(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 326 175**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05291364 .7**
(96) Fecha de presentación : **24.06.2005**
(97) Número de publicación de la solicitud: **1612991**
(97) Fecha de publicación de la solicitud: **04.01.2006**

(54) Título: **Procedimiento y sistema de votación electrónica en red de alta seguridad.**

(30) Prioridad: **30.06.2004 FR 04 07267**

(45) Fecha de publicación de la mención BOPI:
02.10.2009

(45) Fecha de la publicación del folleto de la patente:
02.10.2009

(73) Titular/es: **FRANCE TELECOM**
6, place d'Alleray
75015 Paris, FR

(72) Inventor/es: **Vernay, Francois;**
Traore, Jacques y
Bonamour, Antoine

(74) Agente: **Justo Bailey, Mario de**

DESCRIPCIÓN

Procedimiento y sistema de votación electrónica en red de alta seguridad.

La invención se refiere a un procedimiento y a un sistema de votación electrónica en red de alta seguridad.

Los procedimientos y sistemas de votación automatizada han sido objeto de profundos estudios debido a las implicaciones psicológicas, humanas y políticas que de ellos se derivan y a las soluciones técnicas que permiten resolver los problemas que éstas plantean.

Según un primer tipo de estos procedimientos y sistemas, la identidad del elector votante se controla manualmente. Este control da acceso al sistema de votación electrónica, que ya sólo tiene que gestionar un encaminamiento fiable de una papeleta de votación electrónica hacia una máquina de recuento de votos.

Un primer tipo precitado corresponde sensiblemente al descrito por la solicitud de patente US2003208395, en la que el elector votante carga en su máquina una papeleta de votación electrónica, constituida por ejemplo por una miniaplicación ("applet"), siendo realizadas por el mismo servidor las operaciones de entrega de la papeleta de votación electrónica, de control de la identidad del elector votante y la recepción de la papeleta de votación electrónica emitida por este último. El modo de autenticación es de tipo biométrico.

El procedimiento y el sistema descritos para la solicitud de patente precitada permiten la puesta en práctica de un procedimiento de autenticación fuerte del elector votante, a costa sin embargo de un desplazamiento físico de éste. Además, el elector votante no puede adquirir la certeza de que su papeleta electrónica ha llegado a su destino, hasta la urna electrónica.

Según un segundo tipo de estos procedimientos y sistemas, estos permiten organizar, dirigir y controlar una votación utilizando Internet. Generalmente, los procedimientos y sistemas ponen en práctica mensajes transmitidos por Internet, obteniéndose estos mensajes, denominados mix-net, mediante baraje o mezclado de los datos.

Un procedimiento de este tipo lo describe, por ejemplo, la solicitud de patente EP1374188, en la que se origina un mix-net mejorado.

En los sistemas precitados, si los módulos de baraje o mezclado utilizan técnicas tales como el cifrado eficaz, es difícil entonces asegurar la integridad de los datos a la salida del procesamiento. Con todo, si se introduce un medio de control de la integridad de los datos, la mezcla obtenida es entonces reversible, lo que rebaja el nivel de seguridad y de confidencialidad de los datos transmitidos.

Según un tercer tipo de estos procedimientos y sistemas, estos últimos utilizan máquinas dedicadas equipadas con medios de autenticación fuerte e interconectadas con una red virtual. Este último tipo ofrece una seguridad óptima, basada en el procedimiento de autenticación fuerte del elector votante, certificado de autenticación de nivel 3, el uso de redes privadas virtuales, de muy difícil implantación, y de puntos de votación.

La solicitud de patente US2002138341 describe un procedimiento y un sistema comparables con los del tercer tipo precitado, al menos por lo que se refiere al uso de mensajes mix-net, un procedimiento de autenticación fuerte, mediante certificado X 509, archivo de texto que contiene información referente a una persona física, firmada y cifrada, estando además la papeleta de votación electrónica cifrada mediante cifrado híbrido.

El sistema descrito en el documento precitado pone además en práctica varios servidores.

Sin embargo, el sistema y el procedimiento precitados no proponen una solución satisfactoria en lo referente al criterio de confianza en los administradores de estos servidores.

En efecto, en el sistema y el procedimiento descritos en este documento, las papeletas firmadas electrónicamente por el elector votante pasan por una primera máquina que comprueba la firma electrónica de este último y la sustituye por una firma específica, propia de la primera máquina, antes de transmitir la papeleta de votación electrónica nuevamente firmada a la urna electrónica.

Esta primera máquina, que desempeña la función de mediador de transacciones, o en su defecto de tercero de confianza, conserva no obstante plena autonomía, antes de introducir o no la papeleta de votación electrónica en la urna electrónica, de romper el anonimato.

Además, el elector votante recibe una papeleta de votación en blanco y la autenticación de la identidad de este último equivale a la autorización de voto, sin más control. La papeleta de votación electrónica cifrada está vinculada al elector votante, al menos en la primera máquina, y cifrada con una fecha.

El procedimiento de cifrado fechado precitado permite protegerse contra la nueva copia de papeletas de votación electrónicas interceptadas de forma ilícita, pero, en contrapartida, presenta el riesgo de permitir la ejecución de inferencias significativas por cotejo.

La problemática que plantea la puesta en práctica de procedimientos y de sistemas de votación electrónica en red aplicada a Internet por vía de procedimientos de autenticación débil y respectivamente fuerte se puede resumir a continuación.

Cuando, por razones de coste de materiales y de complejidad de logística de instauración de la votación, los organizadores eligen una votación electrónica por Internet de autenticación débil, asumen globalmente el riesgo de una seguridad escasa del sistema al menos en tres esferas:

- Los servidores pueden ser víctimas de denegaciones de servicio. Los electores pueden participar, en ocasiones involuntariamente si son víctimas de virus informáticos, en tales disfunciones.

- Los electores votantes, por su parte, están obligados a fiarse de los proveedores de servicios que gestionan las máquinas de votación en lo que respecta tanto al respeto de su anonimato como a la sinceridad del escrutinio.

- Usuarios malintencionados pueden usar el código ubicado en su máquina para ayudarles a llevar a cabo su voto pero tratar de perjudicar la credibilidad de la votación.

El esquema de arquitectura más rudimentaria de un sistema de votación electrónica en red de autenticación débil es el siguiente:

- Se informa al elector votante sobre la dirección del servidor de votación electrónica, por cualquier medio (correo, correo electrónico, prensa...).

- El elector votante se conecta, el día de la votación, desde un terminal, una máquina u otro servidor de votación gracias a la dirección del servidor de votación comunicada.

- El servidor de votación controla los derechos de votar del elector votante, remite una papeleta de votación electrónica "en blanco" a este último, quien la rellena, la devuelve al servidor de votación, que lo contabiliza o no, a título de voto expresado, con las demás papeletas de votación electrónica.

El esquema precitado permite poner de manifiesto los riesgos que verdaderamente se corren en las siguientes esferas:

- Anonimato: el elector votante tiene que identificarse para que se compruebe su derecho de voto. Si las comunicaciones son interceptadas o espiadas, es posible saber a quién vota el elector votante. Por tanto, las comunicaciones tienen que cifrarse. Con el fin de producir un grado de confianza en el sistema, con independencia de la confianza que los electores puedan depositar en el administrador del sistema, hay que utilizar al menos dos servidores distintos, un servidor administrador de votación, para controlar los derechos al voto y autenticar al elector votante y un servidor de recuento de votos, para computar las papeletas.

Sólo una colusión entre los administradores de ambos servidores es susceptible de permitir que se rompa el anonimato. Con todo, se indica que la problemática precitada se plantea para cualquier autoridad que organiza la votación, incluso en su forma clásica por papel.

Generalmente, la mayoría de los sistemas multiservidor están configurados de forma que los distintos administradores directamente relacionados o no con las personas interesadas en los resultados de la votación se vigilan unos a otros.

- Secreto del resultado hasta el final del escrutinio:

Incluso si las comunicaciones están cifradas a nivel de servidor, si el administrador del servidor de recuento de votos no es honesto, éste puede conocer los resultados antes del cierre del escrutinio. Es necesario por tanto proceder a un cifrado a nivel de la aplicación de recuento de votos, con claves de cifrado que no se revelan sino al final de la votación.

- Seguridad:

Si las máquinas de los servidores no están suficientemente protegidas, un intruso malicioso puede introducirse y provocar daños.

- Sinceridad:

El riesgo de inundación de una urna electrónica es considerable. La potencia de los soportes informáticos físicos y lógicos es tal que el descubrimiento o la revelación de una brecha permite a cualquiera que lo sepa utilizar esta última a muy amplia escala.

El uso de certificados y de firmas electrónicas permite protegerse del riesgo precitado.

Ya se han propuesto algunos sistemas que dan respuesta a las restricciones precitadas. Éste es particularmente el caso de las infraestructuras ICP, que soportan la utilización de criptografía de clave pública, gracias a sistemas generadores de pares de claves pública-privada, con el fin de permitir una protección del acceso a la clave privada, secreta por definición, que sólo puede ser utilizada por el individuo, elector votante, cuya identidad se ha asociado con esta clave privada.

Instalar una infraestructura ICP a gran escala -una votación puede contar con más de treinta millones de electores- es aún hoy difícil, y proporcionar un número suficiente de cabinas protegidas implica costes financieros elevados.

Los sistemas de votación electrónica por Internet tienen por objeto simplificar la organización del escrutinio y disminuir los costes, por lo que no pueden recurrir fácilmente a tales estructuras.

Cuando, por el contrario, estos mismos organizadores eligen una infraestructura considerablemente protegida, el coste y la complejidad de implantación son mucho menos dados a experimentaciones y a una subsiguiente generalización de uso.

Sólo una voluntad política fuerte, una asociación con otros desarrollos estructurantes, tales como el carné de identidad electrónico, y una estrecha colaboración entre varios agentes implicados en el país considerado, permitiendo una reutilización de estas estructuras en circunstancias parecidas a las de una votación, pero no necesariamente vinculados a este tipo de acontecimiento, permitirían contemplar un despliegue de tal estructura.

