(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 425 618**

(21) Número de solicitud: 201230268

(51) Int. CI.:

G06Q 20/04 (2012.01)
G07B 15/00 (2011.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

22.02.2012

(43) Fecha de publicación de la solicitud:

16.10.2013

(56) Se remite a la solicitud internacional:

PCT/ES2013/000045

(71) Solicitantes:

UNIVERSITAT ROVIRA I VIRGILI (50.0%)
C/ de l'Escorxador, s/n
43007 TARRAGONA ES y
UNIVERSITAT DE LES ILLES BALEARS (50.0%)

(72) Inventor/es:

DOMINGO FERRER, Josep;
CASTELLÀ ROCA, Jordi;
VIVES GUASCH, Arnau;
ARAGONÉS VILELLA, Jordi;
HUGUET ROTGER, Llorenç;
FERRER GOMILA, Josep Lluís;
MUT PUIGSERVER, Macià y
PAYERAS CAPELLA, M. Magdalena

(74) Agente/Representante:

TORNER LASALLE, Elisabet

(54) Título: **Método para realizar transacciones con billetes digitales**

(57) Resumen:

Método para realizar transacciones con billetes digitales.

El método es aplicable a billetes digitales provistos de un identificador, una prueba de validez y una información relativa a un derecho de uso asociado a dicho billete digital, comprendiendo las etapas de:

a. envío por un usuario propietario UP de una oferta de transacción del billete digital;

b. verificación de la prueba de validez de dicho billete digital por parte de un usuario receptor UR;

c. generación de una petición de transferencia de dicho UR a dicho UP;

d. verificación por dicho UP de dicha petición de transferencia y generación por dicho UP de una aceptación de transferencia;

e. verificación por dicho UR de dicha aceptación de transferencia; y

f. transferencia del billete digital a UR que adquiere el derecho de uso.

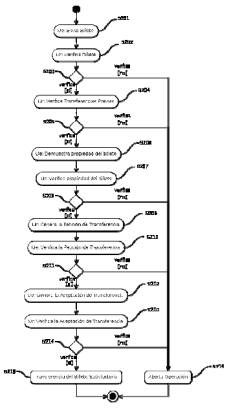

FIG.5

ES 2 425 618 A1

DESCRIPCIÓN

Método para realizar transacciones con billetes digitales

Sector de la técnica

La presente invención concierne en general, a un método para transacciones con billetes digitales/electrónicos y en particular, a un método que comprende la obtención y uso de un billete digital entre usuarios.

La presente invención contiene partes tales como las explicaciones detalladas acerca de los protocolos empleados, y en particular el protocolo de transferencia de un billete digital, susceptibles de protección bajo Copyright y los inventores se reservan los derechos de autoría sobre las mismas.

Antecedentes de la invención

La evolución de los dispositivos móviles, y sobre todo el aumento del uso de Internet en estos dispositivos, ha permitido que ciertas actividades comunes, como por ejemplo comprar, buscar información, o jugar se puedan realizar remotamente. La presente invención concierne a la compra del derecho de uso de un servicio mediante la obtención y uso de un billete digital. Por ejemplo y sin que deba entenderse como limitativo contratar un servicio como una entrada para un evento o medio de transporte.

El billete digital es una representación digital de un billete físico, ya sea un billete de un medio de transporte o bien, una entrada de acceso a un evento determinado. Una vez realizada la compra o el pago, el billete digital existe sólo como un registro digital. El comprador recibe en su dispositivo móvil el equivalente al billete real, y este será usado para garantizar el acceso al servicio contratado.

Ejemplos del uso de un billete digital se encuentran en el transporte aéreo. En Mayo de 2007 Vodafone y Spanair realizaron un test de billete digital en España. Los pasajeros recibían una tarjeta de embarque digital en su dispositivo móvil, esto daba derecho al pasajero a acceder directamente a la zona de control y, seguidamente, al avión.

La IATA (International Air Transport Association) empezó en 2004 un programa para potenciar el uso de los billetes digitales. Se realizó una estimación de que el uso de dichos billetes digitales ahorraría a las compañías aéreas una cantidad muy significativa de dinero.

Otro ejemplo del uso de los billetes digitales se da en la República Checa donde AMSBUS permite la reserva de transporte mediante mensajes SMS.

El equipo de futbol Leeds United, puso a disposición de sus seguidores la reserva de entradas para sus partidos. Dichos seguidores recibían en sus dispositivos móviles un SMS con la confirmación de la reserva además de información adicional, como por ejemplo, el asiento reservado.

Por la WO2009/141614 se conoce un método para transacciones con billetes digitales en el cual una imagen se muestra en un dispositivo móvil para facilitar una inspección. El método comprende recibir datos específicos del billete digital en un dispositivo móvil. Los datos se presentan en la forma de un código leíble por una máquina que define al menos un único número de billete y unos medidos de autenticación. El método comprende también ejecutar una aplicación en el dispositivo móvil de manera que proporcione información textual y gráfica en la pantalla del dispositivo móvil para permitir una autenticación de la información textual.

Estos ejemplos muestran la introducción del billete digital en distintos servicios y el aumento del uso de los dispositivos móviles como unidad de almacenamiento. Uno de los puntos clave para su implantación definitiva recae en la seguridad que estos puedan ofrecer, esto es debido a la facilidad de copia de la información digital. Los billetes digitales deben ofrecer la misma seguridad que la proporcionada por los billetes en papel.

En un billete real, normalmente de soporte papel, el propietario de dicho billete puede comprobar su veracidad por distintos medios. El billete puede incorporar medidas antifraude, como por ejemplo, un tipo determinado de papel, uso de tinta específica, zonas con hologramas, etc… En cambio, en el caso del billete digital el comprador necesita que el billete contenga distintas características que garanticen su seguridad que normalmente no se pueden comprobar por inspección visual.

Las características básicas que un billete digital debe ofrecer son las siguientes:

- No repudio: el ente que ha emitido el billete digital no puede negar su autenticidad.

- Integridad: el billete digital no puede ser modificado sin que dicha modificación sea detectada.

- Anonimato y revocabilidad: el billete digital es anónimo aunque, si el usuario hace un uso indebido, dicho usuario puede ser identificado. La característica de anonimato puede no ser posible, según el servicio.

- Reusabilidad: dependiendo de las necesidades y características del servicio el billete digital puede ser usado una o múltiples veces. Cada servicio tendrá unos u otros requisitos.

- Fecha de validez: el billete digital puede ser válido durante un intervalo definido de tiempo.

- Online/Offline: la verificación del billete digital puede requerir (o no) una conexión a una red de ordenadores para su validación.

- Exculpabilidad: el proveedor del servicio no puede acusar falsamente al usuario del billete digital de no haberlo validado antes de usarlo.

- Transferibilidad: el billete digital puede ser transferido a otros usuarios conservando todas las características mencionadas anteriormente.

Existe un amplio abanico de medidas de seguridad digital genéricas que pueden ser empleadas para aportar seguridad a un sistema de billete digital. Dependiendo del sistema utilizado la aplicación variará. Un ejemplo de tales medidas serían las basadas en Smart-cards. Dichas Smart-cards verifican cada operación, de modo que el usuario no puede realizar ninguna acción no permitida. La seguridad de estos sistema está basada en la propia seguridad de la propia Smart-card, si esta falla, el sistema se ve comprometido como es el caso de "*A practical attack on the mifare classic*" de Gerhard Koning Gans, Jaap-Henk Hoepman y Flavio D. Garcia, donde comprometen la seguridad de las tarjetas Mifare. En la literatura científica se encuentran distintas medidas de seguridad implementadas en las Smart-cards, como por ejemplo, *Electronic ticket scheme for its* de S. Matsuo y W. Ogata, *Application of electronic ticket to online trading with smartcard technology* de W.I. Siu y Z.S. Guo, *The secure communication protocol for electronic ticket management system* de W.I. Siu y Z.S. Guo.

Para sistemas no basados en Smart-cards, como es el caso de esta invención, se propone el uso de distintas técnicas criptográficas, que requieren cálculos avanzados y, por lo tanto, el uso de dispositivos móviles con capacidad avanzada de cálculo, como los teléfonos móviles, PDAs, etc. Estos sistemas pueden ser de dos tipos: 1) No anónimos, hay servicios que el anonimato no es una opción, en estos casos la firma digital es la técnica criptográfica más común, un ejemplo es *Digital-ticket-controlled digital ticket circulation* de K. Fujimura, H. Kuno, M. Terada, K. Matsuyama, Y. Mizuno y J. Sekine. 2) No-repudiación-anonimato, una técnica habitual para proporcionar el anonimato es mediante el uso de seudónimos, y nuevamente, la técnica más común es la firma digital, esta técnica proporciona al billete digital las propiedades de autenticidad, no repudiación e integridad. Algunas propuestas de interés aparecen en *Ticket based service Access for the mobile user* de B. Patel y J. Crowcroft, *Motet: Mobile transactions using electronic tickets* de D. Quercia y S. Hailes. En el caso de la propuesta realiza por Patel y Crowfort los billetes pueden ser reutilizados; Quercia y Hailes considera que la reusabilidad depende del servicio. Otras propuestas proponen una solución para la propiedad de online/offline, es el caso de *Privacy for Public Transportation* de T.S. Heydt-Benjamin, H.J. Chae, B. Defend y K. Fu (online) y *Electronic-onboard-ticketing: Software challenges of an state-of-the-art m-commerce application* de F. Hanenberg, K. Stenzel y W. Reif.

Algunas invenciones previas presentan sistemas y/o métodos de billete digital que garantizan alguna de las propiedades anteriores pero no todas a la vez. Los ejemplos más remarcables son las invenciones descritas en US7809593 *Method and system for automatically keeping travel data consistent between passenger reservation records and corresponding electronic tickets* de Douck *et al*. US7907896 *Mobile commerce method and device* de Chitti, US7685020 *Mobile commerce receipt system* de Do et al. US7520427 *Method of operating a ticketing system* de Boyd, US2010170947 *System and method for electronic ticket verification, identification, and authorization with a wireless communication device* de C. Bruce, PCT/IB2005/000948 *Methods and systems to purchase bookings* de A. Rangnekar et al. Todas estas invenciones únicamente describen la operatividad del método de comunicación y verificación de los billetes digitales, pero no hacen hincapié en los problemas de seguridad y privacidad mencionados anteriormente.

