(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 449 190**

(21) Número de solicitud: 201200837

(51) Int. CI.:

H04L 9/32 (2006.01)
G06Q 20/32 (2012.01)

(12) SOLICITUD DE PATENTE A2

(22) Fecha de presentación:

21.08.2012

(43) Fecha de publicación de la solicitud:

18.03.2014

(71) Solicitantes:

BANKINTER S.A (50.0%)
Paseo de la Castellana, 29
28049 Madrid ES y
SEGLAN, S.L. (50.0%)

(72) Inventor/es:

PÉREZ LAFUENTE, Carlos Alberto y
GARCÍA MURGA, Imanol

(74) Agente/Representante:

LORENTE BERGES, Ana

(54) Título: **Método y sistema para habilitar ticketing/pagos móviles sin contacto por medio de una aplicación de teléfono móvil**

(57) Resumen:

La invención se refiere a un método para el ticketing/pagos móviles sin contacto utilizando una aplicación disponible en el teléfono móvil donde cada credencial preparada está unívocamente asociada al teléfono móvil del usuario registrado y a un código de activación, y habilita parcialmente el teléfono móvil para el acceso a ticketing sin contacto, en caso de credenciales de ticketing, o para pagos móviles sin contacto, en caso de credenciales de pagos; donde la habilitación del teléfono móvil para cada acceso a ticketing sin contacto o pago móvil sin contacto también requiere que el usuario inserte un número de identificación personal en la aplicación de ticketing/pagos del teléfono móvil; y donde el módulo de servidor de ticketing/pagos envía las credenciales al teléfono móvil del usuario registrado después de validar con éxito una contraseña de un solo uso (OTP) recibida desde la aplicación de ticketing/pagos del teléfono móvil.

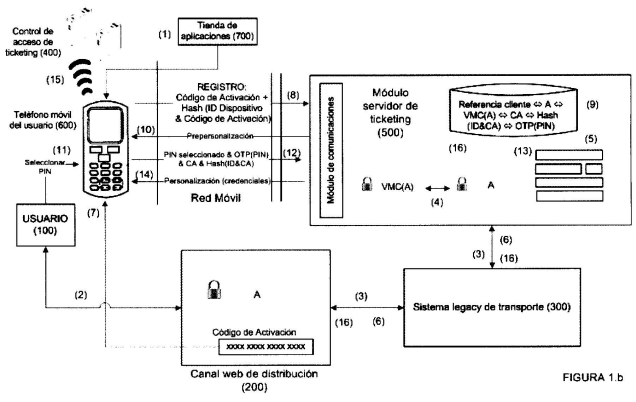

FIGURA 1.b

ES 2 449 190 A2

DESCRIPCIÓN

Método y sistema para habilitar ticketing/pagos móviles sin contacto por medio de una aplicación de teléfono móvil

Esta invención se refiere a un método para ticketing/pagos móviles sin contacto utilizando una aplicación disponible en el teléfono móvil. Esta invención se refiere también a un sistema, un servidor y un teléfono móvil adecuados para llevar a cabo dicho método.

ANTECEDENTES

El desarrollo de soluciones para ticketing utilizando tarjetas inteligentes ha tenido un crecimiento significativo a lo largo de la última década en un número significativo de mercados. El paso desde tarjetas inteligentes de contacto a tarjetas inteligentes sin contacto para aplicaciones relativas a ticketing comenzó hace años, mientras que el uso de teléfonos móviles dotados de NFC (*Near Field Communications, o Comunicación de Campo Cercano)* para aplicaciones de ticketing está actualmente en una etapa inicial.

Los pagos lideran mundialmente el número de iniciativas NFC, aunque existe aún cierta incertidumbre con relación al tiempo necesario para que los establecimientos comerciales cuenten de forma generalizada con terminales Punto de Venta sin contacto.

El creciente número de teléfonos móviles dotados de NFC hace que los proveedores de servicios y las empresas relacionadas con el ecosistema NFC ambicionen un prometedor canal y negocio de ticketing/pagos a través del teléfono móvil. Es indudable que el teléfono móvil ofrece al usuario, en comparación con soluciones basadas en tarjetas inteligentes sin contacto, una experiencia mejorada en términos de interfaz de usuario y aprovisionamiento remoto.