Si, en una situación de este tipo, estos organizadores recurren a un sistema de votación electrónica menos seguro, el riesgo de pérdida de confianza por parte de los electores es enorme, lo que de ningún modo puede aceptarse, debido al riesgo de descrédito frente a estos organizadores, incluso de la clase política, por aceptar tales sistemas.

Por otro lado, se describe un sistema de votación electrónica en el documento “A practical secret voting scheme for large scale elections” de Fujiok A y col., Advances in cryptology - Proceedings of the auscrypt workshop on the theory and application of cryptographic techniques, 1992, páginas 244-251, XP000572977.

La presente invención tiene por objeto solventar el conjunto de los inconvenientes y limitaciones de los actuales procedimientos y sistemas de votación electrónica, que obligan particularmente a los electores a fiarse de los administradores técnicos de la votación.

Particularmente, la presente invención tiene por objeto un procedimiento y un sistema de votación electrónica en red cuya estructura esté en disposición de permitir que se garantice un reparto de las responsabilidades entre varios agentes administradores, quienes, salvo en caso de acuerdo ilícito de estos últimos, no podrán atentar contra la integridad del escrutinio, sin que sean desveladas las correspondientes tentativas de fraude.

Además, la presente invención tiene por objeto proporcionar un procedimiento y un sistema de votación sencillos, que no precisan de la utilización de un complicado sistema de autenticación, pero que no obstante presenta un alto grado de seguridad.

La presente invención tiene asimismo por objeto proporcionar un procedimiento y un sistema que permiten protegerse de cualquier intento de descrédito del procedimiento de votación, mediante la supresión de cualquier posibilidad de tentativas consistentes en depositar, baja una determinada identidad, una papeleta de votación electrónica firmada con otra identidad, con objeto de crear divergencias entre la lista de electores que realmente han participado en la votación y la lista de electores que han firmado un registro de control.

Finalmente, la presente invención tiene por objeto la puesta en práctica de un procedimiento y de un sistema de votación electrónica que permiten introducir un procedimiento de derecho a firmar el registro electoral electrónico del elector que ha participado en la votación y, por tanto, ha votado realmente.

La invención tiene por objeto un procedimiento de votación electrónica según la reivindicación 1.

La invención tiene asimismo por objetos un sistema de votación electrónica según la reivindicación 9, un servidor administrador según la reivindicación 10 y un servidor de recuento de votos según la reivindicación 18.

En las reivindicaciones dependientes se enuncian otras características de la invención.

El procedimiento y el sistema de votación electrónica en red que son objeto de la presente invención encuentran aplicación en la organización de votaciones políticas, de sondeos políticos públicos o privados ante particulares, en condiciones óptimas de autenticidad y de confidencialidad, con costes de desarrollo y/o de despliegue sensiblemente reducidos.

Se entenderán mejor los mismos con la lectura de la descripción y con la observación de los dibujos, en los que:

la figura 1a representa, a título ilustrativo, un organigrama de las etapas esenciales de puesta en práctica del procedimiento de votación electrónica en red objeto de la presente invención;

las figuras 1b y 1c representan, a título ilustrativo, un organigrama detallado de puesta en práctica de etapas específicas del procedimiento objeto de la presente invención, tal como se representa en la figura 1a;

la figura 2 representa, a título ilustrativo, un esquema general de una arquitectura de un sistema de votación electrónica en red conforme al objeto de la presente invención;

la figura 3 representa, a título ilustrativo, una arquitectura, en forma de diagrama de bloques, según una alternativa preferente, de un sistema de votación electrónica en red conforme al objeto de la presente invención;

la figura 4a representa, a título ilustrativo, un detalle de puesta en práctica de una sesión de votación electrónica por un usuario, utilizando un sistema de votación electrónica conforme al objeto de la presente invención, tal como se representa en la figura 3;

la figura 4b representa, a título ilustrativo, un detalle de puesta en práctica de una sucesión de etapas o de un protocolo mediante la arquitectura de un sistema de votación electrónica tal como se representa en la figura 3.

Ahora se dará, en relación con la figura 1a y las figuras siguientes, una descripción más detallada del procedimiento de votación electrónica en red de alta seguridad objeto de la presente invención.

El procedimiento de votación electrónica en red objeto de la presente invención se pone en práctica entre un elector usuario Eu de un terminal elector Te conectado en red al menos a un servidor administrador SA y a un servidor de recuento de votos SCV.

Con carácter general, se indica que el terminal elector Te puede estar constituido por un terminal de tipo variado, tal como un ordenador personal conectado a través de Internet, una cabina específica instalada en un colegio electoral y conectada a Internet o también por una cabina en un lugar público cualquiera también conectada a Internet y, particularmente, al servidor administrador SA y al servidor de recuento de votos SCV precitados, del modo que se describirá posteriormente en la descripción.

De acuerdo con un aspecto destacable del procedimiento objeto de la presente invención, éste consiste al menos en una etapa A de calcular y transmitir, del servidor administrador SA al elector usuario Eu y al terminal elector Te, un certificado de autenticación CA y respectivamente una contraseña de un solo uso exclusiva de este elector, contraseña de un solo uso indicada como UPWe.

Las operaciones de cálculo y de transmisión de la etapa A quedan simbolizadas por la relación

$$SA \xrightarrow{[CA,\,UPWe]} Te$$

Con carácter general, se indica que la simbolización de los datos transmitidos en los mensajes representados entre corchetes, tal como se representa en la relación anterior, corresponde a una transmisión de estos datos de forma cifrada con un grado de cifrado que se aclarará posteriormente en la descripción.

Por supuesto, se entiende que la contraseña de un solo uso especialmente UPWe se transmite al elector usuario Eu y/o al terminal elector Te en forma cifrada, con el fin de evitar cualquier riesgo de intrusión y de uso fraudulento de esta última por terceros.

Las condiciones de cálculo y de transmisión respectivamente del certificado de autenticación CA y de la contraseña de un solo uso UPWe se aclararán posteriormente en la descripción.

La etapa A precitada viene seguida entonces de una etapa B_0 consistente en transmitir, del terminal elector Te al terminal de recuento de votos SCV, una papeleta de votación electrónica, indicada EB, elegida por el elector usuario Eu, acompañada de la contraseña de un solo uso UPWe exclusiva de este elector.

La etapa B_0 de la figura 1a representa, a título puramente ilustrativo, la transmisión por parte del terminal elector Te de la papeleta de votación electrónica EB y de la contraseña de un solo uso UPWe y la recepción de estas últimas según la forma simbólica

$$Te \xrightarrow{[EB,\,UPWe]} SCV$$

La operación de transmisión B_0 precitada y de recepción por el servidor de recuento de votos SCV viene seguida entonces de una etapa consistente, a nivel del servidor de recuento de votos, en comprobar el valor verdadero del valor de la contraseña de un solo uso exclusiva UPWe en una etapa B_1.

Ante una respuesta positiva de la etapa de comprobación B_1, el procedimiento objeto de la invención consiste en validar la papeleta de votación electrónica EB y la votación electrónica del elector usuario Eu, con el fin de computar esta papeleta de votación electrónica en función del valor facial de esta última.

De forma clásica, el valor facial de la papeleta de votación electrónica puede estar constituido por un valor facial correspondiente a una papeleta válida dependiente de la elección del elector usuario, una papeleta en blanco o una papeleta nula, por ejemplo, según la excepción clásica, propio del contenido de las papeletas.

Con referencia a la figura 1a, se indica que, ante una respuesta negativa a la prueba de comprobación B_1, puede preverse una etapa B_2 de retorno para reinicializar el procedimiento en la etapa A y, en su caso, tratar de reinicializar el procedimiento para el mismo terminal electrónico Te y el mismo elector usuario Eu, aunque por un número limitado de intentos.

Por el contrario, ante una respuesta positiva a las pruebas de comprobación B_1, la validación de la papeleta de votación electrónica EB y de la votación electrónica se representa en la etapa B_3, conllevando esta operación el cómputo de la papeleta electrónica emitida, con arreglo al valor facial de esta última.

La etapa B_3 de validación de la papeleta electrónica y de la votación electrónica puede ir seguida entonces de una etapa B_4, consistente en transmitir, del servidor de recuento de votos SCV al terminal elector Te, un acuse de recibo ACW y un documento de registro electoral electrónico, indicado DVR.

En la figura 1a, la etapa de transmisión del acuse de recibo y del documento de registro electoral viene indicada de forma simbólica

$$SCV \xrightarrow{[ACW, DVR]} TE$$

La etapa B_4 puede ir entonces seguida ventajosamente de una etapa C consistente en calcular y transmitir, del terminal elector Te al servidor administrador SA, un documento de registro electoral firmado electrónicamente por el usuario, indicándose este documento como SDVR.

La operación de transmisión del terminal elector Te al servidor administrador SA se indica simbólicamente

$$Te \xrightarrow{[SDVR]} SA$$

Como consecuencia de la recepción del documento de registro electoral firmado electrónicamente SDVR, el servidor administrador SA procede entonces a una etapa de comprobación D_0 del valor verdadero del documento de registro electoral firmado SDVR. Esta operación se indica simbólicamente:

$$v(\text{SDVR}) = \text{verdadero}$$

Ante una respuesta negativa a la prueba D_0, se puede llevar a cabo una etapa de retorno D_2 a la etapa A, con el fin de realizar uno o varios nuevos intentos de votación concedidos al elector usuario Eu, aunque con número limitado.

Por el contrario, ante una respuesta positiva a la prueba D_0 de comprobación del valor verdadero del documento de registro electoral firmado, el servidor administrador SA procede al cierre de la operación de votación del elector usuario Eu del terminal elector Te.

El procedimiento de votación electrónica en red de alta seguridad objeto de la presente invención se revela especialmente destacable por cuanto la contraseña de un solo uso UPWe se puede calcular como un valor único para cada elector usuario Eu.