Un segundo grupo, siendo ejemplos representativos CN1987903 *Non-contact paper base electronic passenger ticket based on electronic label technology* de K. K. Hu et al., EP1752936 *Method of downloading ticketing keys* de R. Denis et al., WO2005111953 *Improved ticketing scheme* de H. B. SIM et al., KR20050057563 *Wireless communication device providing a contactless interface for a Smart card reader* de P. Lauri, EP2081140 *Method and system for protecting a transaction* de S. Spitz et al. contemplan tan sólo la seguridad a nivel de hardware. Dichas invenciones cifran las comunicaciones y el almacenaje del billete digital para asegurar su privacidad, sin

importar la seguridad y/o privacidad del propio billete digital. Estos métodos no garantizan las propiedades equivalentes en un billete real.

Las invenciones descritas en US6725376 *Method of using an electronic ticket and distributed server computer architecture for the same* de S. Levent, US2010005304 *Security and ticketing system control and management* de M. Hiroshi, WO03048892 *Access, identity, and ticketing system for providing multiple access methods for Smart devices* de S.M. Myra, contemplan la seguridad en el billete digital proporcionando algunas características como el anonimato o la integridad. Las anteriores invenciones utilizan un sistema de criptografía basada en hash. Un ejemplo del uso de criptografía basada en hash aparece en *Method of using an electronic ticket and distributed server computer architecture for the same* donde la información que contiene el billete digital es utilizada para obtener un valor hash. Este valor hash es cifrado utilizando un servidor de autenticación y una clave privada, y se concatena el valor resultante con la información del billete digital. De esta manera al hacer la validación del billete digital se asegura la integridad de dicho billete y puede ser transmitido por medios no seguros. Esta invención no asegura el anonimato del billete digital, tan sólo su integridad. El problema de la solución propuesta en dicha invención es que no incluye características como revocabilidad, exculpabilidad, anonimato, etc.

La US 7188358 describe un billete digital de acceso personalizado y período de validez prefijado, que contiene unas identificaciones anónimas de un remitente y de un receptor en una correspondencia por e-mail, así como un esquema para una comunicación en red con un mecanismo de ocultación.

En la US 7630927 se describe un método de pago anónimo y seguro, en línea, y un método basado un una firma criptográfica ciega parcial, con anonimato revocable.

Se consideran también de interés por la forma de construir el billete digital o por las propuestas relativas a la transacción de los billetes los documentos US 7630927 y US 2011/0119098.

Breve descripción de la invención

De lo anteriormente expuesto se desprende que es necesaria una alternativa al estado de la técnica que permita la obtención y uso de un billete digital ofreciendo las características básicas que este tipo de billetes requieren, antes citadas en lo que se refiere por lo menos a la: seguridad, privacidad, anonimato, revocabilidad y exculpabilidad, y que posibilite ser transferido conservando todas estas propiedades que son trasladadas al nuevo propietario.

Para ello la presente invención concierne a un método para realizar transacciones con billetes digitales, en donde dicho billete digital contiene al menos:

un identificador enlazado directa o indirectamente a unas condiciones de contrato;

una prueba de validez creada por el emisor de dicho billete digital, y

una información relativa al derecho de uso de un usuario propietario (UP) que ha adquirido dicho billete digital.

El citado identificador en una primera realización contiene la fecha de emisión del billete digital y dicha prueba de validez contiene una firma digital de dicho emisor que garantiza autenticidad, no repudio e integridad de dicho billete digital.

Por su parte dicho derecho de uso comprende al menos una vinculación entre dicho identificador del billete digital y dicho UP realizada mediante una firma digital de dicho UP o un certificado digital de dicho UP.

En una realización alternativa dicho derecho de uso comprende una vinculación entre dicho identificador del billete digital y dicho UP realizada mediante una primera firma digital de grupo que proporciona un anonimato revocable a dicho UP.

La información relativa al derecho de uso de un usuario receptor (UR) que ha adquirido el billete digital contiene además datos acerca de transferencias anteriores y comprende una etapa adicional de verificación de dichas transferencias anteriores por parte de dicho UR.

Por otro lado el referido billete digital de acuerdo con una realización de esta invención ha sido obtenido mediante las siguientes etapas:

- generar un precontrato (compromiso efectivo entre un emisor y un UP) a partir de una petición de billete digital por parte de dicho UP mediante una firma digital de dicho emisor;

- verificar dicho precontrato por parte de dicho UP;

- aceptar dicho precontrato creando una vinculación UP billete digital; y

- emitir el billete digital mediante una firma digital del emisor.

El método de la presente invención comprende, de acuerdo con lo anteriormente indicado, una transmisión segura de dicho billete digital entre usuarios: usuario propietario UP y usuario receptor UR, con transferencia segura de dicho derecho de uso, y las restantes propiedades indicadas.

El método, en relación con dicha transferencia segura, comprende las siguientes etapas:

a) envío por parte de dicho UP de una oferta de transacción; a dicho UR;

b) verificación de dicha prueba de validez por parte de dicho UR (esta verificación puede realizarse por medios diversos);

c) generación de una petición de transferencia de dicho UR a dicho UP;

d) verificación de dicha petición de transferencia por parte de dicho UP (igualmente llevada a cabo por medios diversos), y generación por dicho UP de una aceptación de transferencia; y

e) verificación por dicho UR de dicha aceptación de transferencia; y f) transferencia del billete digital adquiriendo dicho UR el citado derecho de uso de dicho UP.

La citada verificación de dicha prueba de validez consiste en la verificación de dicha firma digital de dicho emisor UP.

Para dicha transmisión se ha previsto en un ejemplo de ejecución (en el caso de vinculación entre dicho identificador del billete digital y dicho UP realizada mediante una firma digital de grupo) realizar una segunda firma digital de grupo por parte de dicho UP que se enlaza con dicha primera firma digital de grupo proporcionando una garantía de que UP es el que transfiere preservando su anonimato.

El método incluye para reforzar la estrategia de protección una etapa adicional consistente en proporcionar a dicho UP una prueba de su derecho de uso del billete digital a dicho UR, que prueba dicha vinculación entre identificador y UP.

Breve descripción de las figuras

Las anteriores y otras ventajas y características se comprenderán más plenamente a partir de la siguiente descripción detallada de unos ejemplos de realización con referencia a los dibujos adjuntos, que deben tomarse a título ilustrativo y no limitativo, en los que:

La Fig. 1 muestra la arquitectura utilizada para la emisión del billete digital. La nomenclatura utilizada en la figura es la que se detalla a continuación:

100: usuario, 105: relación de interacción física usuario-dispositivo, 110: terminal portátil del usuario, 120: aplicación del terminal de usuario, 125: sistema de almacenamiento del terminal de usuario, 130: terminal del emisor, 140: aplicación del terminal del emisor, 145: sistema de almacenamiento del terminal del emisor, 150: sistema de comunicación terminales usuario-emisor, 160: terminal bancaria, 170: sistema de comunicación terminales usuario-banco, 180: sistema de comunicación terminales emisor-banco.

La Fig. 2 muestra la arquitectura utilizada para la transferencia del billete digital. La nomenclatura utilizada en la figura es la que se detalla a continuación:

200: usuario emisor, 201: usuario receptor, 205: relación de interacción física usuario emisor-dispositivo, 206: relación de interacción física usuario receptor-dispositivo, 210: terminal portátil del usuario emisor, 220: aplicación del terminal del usuario emisor, 225: sistema de almacenamiento del terminal del usuario emisor, 230: terminal portátil del usuario receptor, 240: aplicación del terminal del usuario receptor, 245:

sistema de almacenamiento del terminal del usuario receptor, 250: sistema de comunicación de terminales usuarios emisor-receptor, 260: terminal bancaria, 270: sistema de comunicación de terminales usuario emisor-banco, 280: sistema de comunicación de terminales usuario receptor-banco.

La Fig. 3 muestra la arquitectura utilizada para la utilización del billete digital. La nomenclatura utilizada en la figura es la que se detalla a continuación:

300: usuario, 305: relación de interacción física usuario-dispositivo, 310: terminal portátil del usuario, 320: aplicación del terminal de usuario, 325: sistema de almacenamiento del terminal de usuario, 330: terminal del proveedor de servicios, 340: aplicación del terminal del proveedor de servicios; 345: sistema de almacenamiento del terminal del proveedor de servicios, 350: comunicación usuario-proveedor.

Las Figs. 4, 5 y 6 muestran unos diagramas de secuencia utilizados para la emisión, transferencia y utilización del billete digital, respectivamente.

Exposición en detalle de la invención

Para las firmas en el sistema hechas por el usuario, la presente invención utiliza las propiedades de las firmas digitales y de grupo. Aunque existen diferentes propuestas en la presente invención se utiliza el esquema propuesto en SDH (*Strong Diffie-Hellman)*, [BBS04]. Por esta razón, se presentan a continuación las principales definiciones. La notación en la parte que sigue es específica para la explicación de estas definiciones.

En el esquema [BB04]) se consideran grupos cíclicos (multiplicativos) G_1 y G_2 de orden primo p con sus respectivos generadores g_1 y g_2., además de una aplicación bilineal e: $G_1 \times G_2 \rightarrow G_T$ y una función hash $H: \{0,1\}^* \rightarrow Z_p^*$. Los parámetros públicos son $g_1, u, v, h \in G_1$ y $g_2, w \in G_2$. Aquí $w = g_2^{\gamma}$ para un valor secreto $\gamma \in Z_p$.