Las soluciones móviles sin contacto más conocidas para ticketing/pagos se

denominan "basadas en SIM", lo que significa que una aplicación de transporte/pagos y unas credenciales de usuario son almacenados en un elemento seguro tarjeta SIM, que pertenece al correspondiente operador de telecomunicaciones. En este contexto, los proveedores de servicios de transporte/pagos están obligados a llegar a un acuerdo con el operador de telecomunicaciones para proporcionar los servicios de ticketing/pagos NFC. Como consecuencia, los proveedores de servicios de transporte/pagos pueden ver limitado el modo en que proporcionan sus propios servicios a través del teléfono móvil ya que, con esta solución, parte del servicio es proporcionado dentro del dominio del operador de telecomunicaciones.

Por tanto, puede ser interesante para los proveedores de servicios tener acceso a nuevas soluciones seguras que puedan estar plenamente disponibles dentro del dominio de la propia entidad de transporte/pagos, pero que a la vez presenten todos los beneficios que proporciona el ticketing/pagos sin contacto basados en el uso de teléfonos móviles NFC.

DESCRIPCIÓN DE LA INVENCIÓN

Por tanto, un objeto de la invención es dotar a los proveedores de servicios de transporte/pagos de un método seguro que pueda llevarse a cabo completamente dentro de su propio dominio, permitiéndoles así continuar manteniendo un control completo del servicio en cuanto a posicionamiento de marca, negocio y aprovisionamiento para ticketing/pagos móviles NFC, evitando restricciones de terceras partes.

Este objeto se consigue de acuerdo con la reivindicación 1 proporcionando un método para habilitar ticketing/pagos móviles sin contacto a través de una aplicación de teléfono móvil, comprendiendo el método los siguientes pasos:

(a) Un usuario paga al proveedor de servicios por ciertos servicios de ticketing/pagos.

(b) Asociado al pago y a un correspondiente derecho concedido para utilizar los servicios de ticketing/pagos correspondientes, un módulo

servidor de ticketing/pagos prepara credenciales de ticketing/pagos para su uso por el usuario y las envía al teléfono móvil del usuario.

(c) El teléfono móvil del usuario recibe las credenciales y las almacena para su uso en el sistema de ticketing para transporte sin contacto, en caso de credenciales de ticketing, o para su uso en pagos móviles sin contacto, en caso de credenciales de pagos.

Dicho método está caracterizado porque cada credencial está unívocamente asociada al teléfono móvil del usuario registrado y a un código de activación, y habilita parcialmente el teléfono móvil para el acceso a ticketing sin contacto, en caso de credenciales de ticketing, o a pagos móviles sin contacto, en caso de credenciales de pagos; donde la habilitación del teléfono móvil para cada acceso a ticketing sin contacto (o pago móvil sin contacto) también requiere que el usuario inserte un Número de Identificación Personal (PIN, Personal Identification Number) en la aplicación de ticketing/pagos del teléfono móvil; y donde el módulo servidor de ticketing/pagos envía credenciales al teléfono móvil del usuario registrado después de una validación correcta de una Contraseña de un Solo Uso (OTP, One Time Password) recibida desde la aplicación de ticketing/pagos del teléfono móvil.

De acuerdo con la presente invención, sólo los usuarios registrados pueden obtener credenciales de ticketing/pagos después del pago, y el uso de dichas credenciales está asociado al teléfono móvil seleccionado durante el proceso de registro (y a un código de activación) y a un Número de Identificación Personal elegido por el usuario, de modo que se requiere una autenticación de dos factores. Además, las credenciales sólo se envían a la aplicación del teléfono móvil del usuario registrado después de verificar una OTP generada por dicha aplicación del teléfono móvil después de la interacción con el usuario, de modo que el proceso de descarga de credenciales está adecuadamente controlado por el usuario y por el proveedor de servicios de transporte/pagos.

