por el sitio de internet 21 de voto electrónico.

Las etapas S10 a S40 permiten garantizar el cifrado ininterrumpido de la papeleta de voto desde su emisión en los medios informáticos del elector. Además, la generación de una papeleta de voto temporal cifrada y de una papeleta de voto de validación cifrada permite garantizar un doble cifrado de los datos.

Además, la petición de validación recibida por la entidad votante permite al votante verificar la integridad de su voto.

Ventajosamente, se puede generar una pluralidad de papeletas de voto de validación cifradas con diferentes claves de cifrado públicas de validación para cada papeleta de voto temporal. Más concretamente, la petición de validación puede ser generada a partir de una papeleta de voto de validación seleccionada aleatoriamente entre la pluralidad de

papeletas de voto de validación. La selección aleatoria de una papeleta de voto de validación entre la pluralidad de papeletas de voto de validación asociadas a la papeleta de voto temporal permite aumentar la seguridad del voto electrónico.

Como está ilustrado en la figura 3, el método puede igualmente comprender, previamente a la etapa S40 de validación, una etapa S31 de verificación por el votante. En el transcurso de la etapa de verificación S31 por el votante, se verifica el contenido de la papeleta de voto de validación.

La etapa de verificación permite limitar los riesgos de pirateo del voto electrónico. En efecto, el votante puede controlar de manera fiable que su voto ha sido tenido en cuenta por el sistema sin haber sido modificado y que por tanto el mismo no ha sido manipulado, por ejemplo, por un programa malintencionado presente en el ordenador utilizado. En particular, el votante puede asegurarse de que la papeleta de voto de validación transmitida es la que el mismo ha emitido.

El método puede comprender igualmente una etapa S01 de selección de al menos una clave de cifrado pública de validación. En el transcurso de la etapa S01 de selección, se selecciona aleatoriamente al menos una clave de cifrado pública de validación entre un conjunto de claves de cifrado públicas de validación.

Ventajosamente, después de la etapa S01 de selección, el método comprende una etapa S02 de envío. Durante la etapa S02 de envío, se envía a una entidad votante al menos una definición de papeleta de voto, una clave de cifrado pública de voto y una clave de cifrado pública de validación.

Después de una etapa de conexión y de identificación de la entidad votante, se puede enviar al navegador de internet de la entidad votante la definición de la papeleta de voto y las claves de cifrado públicas de voto y de validación.

El método puede igualmente comprender una etapa S50 de recuento. Durante la etapa S50 de recuento, se recibe una clave de cifrado privada de voto asociada a la clave de cifrado pública de voto y se descifran las papeletas de voto definitivo por medio de la citada clave de cifrado privada.

Las claves de cifrado privadas de voto tenidas únicamente por el Presidente y sus asesores son cargadas después del cierre del escrutinio en la base de datos en las que quedarán almacenadas para permitir el recuento después del cierre del escrutinio, por ejemplo la base de datos 41 en la que están almacenadas las claves de cifrado. Las claves de cifrado privadas de voto son utilizadas para descifrar las papeletas de voto definitivas de los votantes. Los resultados del voto son transmitidos a una base de datos, por ejemplo a tablas de resultados 45.

Después del relleno de las bases de datos con los resultados de los votos, se envían informes oficiales que contienen informaciones sobre el resultado de la elección y el contenido de las listas de electores, por ejemplo a los miembros de los colegios electorales.

La invención se ha descrito en el caso en que se reciba de la entidad votante una papeleta de voto de validación. Naturalmente, el método según la invención no está limitado en modo alguno al modo de realización descrito e ilustrado, el cual se ha dado solamente a modo de ejemplo. Por el contrario, el método según la invención podría comprender una pluralidad de papeletas de voto de validación asociadas a la papeleta de voto temporal, de modo que se aumente la seguridad del voto electrónico.

REIVINDICACIONES

1. Método de aseguramiento y de verificabilidad de un voto electrónico, siendo puesto en práctica el método por medios informáticos y que comprende:

- una etapa (S10) de recepción de una papeleta de voto temporal, en el transcurso de la cual se recibe de una entidad votante una papeleta de voto temporal, estando la papeleta de voto cifrada por medio de una clave de cifrado pública de voto,

- una etapa (S20) de recepción de una papeleta de voto de validación, en el transcurso de la cual se recibe de la citada entidad votante una papeleta de voto de validación, estando la papeleta de voto de validación cifrada por medio de una clave de cifrado pública de validación,

- una etapa (S30) de descifrado, en el transcurso de la cual se descifra la papeleta de voto de validación por medio de una clave de cifrado privada de validación asociada a la citada clave de cifrado pública de validación,

- una etapa de validación (S40), en el transcurso de la cual se envía a la citada entidad votante una petición de validación generada a partir de la papeleta de voto de validación descifrada, siendo repetidas las etapas precedentes hasta la validación de la petición de validación por la citada entidad votante, a continuación de lo cual la papeleta de voto temporal cifrada es registrada como papeleta de voto definitiva en espera de su recuento.

2. Método según la reivindicación 1, que comprende, previamente a las etapas (S10, S20) de recepción de una papeleta de voto temporal y de validación, una etapa (S02) de envío en el transcurso de la cual se envía a la citada entidad votante al menos una definición de la papeleta de voto, una clave de cifrado pública de voto y un clave de cifrado pública de validación.