- *KeyGen$_G$(n).* En este algoritmo se toma como entrada un parámetro n, que corresponde al número de miembros que formaran el grupo. Se selecciona $h \xleftarrow{R} G_1 \setminus \{1_{G1}\}$ y $\xi_1, \xi_2 \xleftarrow{R} Z_p^*$, y se calcula $u, v \in G_1$ tal que $u^{\xi_1} = v^{\xi_2} = h$. Se selecciona $\gamma \xleftarrow{R} Z_p^*$ y se calcula $w = g_2^{\gamma}$. A continuación, se genera después para cada usuario U_i, $1 \leq i \leq n$, una tupla SDH (A_i , x_i) de este modo: se selecciona $x_i \xleftarrow{R} Z_p^*$ y se calcula $A_i \leftarrow g_1^{1/(\gamma+x_i)}$. La clave privada del creador del grupo (la entidad que puede descubrir la identidad de los firmantes) es gmsk=(ξ_1,ξ_2). Cada clave privada de usuario es su tupla gsk[i] = (A_i , x_i). Ninguna entidad puede conocer el parámetro secreto γ aparte del creador del grupo.

- *Sign$_G$(M).* Dada una clave pública de grupo $gpk = (g_1, g_2, h, u, v, w)$, una clave privada de grupo específica de un usuario $gsk[i] = (A_i, x_i)$ y un mensaje de entrada $M \in \{0,1\}^*$, un usuario calcula y genera $M' = (M, \sigma)$ donde σ es la firma de conocimiento $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta 1}, s_{\delta 2})$. Desde el punto de vista del usuario, él conoce su clave privada de grupo $gsk = (A, x)$ y así se refleja en la siguiente notación.

  1. selecciona $\alpha, \beta \xleftarrow{R} Z_p$ y calcula el cifrado lineal de $A: (T_1,T_2,T_3) \leftarrow (u^{\alpha}, v^{\beta}, Ah^{\alpha+\beta})$ conjuntamente con los valores $\delta_1 \leftarrow x\alpha$ y $\delta_2 \leftarrow x\beta$;

  2. selecciona $r_\alpha, r_\beta, r_x, r_{\delta 1}, r_{\delta 2} \xleftarrow{R} Z_p$ y calcula los valores:

$$R_1 \leftarrow u^{r\alpha}$$

$$R_2 \leftarrow v^{r\beta}$$

$$R_3 \leftarrow e(T_3,g_2)^{rx} \cdot e(h,w)^{-r\alpha-r\beta} \cdot e(h,g_2)^{-r\delta 1-r\delta 2}$$

$$R_4 \leftarrow T_1^{rx} \cdot u^{-r\delta 1}$$

$$R_5 \leftarrow T_2^{rx} \cdot v^{-r\delta 2}$$

  3. obtiene el reto (challenge):

$$c \leftarrow H(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5)$$

4. calcula los valores:

$$s_\alpha \leftarrow r_\alpha + c\alpha$$

$$s_\beta \leftarrow r_\beta + c\beta$$

$$s_x \leftarrow r_x + cx$$

$$s_{\delta 1} \leftarrow r_{\delta 1} + c\delta_1$$

$$s_{\delta 2} \leftarrow r_{\delta 2} + c\delta_2$$

5. genera la salida $\sigma \leftarrow (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta 1}, s_{\delta 2})$.

- *Verify*$_G(M^*)$. Dada una clave pública de grupo $gpk = (g_1, g_2, h, u, v, w)$ y un mensaje firmado con la correspondiente clave privada de un miembro del grupo $M^* = (M, \sigma)$ como entrada, donde M es el mensaje y σ su firma de manera que $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta 1}, s_{\delta 2})$, un usuario cualquiera puede verificar que σ es una firma de conocimiento válida mediante los siguientes pasos.

Obtiene de la forma siguiente $\tilde{R}_1, \tilde{R}_2, \tilde{R}_3, \tilde{R}_4, \tilde{R}_5$:

$$\tilde{R}_1 \leftarrow u^{s\alpha} / T_1^{\,c}$$

$$\tilde{R}_2 \leftarrow v^{s\beta} / T_2^{\,c}$$

$$\tilde{R}_3 \leftarrow e(T_3, g_2)^{sx} \cdot e(h, w)^{-s\alpha - s\beta} \cdot e(h, g_2)^{-s\delta 1 - s\delta 2} \cdot (e(T_3, w) / e(g_1, g_2))^c$$

$$\tilde{R}_4 \leftarrow T_1^{\,sx} / u^{s\delta 1}$$

$$\tilde{R}_5 \leftarrow T_2^{\,sx} / v^{s\delta 2}$$

1. comprueba que $c \stackrel{?}{=} H(M, T_1, T_2, T_3, \tilde{R}_1, \tilde{R}_2, \tilde{R}_3, \tilde{R}_4, \tilde{R}_5)$.

- *Open*$_G(M^*)$. Este algoritmo es utilizado para asignar una firma digital a su concreto firmante del grupo con la finalidad de conocer su identidad. Esta operación únicamente es posible para el creador del grupo, ya que es el único que conoce la clave maestra *gmsk*, y conoce todos los pares (A_i, x_i). Dada la clave pública de grupo $gpk = (g_1, g_2, h, u, v, w)$, la clave privada maestra de grupo $gmsk = (\xi_1, \xi_2)$, y el

mensaje firmado $M^*=(M,\sigma)$ como entrada, siendo M el mensaje y $\sigma=(T_1,T_2,T_3,c,s_\alpha,s_\beta,s_x,s_{\delta 1},s_{\delta 2})$ la firma, se procede como sigue. En primer lugar, recuperar el usuario A_i ejecutando $A_i \leftarrow T_3/(T_1^{\xi 1} \cdot T_2^{\xi 2})$. Si el gestor del grupo tiene los elementos $\{A_i\}$ de las claves privadas del usuario, puede buscar el índice del usuario correspondiente a la identidad A_i recuperada de la firma.

Enlazabilidad entre firmas de grupo

En el sistema de la invención, todos los usuarios tienen que ser anónimos, además, sus firmas no pueden ser enlazables una con otra. En algunos casos, por seguridad, determinadas firmas de un mismo usuario podrían ser enlazables entre ellas para garantizar que se trata del mismo usuario.

Procedimiento $SignLinkable_G$

Se define un procedimiento de firma enlazable llamada $SignLinkable_G(M',M^*)$ para ser utilizada en el protocolo. Dada una clave pública de grupo *gpk*, una clave privada de usuario *gsk[i]* y un mensaje M', computa y genera la salida $M'^*=(M',\sigma')$ que puede ser enlazable con el mensaje firmado M^*. Para utilizar dicho procedimiento correctamente, se sigue el siguiente protocolo:

- Primer uso: firmar de manera normal $Sign_G(M)$:
  - generar un cifrado lineal de A: $(T_1,T_2,T_3) \leftarrow (u^\alpha, v^\beta, Ah^{\alpha+\beta})$ para $\alpha,\beta \xleftarrow{R} Z_p$;
  - dado un mensaje M, firmar el mensaje y generar la salida $\sigma \leftarrow (T_1,T_2,T_3,c,s_\alpha,s_\beta,s_x,s_{\delta 1},s_{\delta 2})$ donde $c \leftarrow H(M,T_1,T_2,T_3,R_1,R_2,R_3,R_4,R_5) \in Z_p$;
- Siguientes usos: $SignLinkable_G(M',M^*)$: equivale a realizar el procedimiento $Sign_G(M)$ sin realizar el 1r paso de la generación de (T_1,T_2,T_3). De este modo, se reutiliza la pareja (α,β) y su resultado $(T_1,T_2,T_3)=(u^\alpha,v^\beta,Ah^{\alpha+\beta})$ y se sigue con el 2º paso del procedimiento $Sign_G(M)$.
  - utilizar la misma pareja (α,β) con el mismo cifrado lineal de A que en la primera firma: $(T_1,T_2,T_3)=(u^\alpha,v^\beta,Ah^{\alpha+\beta})$;
  - dado un mensaje M', firmar el mensaje y generar la salida $\sigma' \leftarrow (T_1,T_2,T_3,c',s_\alpha',s_\beta',s_x',s_{\delta 1}',s_{\delta 2}')$ donde:

$$c' \leftarrow H(M',T_1,T_2,T_3,R_1',R_2',R_3',R_4',R_5') \in Z_p;$$

Se puede demostrar que diferentes firmas son producidas por el mismo usuario, ya que la información (T_1,T_2,T_3) es pública en la misma firma. Además, los valores aleatorios $(r_\alpha',r_\beta',r_x',r_{\delta 1}',r_{\delta 2}')$ deben de ser diferentes que en previos usos, eso es: $(r_\alpha' \neq r_\alpha, r_\beta' \neq r_\beta, r_x' \neq r_x, r_{\delta 1}' \neq r_{\delta 1}, r_{\delta 2}' \neq r_{\delta 2})$ para no revelar información acerca de la identidad del usuario. Nótese también que los valores $(R_1',R_2',R_3',R_4',R_5')$ se establecen en el 2º paso del procedimiento $Sign_G(M)$, y dependen de los valores aleatorios $(r_\alpha',r_\beta',r_x',r_{\delta 1}',r_{\delta 2}')$ generados.