El módulo servidor de ticketing/pagos puede estar incluido al menos parcialmente en los medios de procesamiento de datos del proveedor de

servicios. Todo o parte del mismo puede pertenecer o ser operado por un proveedor externo fiable del proveedor de servicios. Como ejemplo, varios proveedores de servicios de transporte pueden compartir un módulo servidor de ticketing común simplemente llegando a un acuerdo entre ellos, evitando así la complejidad de soluciones basadas en tarjeta SIM en términos de acuerdos adicionales con operadores de telecomunicaciones.

En una realización particular, el módulo servidor de ticketing/pagos divide el derecho concedido de ticketing/pagos en varias particiones y genera una credencial independiente para cada una de dichas particiones.

En una realización particular, se envía un primer conjunto de credenciales a la aplicación del teléfono móvil, y se envían nuevas credenciales a la aplicación del teléfono móvil a medida que sucesivamente sean solicitadas desde el dispositivo móvil del usuario, hasta llegar al límite del derecho concedido relativo al uso de los servicios de ticketing/pagos. Así, el sistema puede monitorizar y limitar en cualquier momento el número de credenciales disponibles en el teléfono móvil para ticketing/pagos.

En una realización particular, al menos una credencial es deshabilitada en, o eliminada de, la aplicación del teléfono móvil mediante el envío de un mensaje de deshabilitación (o eliminación) desde el módulo servidor de ticketing/pagos a la aplicación del teléfono móvil del usuario.

En otra realización particular, el derecho a utilizar servicios de ticketing/pagos puede ser extendido si el usuario paga por ello, de modo que se pueden generar dinámicamente nuevas particiones de derechos de ticketing/pagos en el módulo de servidor ticketing/pagos.

En otra realización particular, la aplicación del teléfono móvil limita la solicitud de nuevas credenciales basándose en información acerca de las credenciales que ya están almacenadas en el teléfono móvil. De modo que si, por ejemplo, el número de credenciales está por debajo de un umbral, se recuerda al

usuario que es necesaria conectividad de datos para tener disponibles nuevas credenciales.

En una realización particular, las credenciales de ticketing/pagos son bloqueadas en la aplicación del teléfono móvil después de la introducción errónea del Número de Identificación Personal un determinado número de veces, y se envía un mensaje de advertencia al módulo servidor de ticketing/pagos.

En una realización particular, el módulo servidor de ticketing/pagos bloquea el derecho de ticketing/pagos concedido después de un determinado número de verificaciones erróneas de una OTP recibida desde la aplicación del teléfono móvil, y se envía un mensaje de bloqueo de credenciales a la aplicación del teléfono móvil.

Así, la entidad de transporte/pagos puede monitorizar inserciones erróneas de PIN que ocurren justo antes de un acceso a servicios de ticketing / intento de pago y aquellas que se producen dentro de un proceso de renovación de credenciales.

En una realización particular para transacciones on-line de pagos móviles sin contacto, una segunda parte de la credencial es calculada por la propia aplicación del teléfono móvil utilizando el valor de la transacción y el PIN del usuario como entradas para generar un resultado OTP (que constituye la segunda parte de la credencial). La primera y la segunda parte de la credencial se utilizan para la transacción móvil sin contacto, y es necesaria la verificación de dicha OTP por el módulo servidor de pagos para aceptar o denegar la transacción. De ese modo, al aprovechar la ventaja de que el valor de la transacción es conocido por el banco emisor durante el proceso de la transacción online, el reto para esta OTP puede utilizarlo y todavía ser verificado como parte del proceso de autorización online.

La solicitud de patente WO 03/038719 describe un método donde una tarjeta

financiera virtual de un solo uso es generada offline para su uso para un pago por internet o una transacción sin contacto de tipo EMV-MSD (datos de banda magnética). Sin embargo, dicha solución no se puede utilizar para generar una tarjeta financiera virtual de un solo uso para una transacción sin contacto de tipo EMV chip & PIN debido al hecho de que se debe calcular una clave derivada en el lado del servidor y enviarla a la aplicación del teléfono móvil antes del intento de pago (para evitar almacenar la clave del emisor en el teléfono móvil); así, la generación de una tarjeta financiera virtual de un solo uso para una transacción sin contacto de tipo EMV chip & PIN requiere manejar un proceso on/off line para cada tarjeta generada. La última realización descrita anteriormente cumple con el requisito de la actualización online, pero ventajosamente también asocia una segunda parte de la credencial generada offline en el móvil al valor de la transacción y al PIN del usuario, creando así una solución de pago conveniente y muy robusta.