3. Método según la reivindicación precedente, que comprende, previamente a la etapa (S02) de envío, una etapa (S01) de selección de al menos una clave de cifrado pública de validación en el transcurso de la cual se selecciona aleatoriamente al menos una clave de cifrado pública de validación entre un conjunto de claves de cifrado públicas de validación.

4. Método según una cualquiera de las reivindicaciones precedentes, en la cual la clave de cifrado pública de validación es diferente de la clave de cifrado pública de voto.

5. Método según una cualquiera de las reivindicaciones precedentes, en la cual la clave de cifrado privada de voto asociada a la clave de cifrado pública de voto es diferente de la clave de cifrado privada de validación asociada a la clave de cifrado pública de validación.

6. Método según una cualquiera de las reivindicaciones precedentes, que comprende, previamente a la etapa (S40) de validación, una etapa (S31) de verificación por la entidad votante en el transcurso de la cual se verifica el contenido de la papeleta de voto de validación.

7. Método según una cualquiera de las reivindicaciones precedentes, en la cual en el transcurso de la etapa (S40) de validación se suprime la papeleta de voto de validación en cuanto se genera la petición de validación.

8. Método según una cualquiera de las reivindicaciones precedentes, en la cual la papeleta de voto temporal no es descifrada.

9. Método según una cualquiera de las reivindicaciones precedentes, en la cual, previamente a la repetición de las etapas, se suprime la papeleta de voto temporal cifrada.

10. Método según una cualquiera de las reivindicaciones precedentes, la clave de cifrado privada de voto asociada a la clave de cifrado pública de la papeleta de voto temporal es accesible únicamente a los asesores del voto.

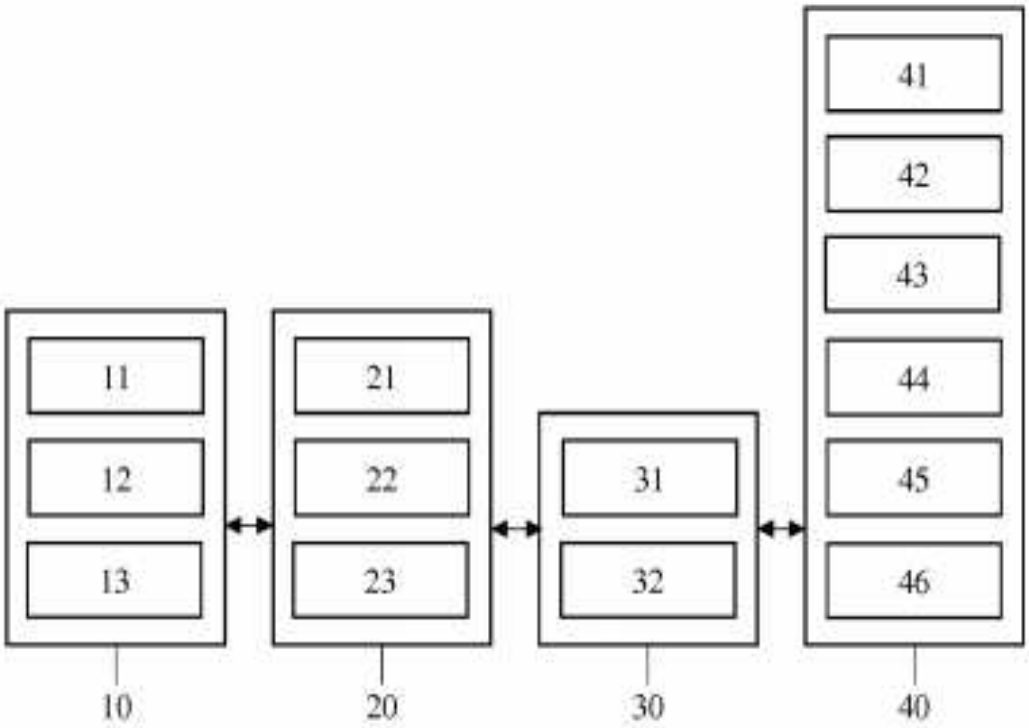

Figura 1

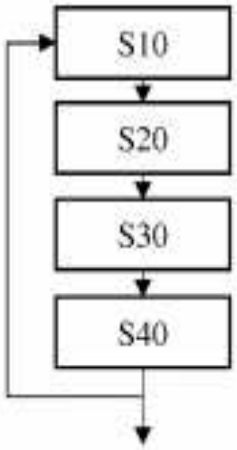

Figura 2

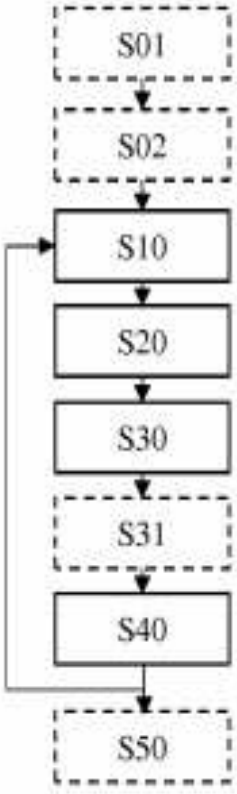

Figura 3