El procedimiento entonces es:

1. reutilizar (α, β) que se generó en el procedimiento de $Sign_G(M)$ como también el cifrado lineal de A: $(T_1,T_2,T_3)=(u^\alpha,v^\beta,Ah^{\alpha+\beta})$, y los valores $\delta_1=x\alpha$ y $\delta_2=x\beta$;

2. seleccionar $r_\alpha',r_\beta',r_x',r_{\delta 1}',r_{\delta 2} \xleftarrow{R} Z_p$ y calcular los valores:

$$R_1' \leftarrow u^{r\alpha'}$$

$$R_2' \leftarrow v^{r\beta'}$$

$$R_3' \leftarrow e(T_3,g_2)^{rx'} \cdot e(h,w)^{-r\alpha'-r\beta'} \cdot e(h,g_2)^{-r\delta 1'-r\delta 2'}$$

$$R_4' \leftarrow T_1^{rx'} \cdot u^{-r\delta 1'}$$

$$R_5' \leftarrow T_2^{rx'} \cdot v^{-r\delta 2'}$$

3. obtener el reto (challenge):

$$c' \leftarrow H(M', T_1, T_2, T_3, R_1', R_2', R_3', R_4', R_5')$$

4. calcular los valores:

$$s_\alpha' \leftarrow r_\alpha' + c'\alpha$$

$$s_\beta' \leftarrow r_\beta' + c'\beta$$

$$s_x' \leftarrow r_x' + c'x$$

$$s_{\delta 1}' \leftarrow r_{\delta 1}' + c'\delta_1$$

$$s_{\delta 2}' \leftarrow r_{\delta 2}' + c'\delta_2$$

generar la salida $\sigma' \leftarrow (T_1, T_2, T_3, c', s_\alpha', s_\beta', s_x', s_{\delta 1}', s_{\delta 2}')$.

Procedimiento VerifyLinkable$_G$

Se define también el procedimiento: *VerifyLinkable$_G$(M^*,M'^*).* Este algoritmo toma como entrada $(M^*=(M,\sigma),M'^*=(M',\sigma'))$ con las 2 firmas $\sigma=(T_1,T_2,T_3,c,s_\alpha,s_\beta,s_x,s_{\delta 1},s_{\delta 2})$ y $\sigma'=(T_1',T_2',T_3',c',s_\alpha',s_\beta',s_x',s_{\delta 1}',s_{\delta 2}')$, y genera la salida 'verdadero' o 'falso' dependiendo de si las firmas han sido producidas por el mismo seudónimo del usuario (T_1,T_2,T_3):

$$(T_1 \stackrel{?}{=} T_1', T_2 \stackrel{?}{=} T_2', T_3 \stackrel{?}{=} T_3')$$

Prueba de conocimiento nulo (Zero-Knowledge Proof) del esquema de firma de grupo (Group Signature)

En el sistema se utilizan tanto las firmas digitales de grupo estándar como las enlazables, de modo que se pueda verificar la información interna del mensaje, como también verificar que algunas firmas concretas están relacionadas con el mismo evento/billete digital y pertenecen al mismo usuario. A pesar de estas ventajas, estas firmas son generadas por el mismo usuario, y su verificación se realiza offline o no directamente con el verificador. En algunas situaciones, aparece la necesidad de realizar pruebas interactivas de conocimiento para verificar que un cierto mensaje pertenece a la persona que está queriendo verificar el mensaje firmado/billete digital: es equivalente entonces a decir que el usuario conoce los parámetros secretos $(\alpha,\beta,x,\delta_1,\delta_2)$ con los cuales se ha generado la firma digital de grupo. Se detallan entonces los protocolos *ZKP$_G$Commit, ZKP$_G$Response y ZKP$_G$Verify* de la siguiente forma:

Procedimiento ZKP$_G$Commit(M^*)

Este procedimiento es realizado por la entidad que quiere demostrar el conocimiento de un cierto valor. Dada una clave pública de grupo $gpk=(g_1,g_2,h,u,v,w)$, una clave privada de grupo de un determinado usuario $gsk[i]=(A_i,x_i)$ y un mensaje auto-firmado $M^*=(M,\sigma)$ donde σ es la firma de conocimiento $\sigma=(T_1,T_2,T_3,c,s_\alpha,s_\beta,s_x,s_{\delta 1},s_{\delta 2})$,

se genera una nueva información de compromiso (commitment) para ser verificada de manera activa: $m'=(T_1,T_2,T_3,R_1',R_2',R_3',R_4',R_5')$.

1. se tiene que demostrar el conocimiento de $(\alpha,\beta,x,\delta_1,\delta_2)$, que ha sido generado para la firma de M^*, guardando entonces los valores resultantes como el cifrado lineal de $A: (T_1,T_2,T_3)=(u^{\alpha},v^{\beta},Ah^{\alpha+\beta})$;

2. seleccionar $r_\alpha',r_\beta',r_x',r_{\delta 1}',r_{\delta 2} \xleftarrow{R} Z_p$ y computar los valores:

$$R_1' \leftarrow u^{r\alpha'}$$

$$R_2' \leftarrow v^{r\beta'}$$

$$R_3' \leftarrow e(T_3,g_2)^{rx'} \cdot e(h,w)^{-r\alpha'-r\beta'} \cdot e(h,g_2)^{-r\delta 1'-r\delta 2'}$$

$$R_4' \leftarrow T_1^{rx'} \cdot u^{-r\delta 1'}$$

$$R_5' \leftarrow T_2^{rx'} \cdot v^{-r\delta 2'}$$

3. generar como salida el compromiso $m'=(T_1,T_2,T_3,R_1',R_2',R_3',R_4',R_5')$

<u>*Procedimiento ZKP_GResponse(m',c')*</u>

Dado un compromiso $m'=(T_1,T_2,T_3,R_1',R_2',R_3',R_4',R_5')$ y un reto (challenge) c' elegido por el verificador, el demostrador genera una respuesta a la *ZKP* como sigue:

1. calcular los valores:

$$s_\alpha' \leftarrow r_\alpha' + c'\alpha$$

$$s_\beta' \leftarrow r_\beta' + c'\beta$$

$$s_x' \leftarrow r_x' + c'x$$

$$s_{\delta 1}' \leftarrow r_{\delta 1}' + c'\delta_1$$

$$s_{\delta 2}' \leftarrow r_{\delta 2}' + c'\delta_2$$

2. generar como salida la respuesta $s'=(s_\alpha',s_\beta',s_x',s_{\delta 1}',s_{\delta 2}')$.

<u>*Procedimiento ZKP_GVerify(m',c',s')*</u>

Dado un compromiso $m'=(T_1,T_2,T_3,R_1',R_2',R_3',R_4',R_5')$, un reto c' elegido por el verificador, y su respuesta $s'=(s_\alpha',s_\beta',s_x',s_{\delta 1}',s_{\delta 2}')$ generada por el demostrador, el verificador prosigue con estos pasos:

1. comprobar que:

$$u^{s\alpha'} \stackrel{?}{=} T_1^{c'} \cdot R_1'$$

$$v^{s\beta'} \stackrel{?}{=} T_2^{c'} \cdot R_2'$$

$$e(T_3,g_2)^{sx'} \cdot e(h,w)^{-s\alpha'-s\beta'} \cdot e(h,g_2)^{-s\delta 1'-s\delta 2'} \stackrel{?}{=} (e(g_1,g_2)/e(T_3,w))^{c'} \cdot R_3'$$

$$T_1^{sx'} \cdot u^{-s\delta 1'} \stackrel{?}{=} R_4'$$

$$T_2^{sx'} \cdot v^{-s\delta 2'} \stackrel{?}{=} R_5'$$

Enlazabilidad entre firmas digitales

Dos firmas digitales convencionales estarán enlazadas si han sido emitidas por el mismo emisor que dispone de la clave privada.

En relación con las citadas Figs. 1 a 3, la nomenclatura utilizada y una posible implementación son las que se detallan a continuación:

En una implementación preferida, pero que no limita la invención, el terminal de usuario (110, 210, 230, 310) puede ser un dispositivo portátil (p.ej. teléfono móvil, smartphone, PDA, Tablet, etc.), la aplicación del terminal de usuario (120, 220, 240, 320) puede ser una aplicación para el dispositivo portátil (p.ej. aplicación J2ME, Android, iPhone, etc.) o incluso una aplicación en modo tarjeta (p.ej. JavaCard), utilizando una unidad de almacenamiento (125, 225, 245, 325) (p.ej. Secure Element del móvil, tarjetas SD, microSD, SIM, UICC, memoria interna del dispositivo, disco duro, base de datos, etc.)

En la parte del emisor del billete, el terminal (130) puede ser una máquina o servidor que tenga una aplicación (140) (con lenguajes de programación diversos, como p.ej. Java, C#, C++, etc.) y con una unidad de almacenamiento (145) (como p.ej. base de datos, etc.).

En la parte del proveedor de servicios, su terminal (330) puede ser una máquina o servidor que tenga una aplicación (340) (con lenguajes de programación diversos, como p.ej. Java, C#, C++, etc.) y con una unidad de almacenamiento (345) (como p.ej. base de datos, etc.).

La comunicación entre las aplicaciones de emisor/proveedor de servicios y usuario (150, 250, 350) puede estar basada en la tecnología de corto alcance Near Field Communication (NFC), tanto en los modos peer-to-peer (ISO18092) como en modo tarjeta (ISO14443, etc.) o Read/Write, pero no excluye otros modos de comunicación como por ejemplo: el acceso a Internet, mediante la pila de protocolos TCP/IP, WAN (Wide Area Network), o WWAN (Wireless Wide Area Network, que incluye 3G, UMTS, HSPA, etc.), RFID o Bluetooth entre otros.

La terminal bancaria (160, 260) puede ser también un entramado de terminales bancarias interrelacionadas entre sí, comunicando las entidades bancarias tanto del usuario como del emisor del billete digital. Así pues, la comunicación (170, 270) entre el terminal de usuario (110, 210, 230) y la entidad bancaria (160, 260) puede ser una conexión de largo alcance, como por ejemplo, a través del acceso a Internet, mediante la pila de protocolos TCP/IP, o a través de una WAN, o WWAN, entre otros. Por otro lado, la comunicación (180, 280) entre la máquina del emisor del billete digital (130) o la máquina del receptor del billete digital (230) y la entidad bancaria (160, 260), se realizará, en una implementación preferida sin que sea limitante, mediante la pila de protocolos TCP/IP, pero no está restringido únicamente a éste. En ambos casos, no se limita a que tenga que ser la propia aplicación la que se conecte a la terminal bancaria, ya que también se considera que puedan usarse otras aplicaciones en el mismo dispositivo que conecten independientemente con el terminal bancario, y la aplicación en sí esté indirectamente conectada con el terminal bancario.