De acuerdo con la presente invención, se proporciona además un sistema para habilitar ticketing/pagos móviles sin contacto a través de una aplicación del teléfono móvil, comprendiendo dicho sistema:

- medios de registro para registrar usuarios en servicios de ticketing/pagos,
- medios de pago para permitir a un usuario pagar por servicios de ticketing/pagos,
- medios de generación de credenciales preparar en el módulo servidor de ticketing/pagos, basándose en unos derechos de ticketing/pagos concedidos, unas credenciales de ticketing/pagos para su uso por el usuario registrado; y medios de transmisión para enviarlos al teléfono móvil del usuario registrado; y medios de recepción y almacenamiento para recibir en el teléfono móvil las credenciales y almacenarlas para su uso en un sistema de ticketing para transporte sin contacto o, en caso de credenciales de pago, para su uso en pagos móviles sin contacto.

caracterizado porque dicho sistema comprende medios de procesamiento para asociar unívocamente cada credencial, que habilita parcialmente el teléfono

móvil para el acceso a ticketing sin contacto o para pagos móviles sin contacto, al teléfono móvil del usuario registrado y a un código de activación; medios de procesamiento y comprobación que permiten habilitar el teléfono móvil para el acceso a ticketing sin contacto o para pagos móviles sin contacto, que está también basada en la inserción por parte del usuario de un Número de Identificación Personal (PIN) en la aplicación de ticketing/pagos del teléfono móvil; medios de procesamiento y trasmisión en la aplicación de ticketing/pagos del teléfono móvil para calcular una OTP y enviarla al módulo servidor de ticketing/pagos; y medios de procesamiento y verificación en el módulo servidor de ticketing/pagos para validar la OTP recibida.

BREVE DESCRIPCIÓN DE LAS FIGURAS

En la siguiente descripción detallada de algunas realizaciones, aparecerán otras características y ventajas, y cada descripción hace referencia a las siguientes figuras:

La Figura 1.a es un diagrama esquemático que ilustra generalmente los principales bloques funcionales de la invención, como una extensión de un sistema de transporte legacy;

La Figura 1.b es un diagrama esquemático que ilustra una realización de un sistema de ticketing de acuerdo con la invención;

La Figura 1.c es un diagrama esquemático que ilustra otra realización de un sistema de ticketing de acuerdo con la invención;

La Figura 2.a es un diagrama esquemático que ilustra en general los principales bloques de la invención como una extensión de un sistema de pagos legacy;

La Figura 2.b es un diagrama esquemático que ilustra una realización de un sistema de pago de acuerdo con la invención;

La Fig. 2.c es un diagrama de flujo que ilustra parcialmente una realización de un método de acuerdo con la invención;

DESCRIPCIÓN DETALLADA

La Figura 1.a es un diagrama esquemático que ilustra en general los principales bloques funcionales de la invención como una extensión de un sistema legacy de transporte; esta figura muestra un sistema legacy 300a de transporte de un proveedor de servicios que soporta tarjetas inteligentes sin contacto (de modo que un usuario de este sistema puede utilizar una tarjeta inteligente sin contactos para acceder a servicios de transporte a través de dispositivos 400a de control de acceso de ticketing). Utilizando el canal 200a web de distribución, los usuarios pueden contratar al menos un servicio, para obtener al menos un título de transporte (perfil) asociado a dicho al menos un servicio y cargar/recargar el al menos un título de transporte. En este ejemplo general, el canal web de distribución pertenece a un banco asociado y el usuario es también cliente de ese banco, de modo que puede pagar a través de la página web utilizando medios de firma electrónica proporcionados por el banco.