Tras el cierre de la votación de Eu o tras el retorno a las etapas B_2 y D_2 en la etapa A en el servidor administrador, este último procede, por ejemplo, a la cancelación de la contraseña de un solo uso y a la destrucción de esta última.

De acuerdo con un aspecto particularmente ventajoso del procedimiento objeto de la invención, tal como se ilustra en la figura 1b, las operaciones consistentes en calcular y transmitir, del servidor administrador SA al terminal elector Te y al elector usuario Eu, respectivamente un certificado de autenticación CA y una contraseña de un solo uso UPWe vinculada a este elector son preferentemente no simultáneas.

El carácter no simultáneo de las dos operaciones precitadas viene representado en la figura 1b por las relaciones simbólicas sucesivas:

$$SA \xrightarrow{[CA]} Te$$
$$SA \xrightarrow{[UPWe]} Eu$$

El carácter no simultáneo de las operaciones precitadas de transmisión permite reducir el riesgo de interceptación de un mensaje único y particularmente el riesgo de asociación de la contraseña de un solo uso UPWe con el certificado de autenticación CA transmitido no simultáneamente.

Naturalmente, la etapa A de la figura 1a se puede ejecutar de forma convencional, ejecutándose la etapa precitada, que consiste en calcular y en transmitir del servidor administrador SA al terminal elector Te el certificado de autenticación CA y después la contraseña de un solo uso UPWe, a petición de autorización de participar en la votación del elector usuario Eu, desde el terminal elector Te.

La petición de autorización precitada consta al menos de datos de identificación personal del elector Eu y el certificado de autenticación se calcula y transmite previa comprobación del valor verdadero de los datos de identificación personal por el servidor administrador.

Las operaciones correspondientes están representadas en la figura 1c, en la que la etapa A_0 indica y representa de forma simbólica la transmisión de la petición según la relación simbólica:

$$Te \xrightarrow{\text{Re } EuTe[IDEu]} SA$$

El servidor administrador SA pone entonces en marcha una etapa de prueba A_1 de comprobación del valor verdadero de los datos de identificación de usuario IDEu, naturalmente después de descifrados estos últimos.

Ante una respuesta negativa a la etapa de prueba A_1, se puede prever un retorno A_2 a la etapa A_0, siendo esta operación comparable a las operaciones de retorno B_2 y D_2 mostradas en la figura 1a.

Por el contrario, ante una respuesta positiva a la etapa de prueba A_1, al comprobarse el valor verdadero de los datos de identificación personal IDEu del elector usuario, la operación de cálculo del certificado de autenticación CA y después de cálculo de la contraseña de un solo uso UPWe se pueden ejecutar entonces en la etapa A_3.

Tal como se ha mostrado en la figura 1c, las operaciones consistentes en calcular y transmitir la contraseña de un solo uso UPWe exclusiva del elector Eu y la operación de transmisión de esta última se ejecutan condicionalmente respecto de la verificación del valor verdadero de los datos de identificación personal IDEu del elector usuario Eu por parte del servidor administrador SA.

Además, esta operación se lleva a cabo preferentemente a raíz de la transmisión del certificado de autenticación CA con arreglo al modo de puesta en práctica mostrado en la etapa A', forma de realización alternativa de la etapa A en la figura 1b.

En la figura 2, se muestra una representación esquemática de una arquitectura que incorpora diferentes tipos de terminales electores Te_1, Te_2, Te_3 interconectados a través de Internet a un servidor administrador SA y a un servidor de recuento de votos SCV.

En la figura 2 precitada, las etapas del procedimiento de votación electrónica conforme al objeto de la presente invención están representadas en su puesta en práctica a nivel de cada uno de los agentes precitados.

A título de ejemplo no limitativo, se indica que el terminal elector Te_1 puede estar constituido por una cabina dedicada como colegio electoral, el terminal elector Te_2 puede estar constituido por un ordenador personal instalado en el domicilio de un elector usuario particular y el terminal elector Te_3 puede estar constituido por una cabina instalada en un lugar público no dedicada específicamente a una votación.

Las operaciones se dirigen de acuerdo con el procedimiento objeto de la invención, a partir de ambos servidores, servidor administrador SA y servidor de recuento de votos SCV, tal como se ha mencionado y descrito anteriormente en la descripción.

El procedimiento y el sistema de votación electrónica en red de alta seguridad objeto de la presente invención permiten obtener, gracias a la utilización de una contraseña de un solo uso, un gran nivel de seguridad en lo referente a la ejecución de la votación, con total integridad y en ausencia de riesgo de fraude por parte de terceros.

Sin embargo, con el fin de protegerse de cualquier riesgo de manipulación y/o de fraude susceptible de ser ejecutado por una entidad responsable de la organización de la votación, el sistema objeto de la presente invención y el procedimiento correspondiente se pueden ejecutar, de forma especialmente ventajosa, a partir de un servidor dedicado que tiene al menos por función el calcular y transmitir la contraseña de un solo uso, siendo dicho servidor dedicado independiente del servidor administrador propiamente dicho y del servidor de recuento de votos anteriormente descrito en relación con la figura 2.

Naturalmente, el servidor dedicado calcula una contraseña de un solo y único uso UPWe asociada al elector usuario.

En la figura 3, se representa una arquitectura correspondiente de un sistema de votación electrónica en red de alta seguridad conforme al objeto de la presente invención, que incorpora particularmente un servidor dedicado SD independiente del servidor administrador y del servidor de recuento de votos.

Con carácter general, se indica que, para poner en práctica la arquitectura mostrada en la figura 3, en la que el cálculo y la transmisión de la contraseña de un solo uso se realizan a partir de un servidor dedicado, se puede considerar de alguna manera el desdoblamiento del servidor administrador SA mostrado en la figura 2 en un primer servidor administrador SA_1 y un segundo servidor administrador SA_2 que desempeña la función del servidor dedicado SD, único autorizado para calcular y transmitir y procesar la contraseña de un solo uso UPWe.

Se entiende, particularmente, que al primer servidor administrador SA_1 y al segundo servidor SA_2 que desempeña la función de servidor dedicado se les puede asignar entonces tareas respectivas perfectamente definidas, que se aclararán a continuación.

Tal como se representa en la figura 3, el servidor dedicado SA_2(SD), segundo servidor administrador, puede poner en práctica ventajosamente las etapas A_1, A_2, A_3 mostradas en la figura 1a y 1c con, además del cálculo, la transmisión y el procesamiento de la contraseña de un solo uso UPWe que es de exclusiva competencia de este servidor.

El primer servidor administrador SA_1 se puede dedicar entonces a la administración propiamente dicha de las listas electorales y a la gestión del cierre de la votación, por ejemplo, para ejecutar las operaciones D_0, D_1 y D_2 mostradas en la figura 1a.

De acuerdo con un aspecto especialmente destacable del sistema de votación electrónica en red de alta seguridad objeto de la invención, se indica que cada uno de los intercambios de mensajes entre cada servidor administrador, primer servidor administrador SA_1, segundo servidor administrador SA_2 que desempeña la función de servidor dedicado SD y el servidor de recuento de votos SCV, se realiza a raíz de un protocolo de autenticación superada con un grado de seguridad muy alto, representado mediante una flecha de línea llena entre estas entidades.

El protocolo de autenticación utilizado puede corresponder, a título de ejemplo no limitativo, a un protocolo de autenticación sin revelación de conocimiento, estando cifrados los diferentes mensajes transmitidos naturalmente en forma cifrada entre primer, segundo servidor administrador que desempeña la función de servidor dedicado y servidor de recuento de votos SCV con un grado de seguridad muy alto, pero transmitidos a raíz de la operación de autenticación superada anteriormente mencionada.

Finalmente, las transacciones o intercambios de mensajes entre el terminal elector Te, o cada terminal electrónico Te_1 a Te_3 mostrado en la figura 2, y el primer servidor administrador SA_1, el segundo servidor administrador SA_2 y el servidor de recuento de votos SCV se representan mediante flechas de líneas de rayas y puntos que ilustran transacciones mediante mensajes cifrados con un grado de cifrado de alta seguridad.

A continuación se da la sucesión de las etapas puestas en práctica por el procedimiento de votación electrónica en red objeto de la invención y mostrada en las figuras 1a a 1c, según las referencias temporales y espaciales entre los diferentes agentes, terminal elector Te, primer servidor administrador SA_1, segundo servidor administrador SA_2 que desempeña la función de servidor dedicado SD y servidor de recuento de votos SCV.

T1: ReEu[IDEu]

T2: Z_0[CA]

T3: Z_1[UPWe]

T4: Z_2[UPWe]

T5: [CA, UPWe]

T6: [CA, UPWe]

T7: [AREu]

T8: [EB,UPWe]

T9: [ACW,DVR]

T10: [SDVR]

Se recuerda que, en la tabla anterior, todas las transacciones Z_0 a Z_2 entre el servidor administrador y el servidor de recuento de votos indican la transmisión de un mensaje cifrado, habiendo cumplido la transacción entre estos elementos un protocolo de autenticación fuerte superada, tal como se ha mencionado anteriormente en la descripción.

Ello permite particularmente asegurar la independencia y la integridad de las transacciones entre los diferentes agentes sometidos totalmente o en parte a la autoridad de un administrador del escrutinio.

Finalmente, en cuanto a las operaciones de transmisión del servidor administrador y particularmente del segundo servidor administrador SA_2 que desempeña la función de servidor SD al elector Eu y al terminal elector Te, del certificado de autenticación y de la contraseña de un solo uso UPWe a este elector, se indica que las operaciones se pueden realizar, de forma especialmente ventajosa, por vía de canales de transmisión distintos.

En cuanto a la transmisión del certificado de autenticación CA, tal como se muestra particularmente en la etapa A' de la figura 1b, se indica que la transmisión precitada se puede realizar a través de la red Internet a raíz de la transmisión de la petición de autorización de votación en la etapa T_1 mostrada en la tabla, del terminal electrónico Te hacia el servidor dedicado, segundo servidor administrador SA_2.