La presente invención propone un método para transacciones de billetes digitales el cual se puede desglosar en 3 fases o protocolos diferentes:

- Emisión del billete digital (Figs. 1 y 4): El usuario recibe un billete digital original de parte de su correcto emisor. El usuario puede utilizarlo para obtener un servicio.

- Transferencia del billete digital (Figs. 2 y 5): El usuario que ha recibido un billete digital, puede transferirlo a otro usuario para que este otro usuario pueda utilizarlo en su lugar. El nuevo usuario que ha recibido el billete digital transferido, puede retransferir otra vez el billete digital a otro usuario.

- Utilización del billete digital (Figs. 3 y 6): El usuario que tiene un billete digital, sea original o transferido, puede utilizar dicho billete para obtener el servicio asociado.

Emisión del billete digital:

La Fig. 1 muestra la arquitectura correspondiente a la parte de emisión del billete digital. La Fig. 4 muestra su diagrama de secuencia.

El protocolo de emisión del billete digital consta de varios pasos:

- En el paso S101, el usuario realiza una petición al emisor para obtener un billete digital, pudiendo especificar el servicio (y/o los términos y condiciones) que se desea recibir posteriormente.

- En el paso S102, el emisor del billete digital genera un primer precontrato donde, en caso de especificar un servicio y/o términos/condiciones, dichos datos queden reflejados. En una implementación preferida, el emisor del billete digital genera un número de serie único, un valor aleatorio, y el servicio y/o términos/condiciones que se desean recibir; estos datos se firman digitalmente con la clave privada que posee el emisor del billete digital. Finalmente, el emisor envía el precontrato al usuario.

- En el paso S103, el usuario verifica los datos del precontrato. En una implementación preferida, el usuario verifica la firma electrónica del precontrato.

- En el paso S104, en caso que la verificación sea correcta, el usuario crea la aceptación del contrato, que comprende la firma digital o de grupo con el número de serie, servicio asociado (si existe) y el número aleatorio del precontrato, y se envía esta aceptación del contrato al emisor del billete digital. En caso que la verificación no sea correcta, se aborta la operación (S111). La utilización de las firmas de grupo garantiza el anonimato en este paso.

- En el paso S105, el emisor del billete digital verifica la aceptación del precontrato. Una implementación preferida, consiste en verificar la firma, ya sea electrónica o convencional, de dicho contrato.

- En la horquilla S106, en caso que la verificación de la aceptación del precontrato sea correcta, se genera el billete digital electrónico (S107). En una implementación preferida, el billete digital contiene el número de serie, el servicio asociado, la aceptación del precontrato creada por el usuario, además de otros parámetros opcionales como los términos y condiciones, etc.; este billete digital se firma electrónicamente con la clave privada del emisor y se envía al usuario. En caso de que la verificación no sea correcta, se aborta la operación (S111).

- En el paso S108, el usuario verifica el billete digital recibido. En una implementación preferida, se verifica la firma electrónica del billete digital.

- En la horquilla S109, en caso de que la verificación sea correcta, se da por concluida la emisión del billete digital de manera satisfactoria (S110); en caso que no sea correcta, se aborta la operación (S111).

Transferencia del billete digital:

La Fig.2 muestra la arquitectura en la parte de transferencia del billete digital. La Fig.5 muestra su diagrama de secuencia.

El protocolo de transferencia del billete digital consta de varios pasos:

- En el paso S201, el usuario emisor envía el billete digital que se dispone a transferir. Dicho billete digital da permiso de utilización únicamente al usuario emisor. En una implementación preferida, en la parte de la transmisión del billete digital, también se puede calcular y enviar un compromiso para verificar que es el correcto usuario del billete digital mediante firma digitales o de grupo enlazables (*) (esta verificación se lleva a cabo en el paso S206 pero puede prepararse en pasos previos para reducir el tiempo de respuesta del protocolo).

- En el paso S202, el usuario receptor verifica el billete digital recibido. En una implementación preferida, se verifica la información y su firma digital o de grupo.

- En el paso S203, se evalúa si se verifica correctamente o no el billete digital. Si es correcto, se continúa en el paso S204; si no es correcto, se aborta la operación de transferencia (S216).

- En el paso S204, se verifican las transferencias previas que el billete digital pueda tener. En una implementación preferida, estas verificaciones consisten en verificar las firma digitales o de grupo y que todas las firma digitales o de grupo estén correctamente enlazadas (*). Es decir, existe un billete digital adaptado para cada usuario que ha tenido en propiedad el billete digital, donde se le dan permisos para que pueda utilizarlo, y si desea retransferir el billete digital, puede hacerlo demostrando que es el correcto usuario y firmando con una firma digital o de grupo enlazable con su anterior generada en la obtención del billete digital. También se genera el reto acorde con el compromiso de emisión enviado por el usuario emisor en el paso S201.

- En la horquilla S205, se evalúa si se verifican correctamente o no las firmas digitales o de grupo y si las mismas enlazan correctamente. Si es correcto, se continúa en el paso S206; si no es correcto, se aborta la operación de transferencia (S216).

- En el paso S207, el usuario emisor demuestra la propiedad del billete digital dando la prueba al usuario receptor. En una implementación preferida, se calcula la respuesta al reto recibido por el usuario receptor (paso S204) teniendo en cuenta el compromiso enviado en el paso S201.

- En la horquilla S208, se evalúa si se verifica correctamente o no la propiedad del billete digital. Si es correcto, se continúa en el paso S209; si no es correcto, se aborta la operación de transferencia (S216).

- En el paso S209, el usuario receptor genera la petición de transferencia. En una implementación preferida, ello consiste en la generación de la firma digital o de grupo con el contenido del billete digital que se desea obtener.

- En el paso S210, el usuario emisor verifica la petición de transferencia. En una implementación preferida, ello consiste en la verificación de la firma digital o de grupo de la petición de transferencia.

- En la horquilla S211, se evalúa si se verifica correctamente o no la petición de transferencia. Si es correcta, se continúa en el paso S212; si no es correcta, se aborta la operación de transferencia (S216).

- En el paso S212, el usuario emisor genera la aceptación de transferencia, que consiste, en una implementación preferida, en firmar la petición del usuario receptor con una firma digital o de grupo enlazada con la firma que se utilizó para la obtención del billete digital anteriormente.

- En el paso S213, el usuario receptor verifica la aceptación de transferencia. Esta aceptación de transferencia incluye entonces el billete digital y los permisos para que el usuario receptor lo pueda utilizar posteriormente. En una implementación preferida, esta verificación incluye la verificación de la firma digital o de grupo, además de comprobar si esta firma coincide con la que utilizó el usuario emisor para obtener el billete digital.

- En la horquilla S214, se evalúa si se verifica correctamente o no la aceptación de transferencia. Si es correcta, se continúa y se llega al estado S215 de transferencia satisfactoria; si no es correcta, se aborta la operación de transferencia (S216).

Utilización del billete digital:

La Fig. 3 muestra la arquitectura en la parte de utilización del billete digital. La Fig. 6 muestra su diagrama de secuencia.

El protocolo de utilización del billete digital consta de varios pasos:

- En el paso S301, el usuario envía el billete digital que se dispone a utilizar.
- En el paso S302, el proveedor de servicios verifica el billete digital. En una implementación preferida, ello consiste en verificar la firma digital o de grupo del billete digital.
- En la horquilla S303, se evalúa la verificación del billete digital. Si es correcta, se continúa en el paso S304; si no es correcta, se aborta la operación (estado S310).
- En el paso S304, se verifican las transferencias previas (si las hay). En una implementación preferida, ello consiste en verificar todas las firma digitales o de grupo de los billetes digitales transferidos, y además verificar que enlazan, para cada usuario, la obtención del billete digital con su posterior transferencia.
- En la horquilla S305, se evalúan las verificaciones de las transferencias previas. Si son correctas, se continúa en el paso S306; si no son correctas, se aborta la operación (estado S310).
- En el paso S306, se demuestra la propiedad del billete digital. En una implementación preferida, ello consiste en realizar una firma digital o de grupo (que sea enlazable con el billete digital obtenido) de un valor enviado por el proveedor de servicios "al mismo momento". De este modo, el usuario no puede conocer el contenido a firmar y lo debe calcular en ese instante.
- En el paso S307, se verifica la propiedad del billete digital. En una implementación preferida, ello consiste en verificar la firma digital o de grupo, y también verificar que dicha firma es enlazable con el billete digital que obtuvo el usuario y ha sido presentado.
- En la horquilla S308, se evalúa la verificación de la propiedad del billete digital. Si es correcta, se llega al estado de utilización satisfactoria S309 y el usuario puede recibir el servicio; si no es correcta, se aborta la operación (estado S310).

La utilización explicada contempla el poder tener billetes digitales reutilizables durante un tiempo limitado, o para un número de usos autorizados.

Referencias

[BBS04]

D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In M. K. Franklin, editor, *CRYPTO*, volume 3152 of *Lecture Notes in Computer Science*, pages 41-55. Springer, 2004.

[BB04]

D. Boneh and X. Boyen. Short signatures without random oracles. In Advances in Cryptology – EUROCRYPT 2004, volume 3027 of *Lecture Notes in Computer Science*, pages 56-73. Springer, 2004.

REIVINDICACIONES

1.- Método para realizar transacciones con billetes digitales, conteniendo dicho billete digital:

un identificador enlazado directa o indirectamente a unas condiciones de contrato;

una prueba de validez creada por el emisor de dicho billete digital, y

una información relativa al derecho de uso de un usuario que ha adquirido dicho billete digital,

estando caracterizado el método por comprender al menos una transmisión de dicho billete digital entre usuarios: usuario propietario UP y usuario receptor UR, con una transferencia segura de dicho derecho de uso, mediante las siguientes etapas:

a. envío por parte de dicho UP de una oferta de transacción relativa a un billete digital;

b. verificación de la prueba de validez de dicho billete digital por parte de dicho UR;

c. generación por dicho UR de una petición de transferencia del billete digital a dicho UP;

d. verificación de dicha petición de transferencia del billete digital por parte de dicho UP y generación por dicho UP de una aceptación de transferencia;

e. verificación por dicho UR de dicha aceptación de transferencia; y

f. transferencia por dicho UP del billete digital adquiriendo dicho UR el citado derecho de uso de dicho UP.