Cuando el usuario solicita, a través del canal web de distribución, los servicios móviles de ticketing de la presente invención (y paga por ellos de acuerdo con un método acordado entre, por ejemplo, el banco referido y el proveedor de servicios de ticketing), el sistema legacy de transporte reenvía la solicitud al módulo 500a servidor de ticketing de la invención. Los bloques funcionales principales de este módulo se ilustran en esta figura.

La Figura 1.b muestra más detalles acerca de los bloques funcionales de la figura 1.a, y es un diagrama esquemático que ilustra una realización de un sistema de ticketing de acuerdo con la invención para habilitar servicios de ticketing móvil sin contacto a través de una aplicación en el teléfono móvil. La figura 1.b muestra el proceso desde el registro del usuario para servicios de

ticketing móvil hasta la provisión de dichos servicios.

En el paso (1), el usuario se descarga la aplicación de ticketing para el teléfono móvil, desde una tienda 700 de aplicaciones a su teléfono móvil dotado de tecnología sin contacto.

En el contexto de la invención, el usuario paga por ciertos servicios de ticketing solicitados al proveedor de servicios. En el paso (2) de esta realización, el usuario solicita servicios de ticketing a través de un canal web de distribución y confirma el pago a través de este medio (por ejemplo, la misma situación que la descrita en la figura 1.a; el canal web de distribución pertenece a un banco asociado). En el paso (3), la solicitud es enviada al sistema legacy de transporte y después reenviada al módulo servidor de ticketing. En esta realización, el módulo de registro del módulo servidor de ticketing recibe en el paso (3) una referencia de cliente y una referencia de derecho de transporte. Asociado al pago y al correspondiente derecho concedido para utilizar ciertos servicios de ticketing, un módulo servidor de ticketing prepara credenciales de ticketing para su uso por el usuario registrado y las envía al teléfono móvil del usuario registrado, como se describe con mayor detalle a continuación.

En el paso (4) el módulo de registro del módulo servidor de ticketing asigna un derecho de transporte al usuario (representado en la fig. 1.b como tarjeta "A" en el módulo servidor), basándose en la referencia de derecho de transporte recibida, y esa información se almacena en la base de datos del módulo servidor de ticketing (referencia de cliente ⇔ A). Luego, el módulo de registro solicita al módulo de credenciales de usuarios que genere una única credencial (representada en la fig. 1.b como tarjeta “VMC(A)" en el módulo servidor) y ésta queda vinculada a la referencia de cliente de transporte y al derecho de transporte en la base de datos del módulo servidor de ticketing (referencia de cliente ⇔ A ⇔ VMC(A)). La credencial generada tiene una fecha de caducidad, de modo que no puede ser utilizada pasada dicha fecha.

En el paso (5), el módulo de credenciales de usuarios solicita al módulo de

seguridad un código de activación; de modo que el módulo de seguridad genera un código de activación con una fecha de caducidad determinada y éste se almacena en la base de datos del módulo servidor de ticketing (referencia de cliente ⇔ A ⇔ VMC(A) ⇔ CA). Un código de activación no puede utilizarse después de la expiración de su fecha de caducidad. En el paso (6), el código de activación es enviado desde el módulo de registro al sistema legacy de transporte, reenviado al canal web de distribución y mostrado al usuario.

En el paso (7), el usuario inserta el código de activación en la aplicación de ticketing del teléfono móvil, y en el paso (8) el teléfono móvil envía al módulo de seguridad del módulo servidor de ticketing, por ejemplo vía https, el [código de activación y el hash (número de identificación del teléfono móvil & código de activación)].

En el paso (9), el módulo de seguridad comprueba si código de activación es correcto; en caso afirmativo, el módulo de seguridad almacena el valor del hash en la base de datos del módulo servidor de ticketing, de modo que los vínculos quedan como sigue: referencia de cliente ⇔ A ⇔ VMC(A) ⇔ CA ⇔ hash (ID&CA).

En el paso (10), la tarjeta "A" es pre-personalizada en la aplicación del teléfono móvil.