La transmisión de la contraseña de un solo uso UPWe, por el contrario, se puede realizar por un canal de transmisión totalmente distinto tal como, por ejemplo, un servicio de mensajería, un correo electrónico o, en su caso, un correo transmitido nominalmente al elector usuario Eu previamente a la fecha del escrutinio.

Particularmente, se indica que se puede considerar ventajosamente la transmisión de la contraseña de un solo uso por vía de un mensaje corto, designado SMS, ya que el elector usuario EU dispone en tal caso, por ejemplo, de un teléfono móvil, cuyo acceso está protegido por el código de identificación del aparato del que el elector usuario es único poseedor.

Cuando la transmisión de la contraseña de un solo uso UPWe al terminal usuario Te o al elector usuario Eu se ha realizado, T5: [CA, UPWe], el elector usuario Eu se conecta, el día de la votación, al segundo servidor administrador, SA_2(SD), servidor dedicado, T6: [CA, UPWe] para presentar su certificado de autenticación CA y su contraseña de un solo uso UPWe. El segundo servidor administrador, SA_2(SD), único habilitado para procesar la contraseña de un solo uso UPWe, procede, tras la comprobación del par CA, UPWe, al cálculo de una referencia anónima para el elector usuario, AREu, que se transmite T7: [AREu] al terminal elector Te.

La referencia anónima para el elector usuario AREu puede consistir en un valor numérico obtenido a partir de una función hash (función para resumir o identificar probabilísticamente un gran conjunto de información), tal como se describirá posteriormente en la descripción.

El terminal usuario Te se conecta a continuación a un servidor de recuento de votos, SCV, y transmite a este último T8: [EB, AREu] su papeleta de votación electrónica EB y la referencia anónima para el elector usuario AREu. El procedimiento se prosigue a raíz de las operaciones de validación de la papeleta de votación y de la votación mediante las operaciones de transmisión de acuse de recibo y de documento de registro electoral T9: [ACW,DVR] y, después, de transmisión del documento de registro electoral firmado SDVR mediante la transacción T10: [SDVR], del terminal elector Te al primer servidor administrador SA_1.

Ahora se dará, en relación con las figuras 4a y 4b, una descripción más detallada del procedimiento de trabajo de una arquitectura de un sistema de votación electrónica en red conforme al objeto de la presente invención, que comprende un servidor dedicado, más particularmente destinado a asegurar el cálculo y la gestión de una contraseña de un solo uso.

En la figura 4a precitada, se indica que se supone que el elector usuario Eu dispone de un terminal de telefonía móvil y de un terminal electrónico Te, tal como, por ejemplo, un ordenador personal conectado a Internet.

El servidor administrador SA_1 desempeña esencialmente la función de servidor de lista electoral, el segundo servidor administrador SA_2 desempeña la función de servidor dedicado SD y el servidor de recuento de votos SCV está interconectado con el primer y con el segundo servidores administradores, tal como se ha mencionado anteriormente en la descripción en relación con la figura 3.

Con preferencia, tal como se muestra en la figura 4a, el sistema de votación electrónica en red objeto de la invención comprende, a nivel de uno de los servidores administradores SA_1 o SA_2, un módulo de cálculo y de transmisión, de ese servidor administrador al elector Eu y al terminal elector Te, de un certificado de autenticación CA y de una contraseña de un solo uso UPWe exclusiva de este elector.

Con referencia a la figura 4a y a la figura 3, se indica que el módulo de cálculo precitado va implantado a nivel del segundo servidor administrador que desempeña la función de servidor dedicado SD, que permite la puesta en práctica de las operaciones A_0, A_1, A_2, A_3 mostradas en la figura 1a e indicadas en la tabla anterior.

El sistema objeto de la invención incorpora, a nivel del servidor de recuento de votos SCV, un módulo de recepción y de procesamiento de un mensaje procedente del terminal elector Te y que contiene al menos la papeleta de votación electrónica EB elegida por este elector y la referencia anónima para el elector usuario AREu que es función de la contraseña de un solo uso UPWe, y exclusiva de este elector. Este módulo de recepción corresponde a la recepción, por parte del servidor de recuento de votos, del mensaje transmitido, en la etapa B_0 de la figura 1a, por el terminal elector Te.

El servidor de recuento de votos SCV incorpora además un módulo de comprobación del valor verdadero de la referencia anónima para el elector usuario AREu y, consiguientemente, de la contraseña de un solo uso exclusiva, recibida.

Este módulo corresponde a la ejecución de la etapa B_1 de la figura 1a, entendiéndose que este módulo ejecuta la ejecución de la comprobación precitada mediante comparación, por ejemplo, de la referencia anónima para el elector usuario AREu o de la contraseña de un solo uso UPWe, transmitida por el segundo servidor administrador que desempeña la función de servidor dedicado SD al servidor de recuento de votos SCV, y de la referencia anónima AREu transmitida anteriormente por el terminal elector Te al servidor de recuento de votos SCV.

El servidor de recuento de votos incorpora asimismo un módulo de validación de la papeleta de votación electrónica EB y de la votación electrónica de este elector, asociado a un módulo de recuento de votos de esta papeleta de votación electrónica, tal como se ha mencionado anteriormente en la descripción, en función del valor facial de esta papeleta de votación electrónica. Los módulos precitados corresponden a la puesta en práctica de la etapa B_3 de la figura 1a y de la figura 3.

Finalmente, el servidor de recuento de votos SCV comprende un módulo de cálculo y de transmisión, al terminal elector Te, de un mensaje de acuse de recibo y de un documento de registro electoral electrónico, operación llevada a cabo en la etapa B_4 de la figura 1a y de la figura 3.

Ahora se dará, en relación con la figura 4a y la figura 4b, un procedimiento de trabajo preferente del protocolo de intercambio de mensajes y transacciones entre los diferentes agentes, primer servidor administrador SA_1, segundo servidor administrador SA_2 que desempeña la función de servidor dedicado SD, servidor de recuento de votos SCV y terminal elector Te.

Con carácter general, con referencia a la figura 4a, se indica que el servidor administrador, particularmente el segundo servidor administrador SA_2 que desempeña la función de servidor dedicado, comprende al menos un módulo de memorización de datos representativo de la lista de las votaciones, de la lista de los candidatos a esas votaciones, vinculada a una o varias circunscripciones.

Esta operación se lleva a cabo 1 bajo la autoridad de los organizadores del escrutinio, designados Administradores, que pueden actualizar el servidor dedicado SA_2.

Este último comprende un módulo de cálculo, ejecutado en 2, de un conjunto de miniaplicaciones en forma de listas, miniaplicaciones MA conocidas como “applets”. Una miniaplicación está asociada con una circunscripción y contiene la lista de los candidatos y de las claves de cifrado de las papeletas de votación electrónica.

Particularmente se entiende que, naturalmente, las papeletas de votación electrónica EB, representadas entre corchetes en el momento de la transmisión están cifradas por medio de las claves de cifrado precitadas con un alto grado de seguridad. Se entiende por el grado de seguridad un cifrado potente por medio de claves de cifrado con claves asimétricas, por ejemplo según el algoritmo RSA u otro.

El segundo servidor administrador SA_2 que desempeña la función de servidor dedicado comprende además un módulo de transmisión de las miniaplicaciones, que contienen la lista de los candidatos y de las claves de cifrado, al primer servidor administrador SA_1.

El primer servidor administrador SA_1 recibe 3 la lista de las miniaplicaciones, procede a la compilación de estas últimas, procede a su firma y publica la lista de los candidatos con fines de control.

Con este objeto, el primer servidor administrador SA_1 comprende naturalmente un módulo de memorización de la lista de las miniaplicaciones, un módulo de compilación de las miniaplicaciones y de firma de las miniaplicaciones compiladas y un módulo de extracción y de publicación de la lista de los candidatos para cada circunscripción y cada miniaplicación, así como un módulo de transmisión de las miniaplicaciones firmadas al segundo servidor administrador SA_2, servidor dedicado SD y al terminal elector de cada elector concernido.

Se entiende particularmente que el primer servidor administrador SA_1 reenvía 4 la lista de las aplicaciones de las miniaplicaciones firmadas al segundo servidor administrador, servidor dedicado SD.

El servidor dedicado precitado procede entonces al control 5 de la integridad de las miniaplicaciones firmadas mediante comprobación de firma y, previa autorización transmitida por el segundo servidor administrador, servidor dedicado SD, al primer servidor administrador, este último está entonces en disposición de transmitir a cada elector concernido las miniaplicaciones originales comprobadas que no se han podido sustituir por miniaplicaciones modificadas.

Por lo que se refiere a la gestión de las contraseñas de un solo uso UPWe, se indica que el segundo servidor administrador SA_2, servidor dedicado SD, genera 6 el conjunto precitado de las contraseñas de un solo uso.

El servidor dedicado SD transmite 7 entonces la contraseña de un solo uso UPWe al elector usuario Eu concernido, tal como se ha descrito anteriormente en la descripción en relación con la figura 3, por ejemplo.

En cuanto a la gestión de las claves de cifrado anteriormente mencionada, se indica que el primer servidor administrador SA_1 recibe, de las autoridades responsables del sistema, es decir, de los administradores que garantizan la gestión del conjunto del sistema, la lista de las claves de cifrado público que permiten la realización de los mensajes cifrados transmitidos, de nuevo designados "mix-net", y el cifrado destinado a impedir la divulgación de las papeletas electrónicas EB antes del final del escrutinio. Las claves de cifrado precitadas se transmiten con cada miniaplicación MA a cada uno de los terminales electores Te concernidos.

Finalmente, la gestión de las claves de autenticación se regula para la puesta en práctica de los certificados de autenticación respectivamente por el primer servidor administrador SA_1 y el segundo servidor administrador SA_2 que desempeña la función de servidor dedicado SD.

Los dos servidores precitados generan respectivamente una lista de las claves de autenticación designada LKA para las claves de autenticación generadas por el servidor dedicado SD y LKB generadas por el primer servidor administrador SA_1.

A cada elector usuario Eu se le atribuye respectivamente un par de claves de autenticación KA generadas por el servidor dedicado SD, segundo servidor administrador, y KB generadas por el primer servidor administrador SA_1.