2.- Método según la reivindicación 1, en donde dicho identificador contiene la fecha de emisión del billete digital y dicha prueba de validez consiste en una firma digital de dicho emisor que garantiza autenticidad, no repudio e integridad de dicho billete digital.

3.- Método según la reivindicación 1, en donde dicho derecho de uso es una vinculación entre dicho identificador del billete digital y dicho UP realizada mediante una firma digital de dicho UP o un certificado digital de dicho UP.

4.- Método según la reivindicación 1, en donde dicho derecho de uso es una vinculación entre dicho identificador del billete digital y dicho UP realizada mediante una primera firma digital de grupo que proporciona un anonimato revocable a dicho UP.

5.- Método según la reivindicación 4, en donde en dicha transmisión se realiza una segunda firma digital de grupo por parte de dicho UP que se enlaza con dicha primera firma digital de grupo proporcionando una garantía acerca de que UP es el que transfiere dicho billete digital preservando su anonimato.

6.- Método según la reivindicación 2, en donde dicha verificación de dicha prueba de validez consiste en la verificación de dicha firma digital de dicho emisor.

7.- Método según la reivindicación 3, el cual incluye una etapa adicional consistente en proporcionar por parte de dicho UP una prueba de su derecho de uso del billete digital a dicho UR, que prueba dicha vinculación entre identificador y UP.

8.- Método según la reivindicación 1, caracterizado porque dicha información relativa al derecho de uso de un usuario que ha adquirido dicho billete digital contiene datos acerca de transferencias anteriores y porque comprende una etapa adicional de verificación de dichas transferencias anteriores por parte de dicho UR.

9.- Método según la reivindicación 1, caracterizado porque dicho billete digital ha sido obtenido mediante las siguientes etapas:

g. generar un precontrato a partir de una petición de billete digital por parte de dicho UP mediante una firma digital de dicho emisor;

h. verificar dicho precontrato por parte de dicho UP;

i. aceptar dicho precontrato creando una vinculación entre UP y dicho billete digital; y

j. emitir dicho billete digital mediante una firma digital del emisor.

10.- Método según la reivindicación 9, caracterizado porque la vinculación de la citada etapa i) se realiza mediante una firma digital de UP.

11.- Método según la reivindicación 9, caracterizado porque la vinculación de la citada etapa i) se realiza mediante una firma de grupo de UP.

12.- Método según la reivindicación 9, caracterizado porque la vinculación de la citada etapa i) se realiza mediante la inclusión de un certificado digital de UP.

13.- Método según la reivindicación 11 o 12, caracterizado porque comprende una etapa adicional de verificación de dicha firma digital.

14.- Método según la reivindicación 2, caracterizado porque dicho billete digital susceptible de ser transferido es verificado por un proveedor de servicio mediante las siguientes etapas:

k) dicho UR presenta o envía dicho billete digital transferido a dicho proveedor;

l) dicho proveedor verifica dicha prueba de validez mediante la comprobación de la firma digital de dicho emisor.

15.- Método según la reivindicación 8, caracterizado porque dicho billete digital susceptible de ser transferido es verificado por un proveedor de servicio mediante las siguientes etapas:

m) dicho UR presenta o envía dicho billete digital transferido a dicho proveedor;

n) dicho proveedor verifica dicha prueba de validez mediante la comprobación de la firma digital de dicho emisor; y

o) dicho proveedor verifica dichas transferencias anteriores.

16.- Método según una cualquiera de las reivindicaciones 14 o 15, caracterizado por incluir una etapa adicional consistente en proporcionar dicho UR una prueba de su derecho de uso del billete digital a dicho proveedor, que prueba dicha vinculación entre identificador enlazado a unas condiciones de contrato y UR.

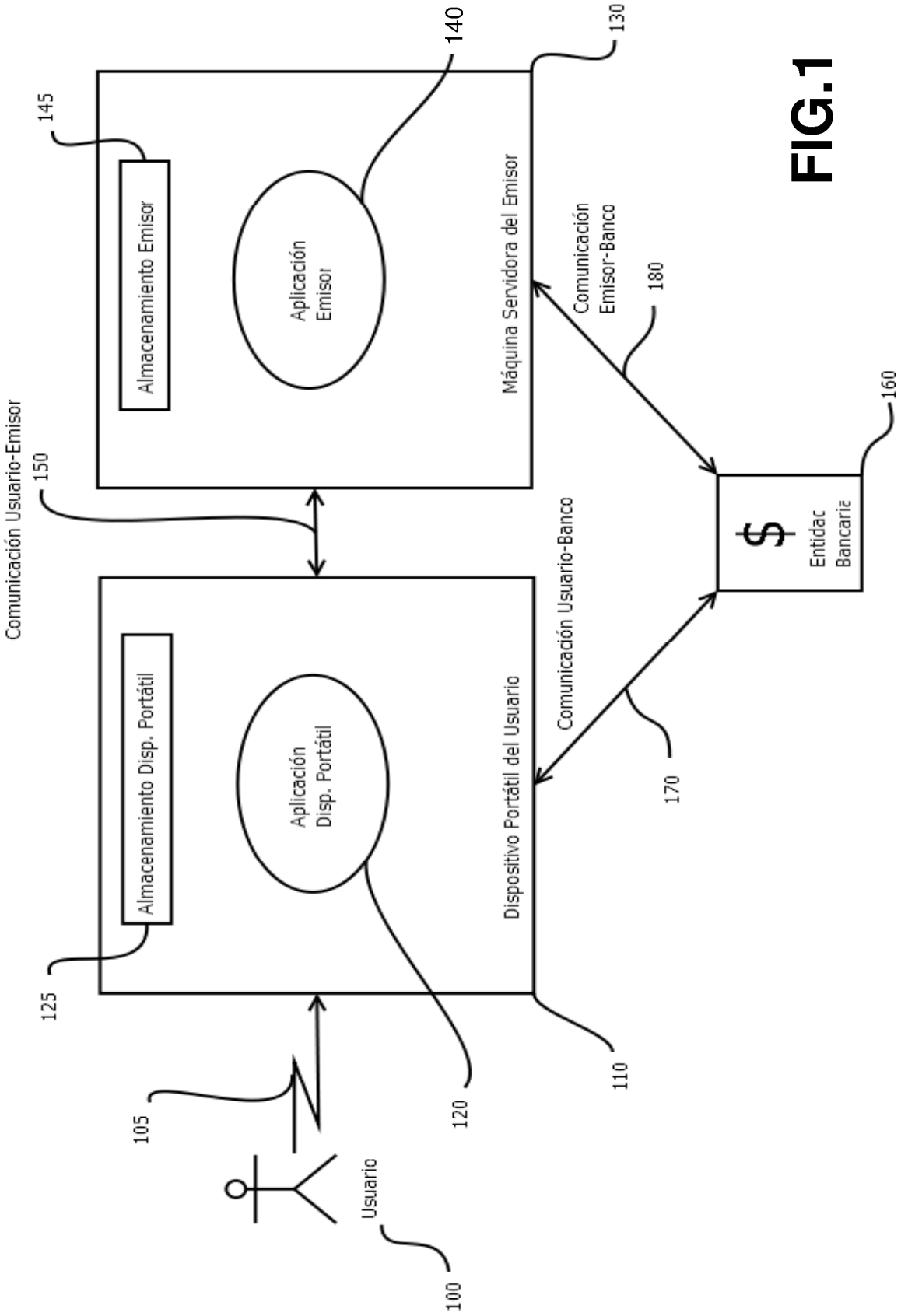
Usuario
100
105
Dispositivo Portátil del Usuario
110
Aplicación Disp. Portátil
120
Almacenamiento Disp. Portátil
125
Comunicación Usuario-Emisor
150
Máquina Servidora del Emisor
130
Aplicación Emisor
140
Almacenamiento Emisor
145
Comunicación Usuario-Banco
170
Comunicación Emisor-Banco
180
Entidad Bancaria
160