La pre-personalización hace referencia al paso anterior a la personalización; y la pre-personalización/personalización de la tarjeta "A" hace referencia a la pre-personalización/personalización de la aplicación de ticketing del teléfono móvil sin contacto de la invención para que funcione en "modo de emulación de tarjeta" para servicios móviles de ticketing sin contacto, de un modo equivalente a una aplicación de ticketing basada en SIM funcionando en "modo de emulación de tarjeta" para servicios móviles de ticketing sin contacto (por ejemplo, emulando la tecnología subyacente de mifare DESFIRE). La personalización completa de la tarjeta "A" en la aplicación de ticketing del teléfono móvil requiere la descarga de credenciales desde el módulo servidor

de ticketing a la aplicación de ticketing del teléfono móvil, como se describe con detalle a continuación.

Cuando el paso (10) termina, el usuario ya está registrado en el sistema de la invención, pero aún está pendiente la recepción de credenciales en la aplicación de ticketing del teléfono móvil. En esta etapa, cada credencial está asociada de manera unívoca al teléfono móvil del usuario registrado y a un código de activación, y habilita parcialmente el teléfono móvil para el acceso a ticketing sin contacto.

En el paso (11), se solicita al usuario que seleccione un Número de Identificación Personal (PIN) para los servicios de ticketing móvil sin contacto. El valor del PIN no se almacena en la aplicación de ticketing del teléfono móvil, sino que se envía de manera segura en el paso (12) al módulo de seguridad del módulo servidor de ticketing, junto con una Contraseña de un Solo Uso (OTP) calculada utilizando el valor del PIN (y los valores del Código de Activación y el hash (CA&ID), para ser capaz de asignar en el módulo servidor de ticketing el PIN seleccionado y la OTP resultante a la referencia de cliente correcta).

En el paso (13), el módulo de seguridad almacena el PIN en la base de datos del módulo servidor de ticketing, junto con las claves y parámetros para calcular un resultado OTP basado en el PIN. Todo este almacenamiento se indica en la base de datos de la figura 1.b como datos "OTP(PIN)". De modo que los vínculos y almacenamiento en la base de datos son ahora los siguientes: referencia de cliente ⇔ A ⇔ VMC(A) ⇔ CA ⇔ hash (ID&CA) ⇔ OTP(PIN).

Todavía en el paso (13), el módulo servidor de ticketing calcula un resultado OTP utilizando el PIN del usuario y las claves y parámetros OTP almacenados, y compara el resultado con el recibido en el módulo de seguridad desde la aplicación de ticketing del teléfono móvil. Si la validación tiene éxito, entonces se pueden enviar credenciales de ticketing desde el módulo de credenciales de

usuarios a la aplicación de ticketing del teléfono móvil. De ese modo, el módulo servidor de ticketing envía credenciales al teléfono móvil del usuario registrado después de la validación con éxito de una Contraseña de un Solo Uso (OTP) recibida desde la aplicación de ticketing del teléfono móvil.

En el paso (14), las credenciales de ticketing son enviadas a la aplicación de ticketing del teléfono móvil; el teléfono móvil del usuario recibe las credenciales y las almacena para su uso en el sistema de transporte de ticketing sin contacto (de modo que el proceso de personalización de la tarjeta "A" queda entonces completado). En una realización, las credenciales han sido cifradas en el módulo de seguridad utilizando el PIN, de modo que para que la aplicación de ticketing del teléfono móvil pueda utilizar una credencial recibida y almacenada es necesario que el usuario inserte su código PIN.

En el paso (15), el usuario registrado puede utilizar el teléfono móvil para acceder a servicios de transporte. En el paso (15), el usuario debe insertar su código PIN en la aplicación de ticketing del teléfono móvil antes de tratar de acceder al sistema 400 de control de acceso de ticketing; de modo que la habilitación completa del teléfono móvil para cada acceso a ticketing sin contacto también requiere que el usuario inserte un código de identificación personal (PIN) en la aplicación de ticketing del teléfono móvil.

En el paso (16), el módulo de credenciales de usuarios del módulo servidor de ticketing sabe que las credenciales de ticketing han sido recibidas y almacenadas con éxito en la aplicación de ticketing del teléfono móvil (éxito en el paso 14), de modo que se envía la confirmación al distribuidor web, que realiza el cargo final del pago e informa al usuario (por ejemplo, a través de un SMS o una alerta en la página web del distribuidor).