Cada uno de los servidores SA_1 y SA_2, servidor dedicado SD, genera respectivamente una lista de las claves de autenticación LKB y LKA que ha generado.

El primer servidor administrador SA_1 que ha generado la lista de las claves de autenticación LKB transmite 9, al servidor dedicado SD, pares de valores formados por la identidad del elector, o un código de identidad vinculado a este último, y una función hash de la clave de autenticación KB con él asociada.

El servidor dedicado SD calcula la función hash de las claves de la lista de claves LKA y empareja la función hash HKB de las claves de autenticación recibida KB con la función hash de la clave de autenticación KA correspondiente.

A continuación procede a la transmisión 10 únicamente de los pares de los valores de función hash HKA, HKB al primer servidor administrador SA_1 en ausencia de asociación alguna con el código de identidad del elector usuario Eu.

En cuanto a la gestión de los certificados de autenticación, esta última se realización según una arquitectura ICP, tal como se ha mencionado anteriormente en la descripción.

Con este objeto, el primer servidor administrador SA_1 genera 11 una lista de certificados indispensables para no dejar participar en la votación más que a los electores usuarios Eu habilitados.

El primer servidor administrador SA_1 genera y asegura la gestión de una lista de revocaciones de los certificados precitados.

Se entiende particularmente que, a raíz de la transacción T_2 mostrada por ejemplo en la figura 3, en la que el primer servidor administrador ha recibido el certificado de autenticación CA, el primer servidor administrador precitado elabora una lista que le permite no dejar participar en la votación más que a los electores habilitados.

El primer servidor administrador SA_1 transmite a continuación 12, a cada elector, su certificado de autenticación según la transacción T_5 mostrada en la figura 3.

El elector usuario Eu está entonces capacitado para instalar el certificado de autenticación CA en su terminal elector Te.

Se aclaran a continuación, en relación con la figura 4b, las transacciones realizadas por el elector usuario y por el conjunto del sistema el día de la votación.

El día de la votación, el elector usuario Eu se conecta 13 al servidor dedicado SA_2 (SD). Transmite su contraseña de un solo uso UPWe y la información que le permite autentificarse. El segundo servidor administrador SA_2 (SD) consulta una base de datos que le da la clave de autenticación KB que se ha asociado con este elector usuario.

En caso de tener lugar dos votaciones el mismo día, estarán disponibles para el elector usuario Eu varias claves de autenticación KB mediante diversificación.

En este supuesto, el servidor dedicado SA_2 (SD) está entonces en condiciones de consultar varios servidores de recuento de votos (SCV) correspondientes a cada elección.

Ante un error del intento de conexión precitada indicado C_{13}, a causa de un error de autenticación, al no haberse podido desarrollar con éxito el procedimiento de autenticación del elector usuario Eu a partir de su certificado de autenticación, se activa un procedimiento de control y entonces se sigue la traza del evento con el fin de poner en práctica, por ejemplo, procedimientos de seguridad antifraude.

Esta operación puede corresponder a una operación lanzada al término del retorno A_2 de la figura 1c ante una respuesta negativa a la identificación del elector usuario.

En ausencia de error de autenticación, el segundo servidor administrador dedicado SA_2 (SD) transmite 14 la clave de autenticación KA al servidor de recuento de votos SCV. El servidor de recuento de votos SCV realiza entonces un control C_{14} en su base de datos para comprobar que esta clave KA no ha sido ya utilizada. En caso de haber sido utilizada esta clave KA, tal como se muestra en la figura 4b, se advierte al elector, mediante el servidor de recuento de votos SCV por vía del servidor dedicado SA_2 (SD), que ya no tiene derecho a participar en la votación para este escrutinio.

Particularmente, ante un error de autenticación, es decir, cuando la clave KA de autenticación ya ha sido utilizada, se sigue la traza C_{14} del evento, suponiéndose que el elector usuario Eu ha tratado de votar dos veces.

El controlador u organismo de control se pone en contacto con el primer servidor administrador SA_1 para comprobar la presencia efectiva de la firma.

En ausencia de error, el servidor de recuento de votos SCV transmite 15 al segundo servidor administrador dedicado SA_2 (SD) la autorización para votar. La clave de autenticación KA se conserva todavía en las claves válidas del servidor de recuento de votos SCV.

El servidor dedicado SA_2(SD) transmite 16 al elector usuario Eu, es decir, de hecho al terminal elector Eu, una miniaplicación de votación MA así como la clave de autenticación KA.

Se recuerda que la miniaplicación de votación y la clave de autenticación KA se han producido en el momento de los preparativos de la votación. Tras la recepción de la miniaplicación MA y de la clave de autenticación KA, el terminal elector Te ejecuta una conexión 17 con el primer servidor administrador SA_1. El navegador del terminal elector Te propone entonces una prueba de identificación a la que el certificado de autenticación CA previamente distribuido e instalado en ese terminal permite responder gracias al sistema PKI y de certificados generados.

El elector elige su candidato o su lista de candidatos mediante la papeleta electrónica EB, y el terminal elector Te procede entonces a un procedimiento de firma ciega por vía de la miniaplicación MA. Esta última oculta la papeleta electrónica EB previamente cifrada mediante un procedimiento de tipo esteganografía y transmite 17 el conjunto al primer servidor administrador SA_1.

En caso de intento de conexión infructuoso, al primer servidor administrador SA_1, se cataloga y se sigue la traza de estos intentos infructuosos C17 y se sigue entonces la traza de un error de autenticación a nivel del primer servidor administrador SA_1 y se transmite al organismo de control o controlador. Este último puede decidir dejar de procesar las solicitudes de votación procedentes de determinadas fuentes, es decir, de ciertos terminales Te, durante un tiempo determinado.

En ausencia de error de autenticación, el elector usuario firma el registro electoral por medio de su clave privada y transmite el registro firmado en 18 al primer servidor administrador SA_1.

El primer servidor administrador SA_1 envía 19 la firma ciega correspondiente a la papeleta ocultada y la clave de autenticación KB al terminal Te del elector usuario Eu. La miniaplicación MA descubre entonces la papeleta y permite obtener la firma válida de la papeleta electrónica EB descubierta pero todavía cifrada. La clave de autenticación KB en posesión del elector usuario y el terminal electrónico Te es la prueba de que efectivamente el registro electoral se ha firmado.

La miniaplicación MA instalada en el terminal elector Te del elector usuario Eu se conecta 20 al servidor de recuento de votos SCV y transmite el conjunto formado por la papeleta electrónica EB cifrada, la firma ciega, la clave de autenticación KA y la clave de autenticación KB.

El servidor de control de votos SCV procede entonces a un control C_{20} de la firma, que tiene que ser la del primer servidor administrador SA_1 y de la clave de autenticación KB que tiene que ser válida.

El criterio de validez consiste entonces en el hecho de que el par de función hash de las claves de autenticación KA y KB, es decir, los pares HKA y HKB, tendrán que formar parte de los pares no utilizados y conocidos.

El servidor de recuento de votos SCV almacena entonces la papeleta electrónica EB cifrada y la firma ciega en una base de datos, en espera del escrutinio. Éste almacena en otra base de datos el par de claves de autenticación KA, KB como prueba de que ha recibido el original de uno de los pares de claves de autenticación autorizadas.

En caso de fallo de no comprobación en la cadena de control ejecutada por el servidor de control de votos SCV anteriormente descrita, el servidor de control de votos precitado transmite C_{20} una notificación de rechazo de papeleta de votación al organismo controlador, tal como se muestra en la figura 4b.

Por el contrario, cuando se ha ejecutado con éxito el conjunto de los controles por parte del servidor de recuento de votos SCV, este último advierte al elector usuario Eu de que su papeleta es admitida.

Se puede implantar un mecanismo de transmisión anónima.

En la figura 4b y en relación con la figura 4a, se indica que el procedimiento de firma del registro electoral en 18 y 19 se hace posible mediante el procedimiento de autenticación por medio de las claves de autenticación KA y KB, que son generadas por separado respectivamente por el primer servidor administrador SA_1 y el segundo servidor administrador SA_2.

En tales condiciones, el servidor de recuento de votos se revela así como un árbitro que permite comprobar, a raíz de la etapa 20 de transmisión de las claves KA y KB, la integridad de la votación y de la dirección de esta última, independientemente por las tres entidades independientes constituidas por el primer servidor administrador SA_1, el segundo servidor administrador dedicado SA_2(SD) y el servidor de recuento de votos SCV.

REIVINDICACIONES

1. Procedimiento de votación electrónica en red de alta seguridad, para un elector usuario de un terminal elector conectado en red al menos a un servidor administrador (SA_1, SA_2) y a un servidor de recuento de votos (SCV), **caracterizado** por consistir al menos en:

- transmitir, del terminal elector (Te) a dicho servidor administrador, una contraseña de un solo uso (UPWe) dedicada a este elector,

- transmitir, de dicho terminal elector (Te) a dicho servidor de recuento de votos (SCV), una papeleta de votación electrónica (EB) elegida por este elector y una referencia anónima para este elector usuario; y, previa comprobación, respecto al valor verdadero, de dicha referencia anónima para el elector usuario,

- validar la papeleta de votación electrónica y la votación electrónica de este elector y computar esta papeleta de votación electrónica en función del valor facial de esta última;

- transmitir, de dicho servidor de recuento de votos a dicho terminal elector, un acuse de recibo;

- calcular y transmitir, del terminal elector a dicho servidor administrador, un documento de registro electoral firmado electrónicamente, procediendo dicho servidor administrador, previa comprobación, respecto al valor verdadero, del documento de registro electoral firmado, al cierre de la operación de votación del elector usuario de este terminal elector.

2. Procedimiento según la reivindicación 1, **caracterizado** porque la referencia anónima es función de la contraseña.

3. Procedimiento según la reivindicación 2, **caracterizado** por comprender una operación consistente en transmitir, de dicho servidor de recuento de votos a dicho terminal elector, un documento de registro electoral.