FIG.1

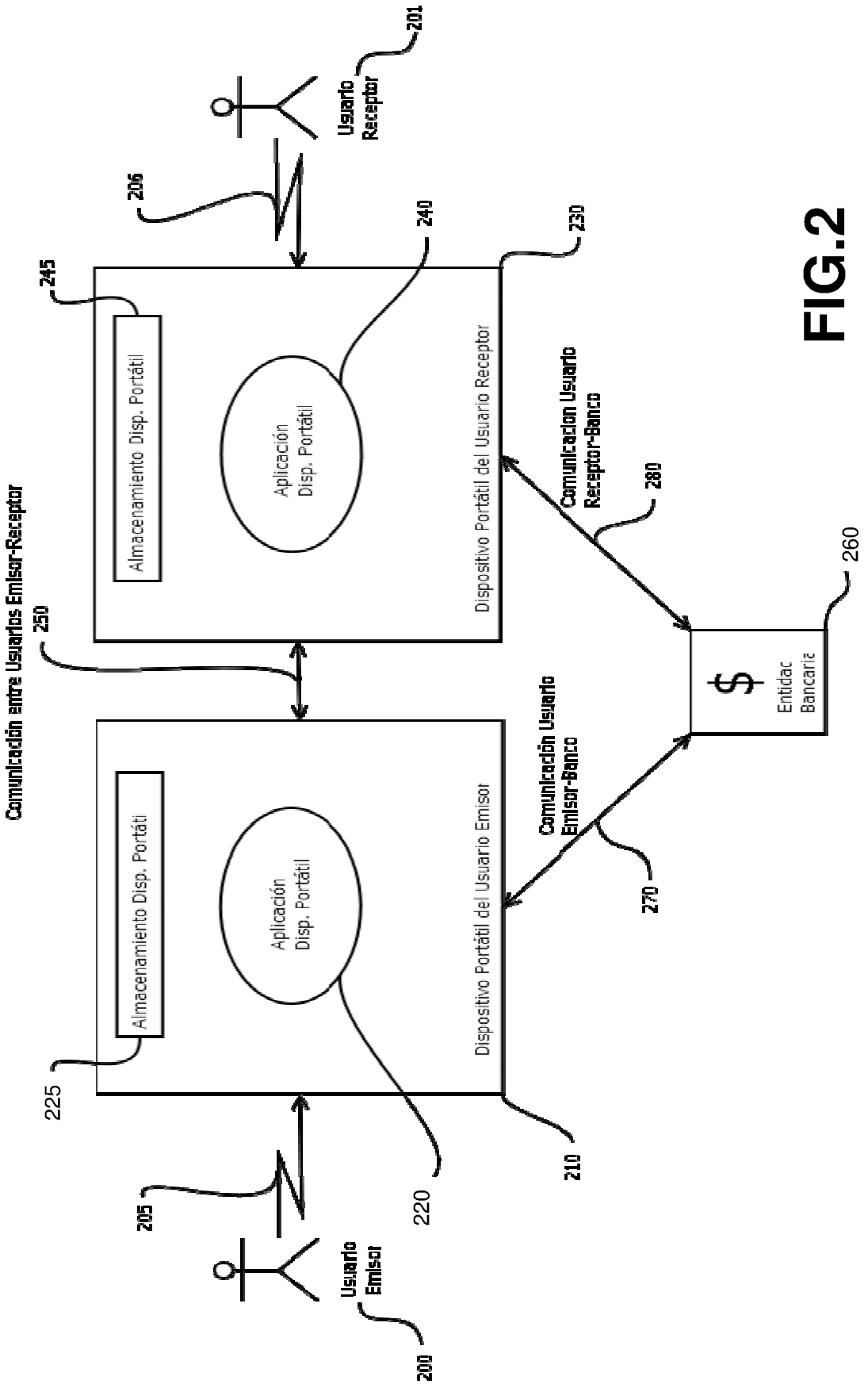
Comunicación entre Usuarios Emisor-Receptor
Usuario Emisor
200
205
Usuario Receptor
201
206
Almacenamiento Disp. Portátil
225
Aplicación Disp. Portátil
220
Dispositivo Portátil del Usuario Emisor
210
Almacenamiento Disp. Portátil
245
Aplicación Disp. Portátil
240
Dispositivo Portátil del Usuario Receptor
230
250
Comunicación Usuario Emisor-Banco
270
Comunicación Usuario Receptor-Banco
280
$
Entidad Bancaria
260

FIG.2

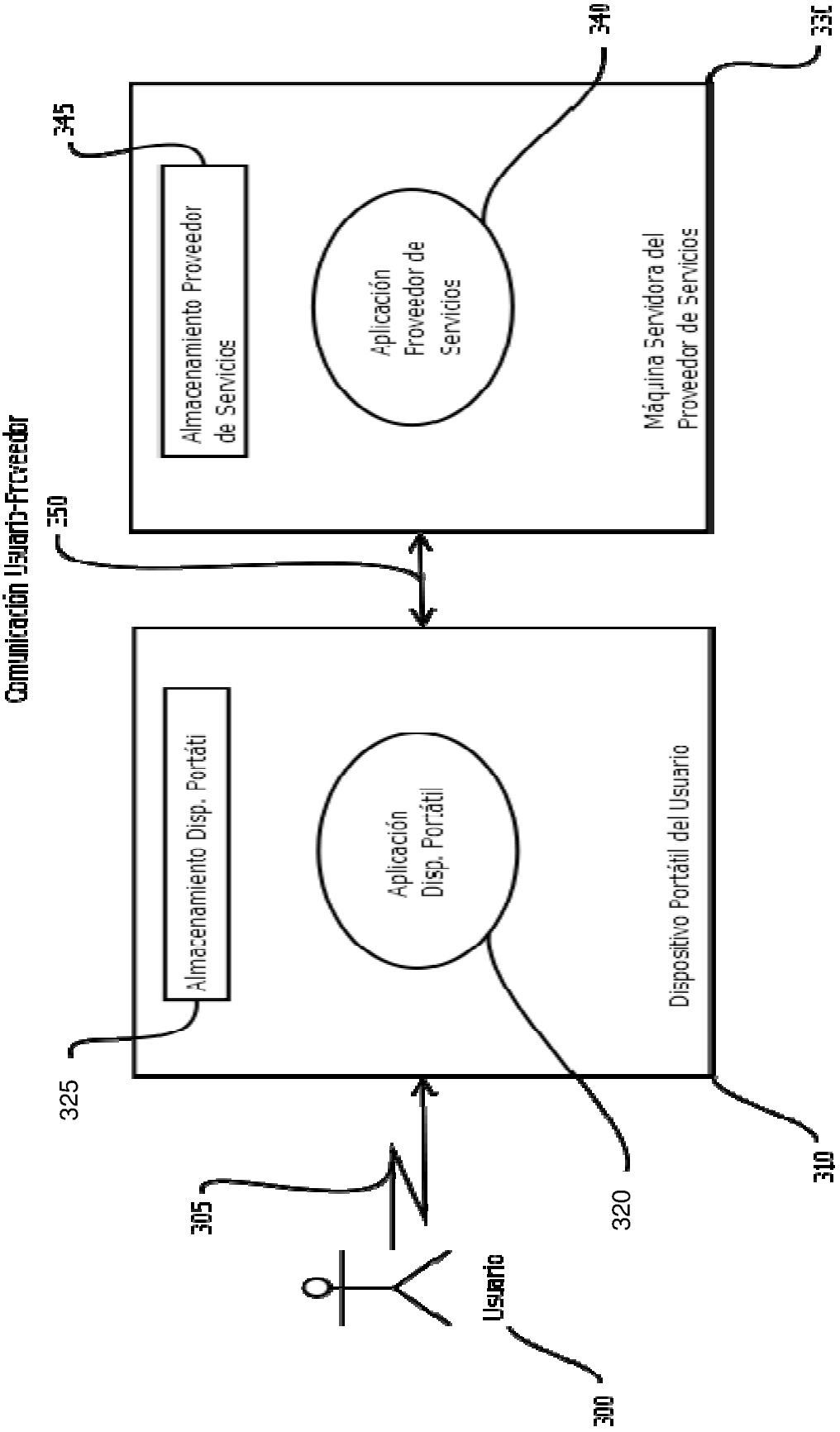
Comunicación Usuario-Proveedor
350
345
Almacenamiento Proveedor de Servicios
Aplicación Proveedor de Servicios
340
Máquina Servidora del Proveedor de Servicios
335
325
Almacenamiento Disp. Portáti
Aplicación Disp. Portátil
Dispositivo Portátil del Usuario
310
305
320
Usuario
300

FIG.3

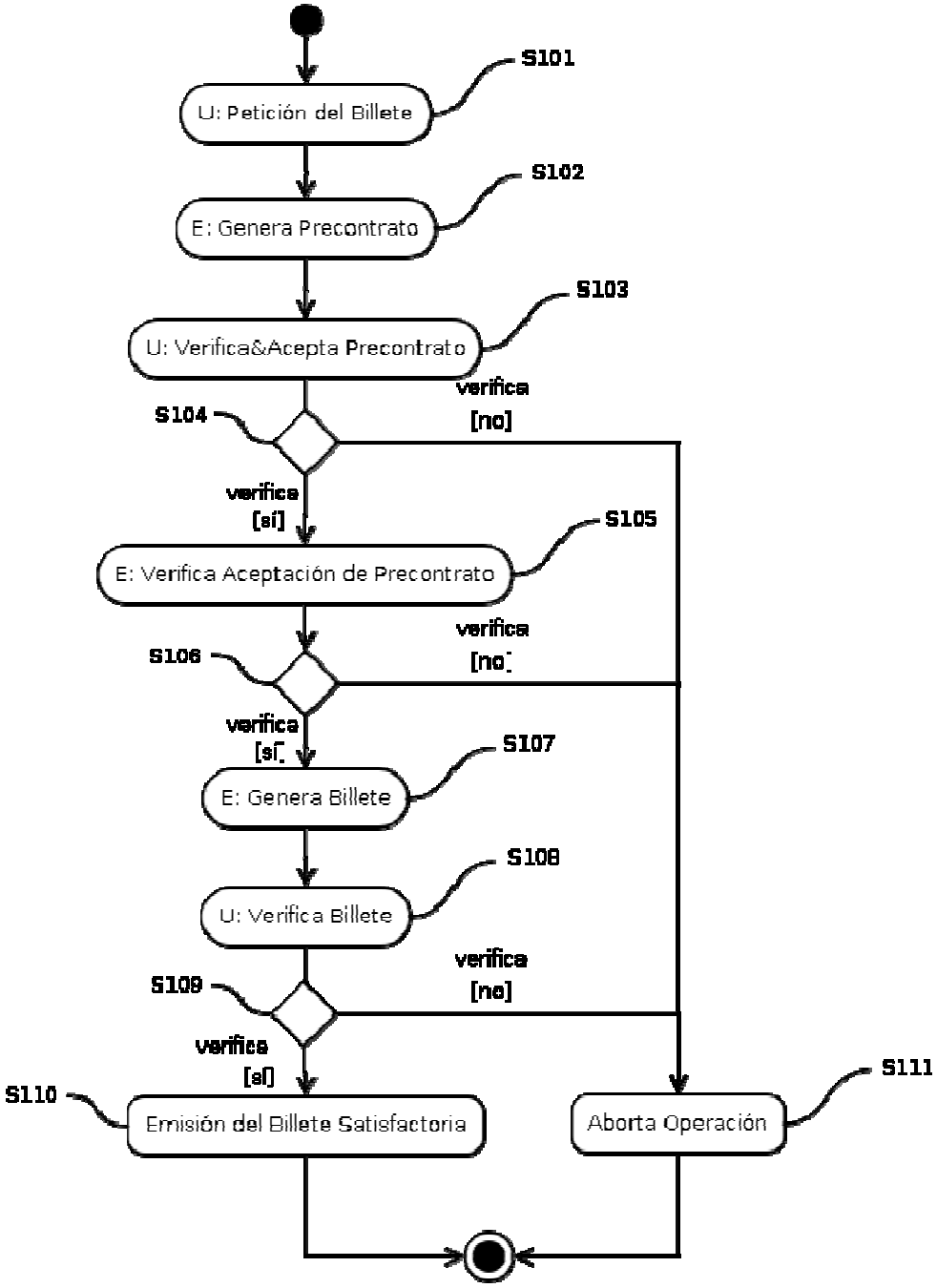
S101
U: Petición del Billete
S102
E: Genera Precontrato
S103
U: Verifica&Acepta Precontrato
verifica
[no]
S104
verifica
[sí]
S105
E: Verifica Aceptación de Precontrato
verifica
[no]
S106
verifica
[sí]
S107
E: Genera Billete
S108
U: Verifica Billete
verifica
[no]
S109
verifica
[sí]
S110
Emisión del Billete Satisfactoria
S111
Aborta Operación

FIG.4

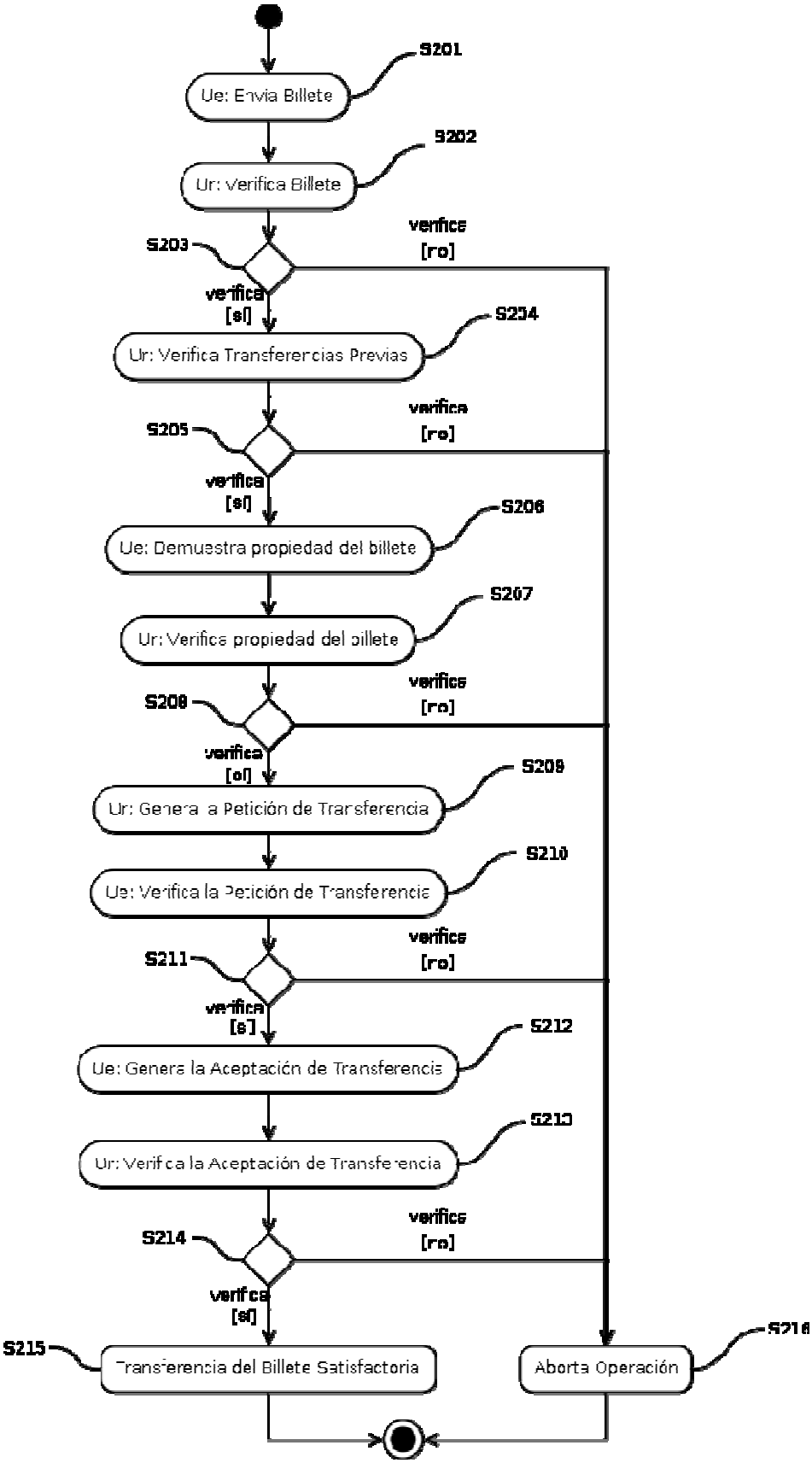
S201
Ue: Envia Billete
S202
Ur: Verifica Billete
S203
verifica
[ro]
verifica
[si]
S204
Ur: Verifica Transferencias Previas
S205
verifica
[ro]
verifica
[si]
S206
Ue: Demuestra propiedad del billete
S207
Ur: Verifica propiedad del billete
S208
verifica
[ro]
verifica
[si]
S209
Ur: Genera la Petición de Transferencia
S210
Ue: Verifica la Petición de Transferencia
S211
verifica
[ro]
verifica
[si]
S212
Ue: Genera la Aceptación de Transferencia
S213
Ur: Verifica la Aceptación de Transferencia
S214
verifica
[ro]
verifica
[si]
S215
Transferencia del Billete Satisfactoria
S216
Aborta Operación

FIG.5

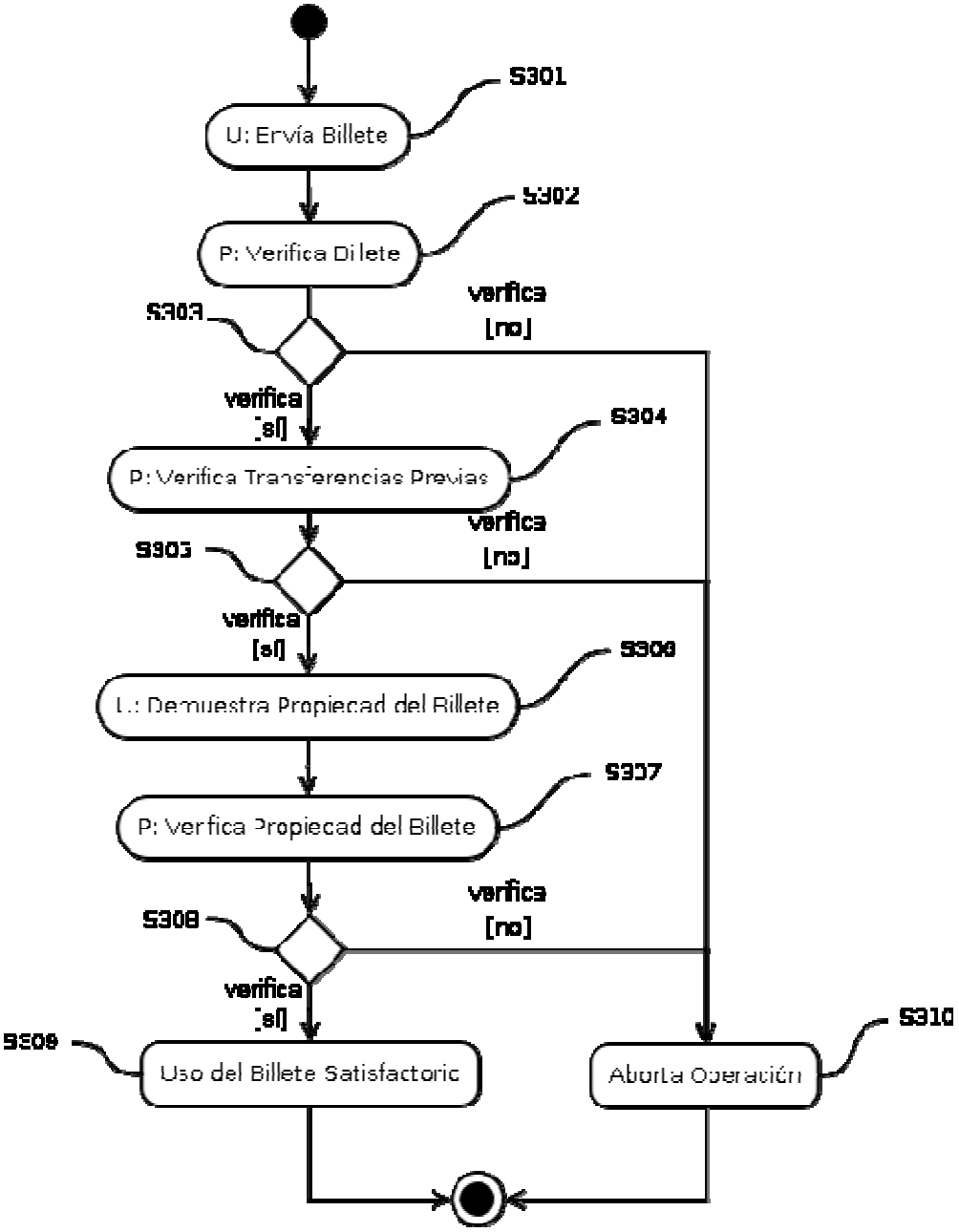
S301
U: Envía Billete
S302
P: Verifica Billete
S303
verifica
[no]
verifica
[si]
S304
P: Verifica Transferencias Previas
verifica
[no]
S305
verifica
[si]
S306
U: Demuestra Propiedad del Billete
S307
P: Verfica Propiedad del Billete
verifica
[no]
S308
verifica
[si]
S309
Uso del Billete Satisfactorio
Aborta Operación
S310

FIG.6