4. Procedimiento según la reivindicación 3, **caracterizado** por comprender una operación consistente en calcular y transmitir, del servidor administrador a dicho elector y al terminal elector, un certificado de autenticación, ejecutándose dicha operación a petición de autorización de participar en la votación del elector usuario de dicho terminal elector, incorporando dicha petición de autorización al menos datos de identificación personal de dicho elector, calculándose y transmitiéndose dicho certificado de autenticación previa comprobación, respecto al valor verdadero, de dichos datos de identificación personal por dicho servidor administrador.

5. Procedimiento según la reivindicación 4, **caracterizado** por comprender una operación consistente en calcular y transmitir, de dicho servidor administrador a dicho elector y a dicho terminal elector, una contraseña de un solo uso exclusiva de este elector, ejecutándose las operaciones consistentes en calcular y transmitir una contraseña de un solo exclusiva de este elector condicionalmente respecto a la comprobación, respecto al valor verdadero, de dichos datos de identificación personal por dicho servidor administrador y a raíz de la transmisión de dicho certificado de autenticación.

6. Procedimiento según una de las reivindicaciones 1 a 5, **caracterizado** porque la operación consistente en calcular y en transmitir una contraseña de un solo uso se realiza a partir de un servidor dedicado independiente de dichos servidor administrador y servidor de recuento de votos, calculando dicho servidor dedicado una sola y única contraseña de un solo uso asociada con dicho elector.

7. Procedimiento según la reivindicación 6, **caracterizado** porque los intercambios de mensajes entre el servidor administrador, el servidor de recuento de votos y el servidor dedicado se realizan entre cada uno de ellos a raíz de un protocolo de autenticación superada sin revelación de conocimiento.

8. Procedimiento según una de las reivindicaciones 1 a 7, **caracterizado** porque la transmisión, del servidor administrador a dicho elector y a dicho terminal elector, de un certificado de autenticación y de una contraseña de un solo uso exclusiva de este elector, respectivamente, se realiza por vía de canales de transmisión distintos.

9. Sistema de votación electrónica en red de alta seguridad para un elector usuario de un terminal elector conectado en red al menos a un servidor administrador y a un servidor de recuento de votos, **caracterizado** por incorporar al menos:

- a nivel de dicho servidor administrador,

  ✣ medios de recepción, a partir del terminal elector, de una contraseña de un solo uso exclusiva de este elector; y

- a nivel de dicho servidor de recuento de votos,

  ✣ medios de recepción y de procesamiento de un mensaje procedente de dicho terminal elector y que contiene al menos una papeleta de votación electrónica elegida por este elector y una referencia anónima para el elector usuario;

  ✣ medios de comprobación, respecto al valor verdadero, de dicha referencia anónima recibida;

  ✣ medios de validación de la papeleta de votación electrónica y de la votación electrónica de este elector y medios de recuento de votos de esta papeleta de votación electrónica, en función del valor facial de esta última;

  ✣ medios de cálculo y de transmisión a dicho terminal elector de un mensaje de acuse de recibo.

10. Servidor administrador de votación electrónica en red de alta seguridad, para un elector usuario de un terminal elector, **caracterizado** por incorporar al menos:

- medios de recepción, a partir del terminal elector, de una contraseña de un solo uso exclusiva de este elector;
- medios de recepción, a partir del terminal elector, de un documento de registro electoral firmado electrónicamente; y
- medios para, previa comprobación, respecto al valor verdadero, del documento de registro electoral firmado, cerrar la operación de votación del elector usuario del terminal elector.

11. Servidor según la reivindicación 10, **caracterizado** por incorporar:

- un primer servidor administrador de gestión de las listas electorales, en función de las circunscripciones y de los candidatos al escrutinio;
- un segundo servidor administrador, servidor dedicado independiente de dichos primer servidor administrador y servidor de recuento de votos, calculando dicho servidor dedicado una contraseña de un solo y único uso asociada con dicho elector.

12. Servidor según la reivindicación 11, **caracterizado** porque dicho servidor administrador, respectivamente dicho segundo servidor administrador, servidor dedicado, comprende al menos:

- medios de memorización de datos representativos de la lista de las elecciones, de la lista de los candidatos a estas elecciones, vinculados a una o varias circunscripciones;
- medios de cálculo de un conjunto de miniaplicaciones en forma de lista, asociándose una miniaplicación con una circunscripción y conteniendo la lista de los candidatos y las claves de cifrado de las papeletas de votación electrónica;
- medios de transmisión de dichas miniaplicaciones a dicho primer servidor administrador.

13. Servidor según la reivindicación 12, **caracterizado** porque dicho primer servidor incorpora al menos:

- medios de memorización de la lista de las miniaplicaciones;
- medios de compilación de las miniaplicaciones y de firma de las miniaplicaciones compiladas;
- medios de extracción y de publicación de la lista de los candidatos para cada circunscripción y cada miniaplicación;
- medios de transmisión de las miniaplicaciones firmadas a dicho segundo servidor administrador, servidor dedicado, y al terminal elector de cada elector concernido.

14. Servidor según la reivindicación 10 u 11, **caracterizado** porque dicho servidor administrador y dicho segundo servidor administrador incorporan además respectivamente medios de codificación que permiten proteger, mediante un código, la contraseña de un solo uso calculada y transmitida a dicho elector.

15. Servidor según una de las reivindicaciones 10 a 14, **caracterizado** porque dicho servidor administrador y dicho primer servidor administrador incorporan respectivamente medios de memorización de claves públicas que permiten generar un baraje y un cifrado de los mensajes transmitidos, particularmente de las papeletas de votación electrónica, con el fin de garantizar la confidencialidad de estas últimas, transmitiéndose dichas claves públicas con dichas miniaplicaciones.

16. Servidor según una de las reivindicaciones 11 a 15, **caracterizado** porque dicho primer servidor administrador y dicho segundo servidor administrador, servidor dedicado, incorporan cada uno medios generadores de una lista de claves de autenticación, asignándose a cada elector usuario de un terminal elector un par de claves de autenticación formado por

- una primera clave de autenticación generada por dicho segundo servidor administrador, servidor dedicado; y por
- una segunda clave de autenticación generada por dicho primer servidor administrador;
- generando dicho primer servidor administrador una lista de segundas claves de autenticación y transmitiendo, desde dicho segundo servidor administrador, servidor dedicado, pares de datos formados por un valor de identidad de un elector candidato al voto, y por un valor de indexación mediante hash de la segunda clave de autenticación asociada con este último; y
- operando dicho segundo servidor administrador, servidor dedicado, un emparejamiento del valor de indexación mediante hash de la segunda clave de autenticación con la primera clave de autenticación y calculando un valor de indexación mediante hash de la primera clave de autenticación y transmitiendo un par formado por el valor de indexación mediante hash de la primera y de la segunda clave de autenticación a dicho servidor de recuento de votos.

17. Servidor según una de las reivindicaciones 11 a 16, **caracterizado** porque dicho primer servidor administrador incorpora además:

- medios de cálculo de una lista de certificados de autenticación para no autorizar la participación en la votación más que únicamente a los electores identificados; y
- medios de gestión de una lista de revocación de dichos certificados de autenticación; y
- medios de transmisión, al terminal elector, del certificado de autenticación asociado con el elector candidato identificado, usuario de ese terminal elector.

18. Servidor de recuento de votos de votación electrónica en red de alta seguridad, para un elector usuario de un terminal elector, **caracterizado** por incorporar al menos:

- ✣ medios de recepción y de procesamiento de un mensaje procedente de dicho terminal elector y que contiene al menos una papeleta de votación electrónica elegida por este elector y una referencia anónima para dicho elector usuario;
- ✣ medios de comprobación, respecto al valor verdadero, de dicha referencia anónima recibida;
- ✣ medios de validación de la papeleta de votación electrónica y de la votación electrónica de este elector y medios de recuento de votos de esta papeleta de votación electrónica, en función del valor facial de esta última;
- ✣ medios de cálculo y de transmisión a dicho terminal elector de un mensaje de acuse de recibo.

19. Servidor según la reivindicación 18 ó 10, **caracterizado** porque la referencia anónima para dicho elector usuario es función de una contraseña de un solo uso exclusiva de este elector.

20. Servidor según la reivindicación 18 ó 10, **caracterizado** porque los medios de cálculo y de transmisión de un mensaje de acuse de recibo están configurados para calcular y transmitir un documento de registro electoral electrónico.

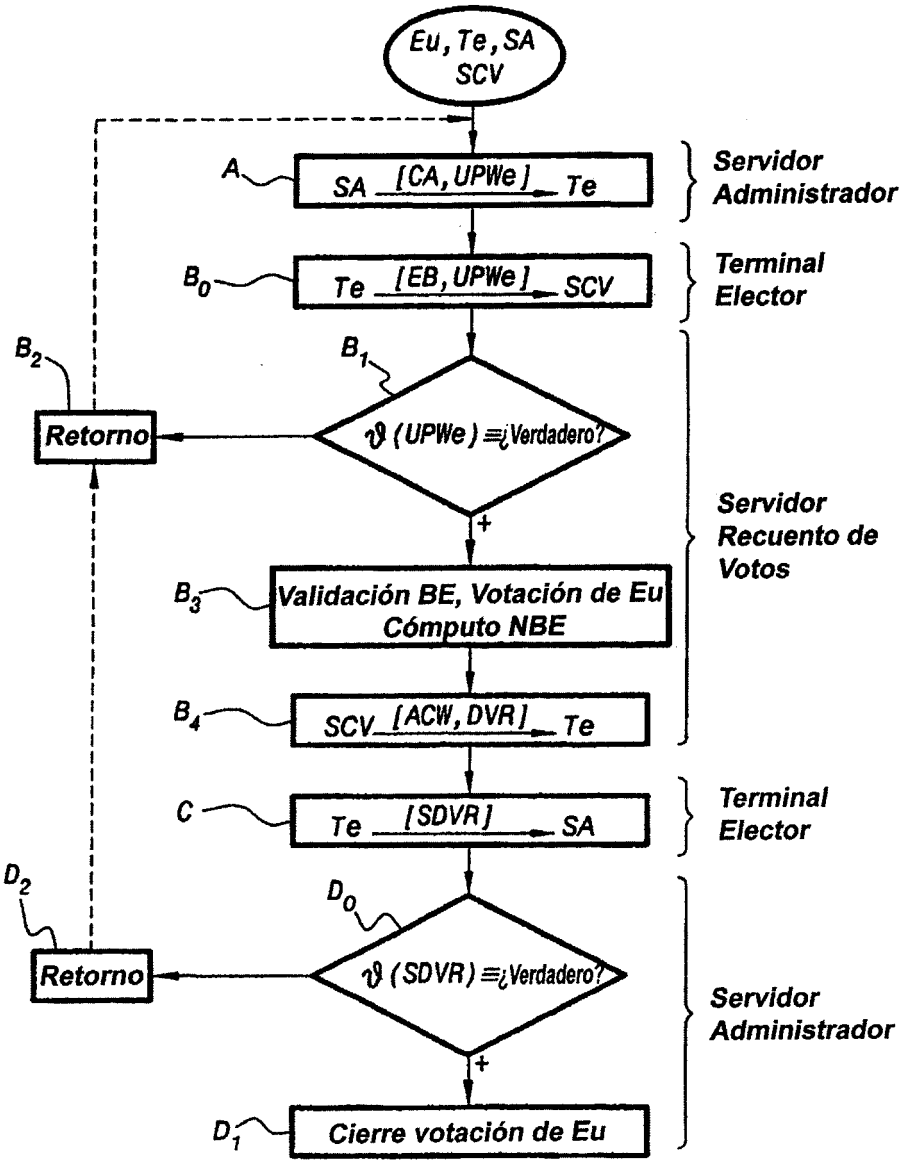
Eu, Te, SA
SCV
A
SA [CA, UPWe] Te
Servidor Administrador
B0
Te [EB, UPWe] SCV
Terminal Elector
B1
B2
Retorno
ϑ (UPWe) ≡¿Verdadero?
+
Servidor Recuento de Votos
B3
Validación BE, Votación de Eu
Cómputo NBE
B4
SCV [ACW, DVR] Te
C
Te [SDVR] SA
Terminal Elector
D2
D0
Retorno
ϑ (SDVR) ≡¿Verdadero?
+
Servidor Administrador
D1
Cierre votación de Eu

FIG.1a

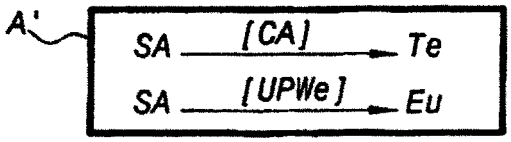
A'
SA
[CA]
Te
SA
[UPWe]
Eu

FIG.1b

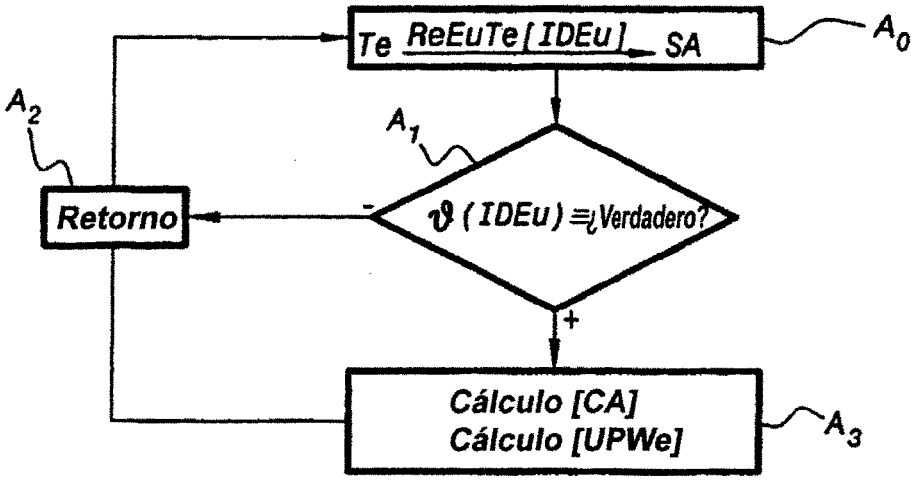
Te ReEuTe[IDEu] SA
A0
A2
A1
Retorno
ϑ (IDEu) ≡¿Verdadero?
-
+
Cálculo [CA]
Cálculo [UPWe]
A3

FIG.1c

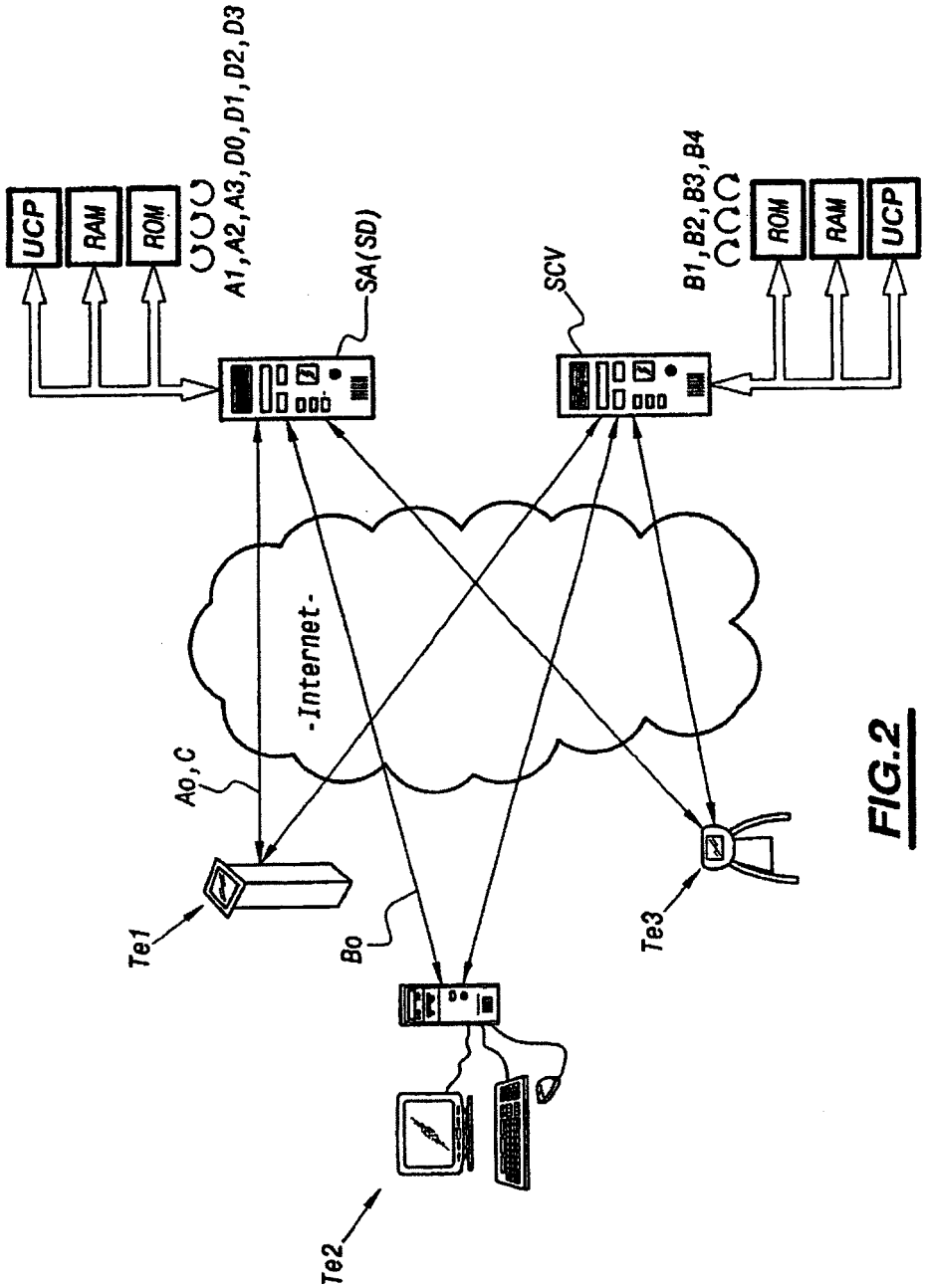
UCP
RAM
ROM
A1, A2, A3, D0, D1, D2, D3
SA(SD)
SCV
B1, B2, B3, B4
ROM
RAM
UCP
-Internet-
Ao, C
Te1
Bo
Te3
Te2

FIG.2

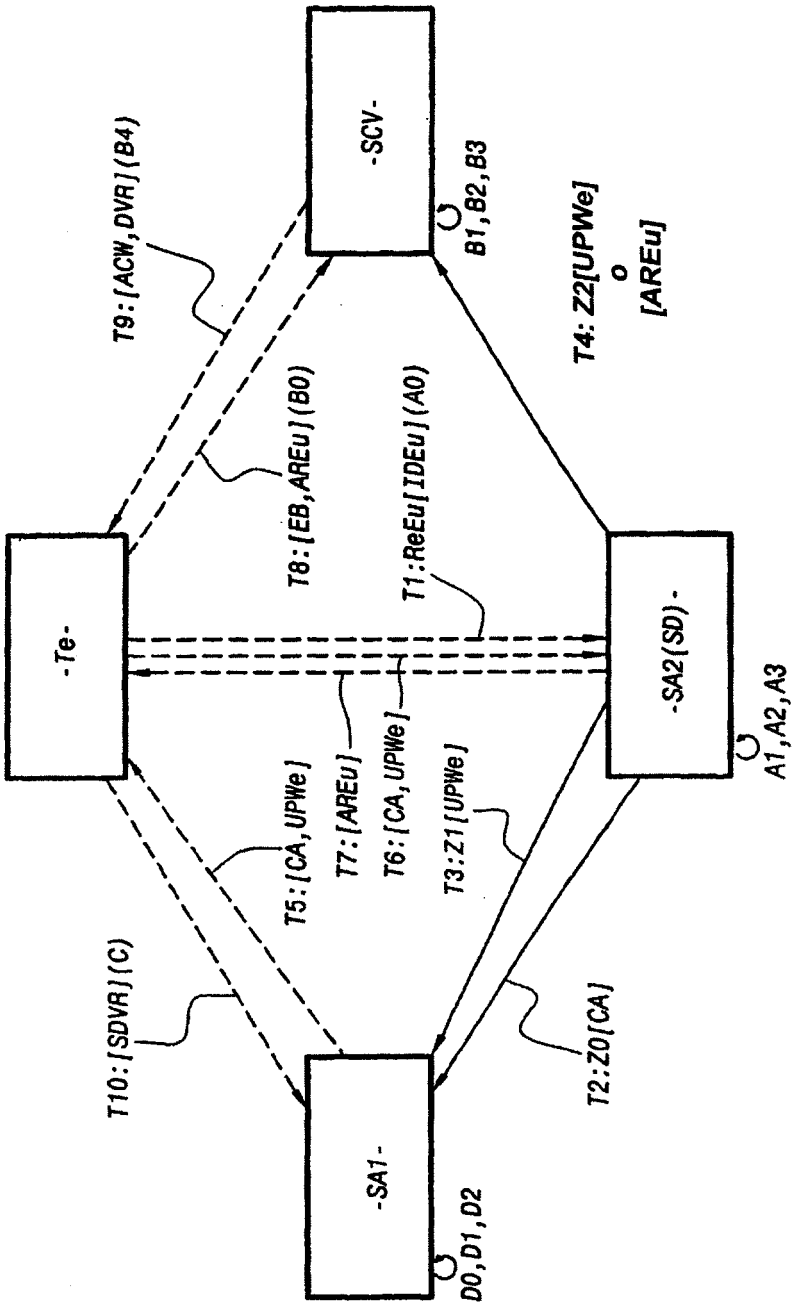
-SCV-
B1, B2, B3
T4: Z2[UPWe]
o
[AREu]
T9: [ACW, DVR] (B4)
T8: [EB, AREu] (B0)
T1: ReEu[IDEu] (A0)
-Te-
-SA2(SD) -
A1, A2, A3
T5: [CA, UPWe]
T7: [AREu]
T6: [CA, UPWe]
T3: Z1 [UPWe]
T10: [SDVR] (C)
T2: Z0 [CA]
-SA1-
D0, D1, D2

FIG.3

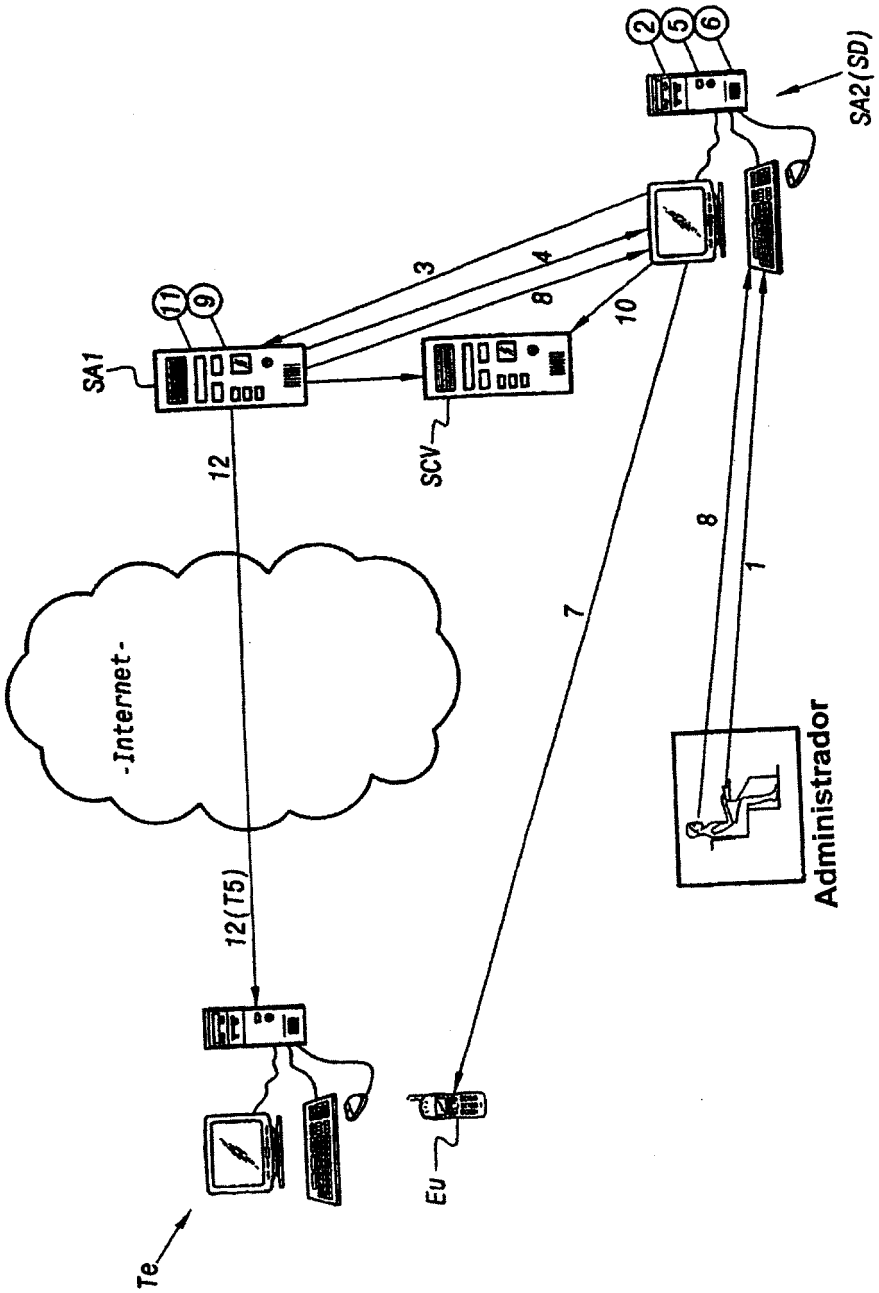
SA2(SD)
2
5
6
3
4
8
10
11
9
SA1
SCV
12
-Internet-
8
1
7
Administrador
12(T5)
Eu
Te

FIG.4a

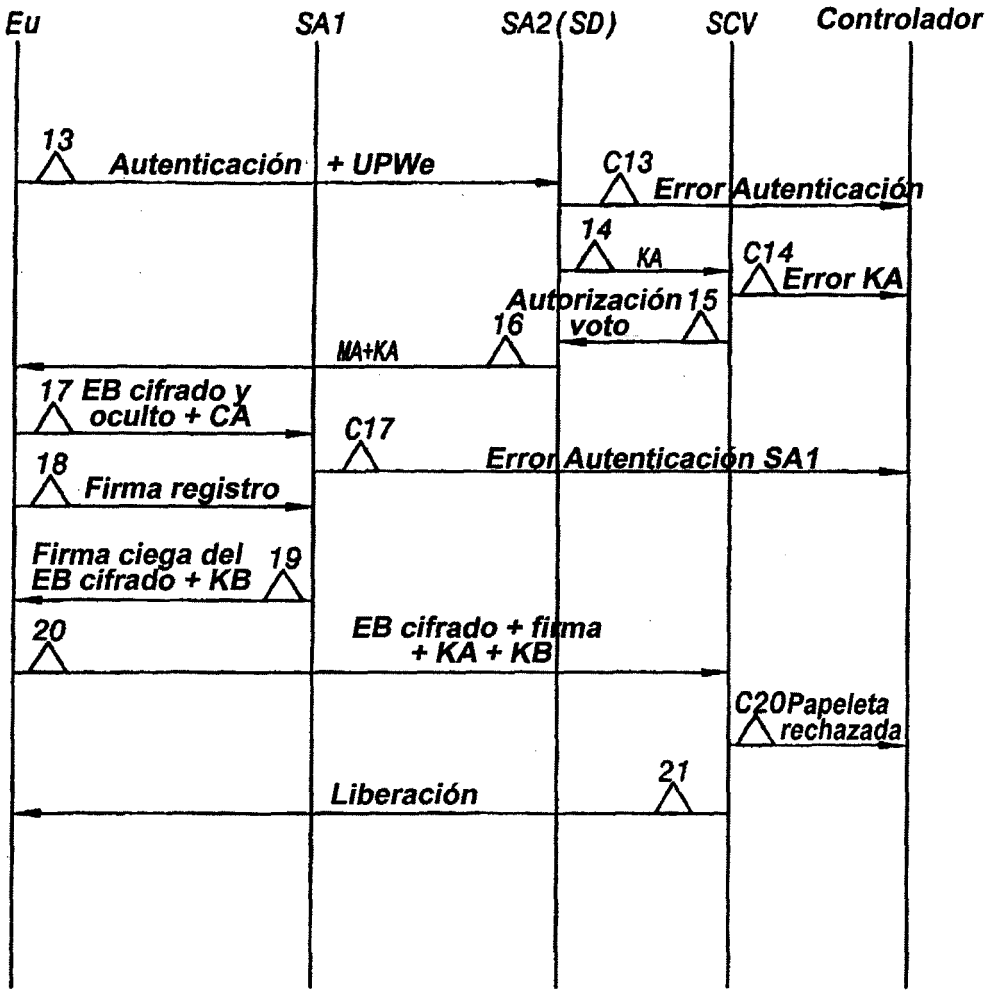
Eu
SA1
SA2 (SD)
SCV
Controlador
13
Autenticación
+ UPWe
C13
Error Autenticación
14
KA
C14
Error KA
Autorización 15
voto
16
MA+KA
17 EB cifrado y oculto + CA
C17
Error Autenticación SA1
18
Firma registro
Firma ciega del EB cifrado + KB
19
20
EB cifrado + firma + KA + KB
C20 Papeleta rechazada
21
Liberación

FIG.4b