La Figura 1.c es un diagrama esquemático que ilustra otra realización de un sistema de ticketing de acuerdo con la invención, para habilitar servicios de ticketing móvil sin contactos a través de una aplicación en el teléfono móvil; la figura 1.c muestra el proceso desde el registro del usuario para servicios de

ticketing móvil hasta la provisión de dichos servicios.

Esta realización toma como referencia la de la figura 1.b con ciertas variaciones que se describen a continuación. Los pasos (1), (2) y (3) son los mismos que los de la figura 1.b.

Asociado al pago y al correspondiente derecho concedido para utilizar ciertos servicios de ticketing, un módulo servidor de ticketing prepara credenciales de ticketing para su uso por el usuario registrado y las envía al teléfono móvil del usuario registrado, como se explica con mayor detalle a continuación. Sin embargo, en esta realización el módulo servidor de ticketing divide el derecho de ticketing concedido en varias particiones y genera una credencial independiente para cada una de dichas particiones.

De modo que en el paso (4) el módulo servidor de ticketing asigna un derecho de transporte al usuario (representado en la fig. 1.c como tarjeta "A" en el módulo de servidor), vinculado a un conjunto de credenciales (representadas en la fig. 1.c como tarjetas "$VMC(A)_1$" a "$VMC(A)_n$" en el módulo de servidor) y a una referencia de cliente de transporte, y almacena estos vínculos en la base de datos del módulo servidor de ticketing (referencia de cliente $\Leftrightarrow$ A $\Leftrightarrow$ $VMC(A)_i$,i=1...n).

En el paso (5), se genera un código de activación y se almacena en la base de datos del módulo servidor de ticketing (referencia de cliente $\Leftrightarrow$ A $\Leftrightarrow$ $VMC(A)_i$,i=1...n $\Leftrightarrow$ CA). En el paso (6), el Código de Activación es enviado al sistema legacy de transporte, reenviado al canal web de distribución y mostrado al usuario.

Los pasos (7), (8) y (9) son los mismos que en la figura 1.b, de modo que los vínculos después del paso (9) son como sigue: referencia del cliente $\Leftrightarrow$ A $\Leftrightarrow$ $VMC(A)_i$,i=1...n $\Leftrightarrow$ CA $\Leftrightarrow$ hash(ID&CA).

En el paso (10), la tarjeta "A" es pre-personalizada en la aplicación del teléfono

móvil.

Al igual que en la realización 1.b, la pre-personalización hace referencia al paso previo a la personalización; y la pre-personalización/personalización de la tarjeta "A" hace referencia a la pre-personalización/personalización de la aplicación de ticketing móvil sin contacto de la invención para que funcione en "modo de emulación de tarjeta" para servicios de ticketing móvil sin contacto, de un modo equivalente a una aplicación de ticketing basada en SIM funcionando en "modo de emulación de tarjeta" para servicios de ticketing móvil sin contacto. La personalización completa de la tarjeta "A" en la aplicación de ticketing del teléfono móvil requiere la descarga de credenciales desde el módulo servidor de ticketing a la aplicación de ticketing del teléfono móvil, como se describe a continuación.

Cuando termina el paso (10), el usuario ya está registrado en el sistema de la invención, pero aún está pendiente la recepción de credenciales en la aplicación de ticketing del teléfono móvil. En esta etapa, cada credencial está unívocamente asociada al teléfono móvil del usuario registrado y a un código de activación, y habilita parcialmente al teléfono móvil para el acceso a servicios de ticketing sin contacto.

En el paso (11), se solicita al usuario que seleccione un Número de Identificación Personal (PIN) para los servicios de ticketing móvil sin contacto. El valor del PIN no se almacena en la aplicación de ticketing del teléfono móvil, sino que se envía de manera segura en el paso (12) al módulo servidor de ticketing junto con una Contraseña de un Solo Uso (OTP) calculada utilizando el valor del PIN (y los valores del Código de Activación y del hash(CA&ID), para ser capaz de asignar en el módulo servidor de ticketing el PIN seleccionado y la OTP resultante a la referencia de cliente correcta).

En el paso (13), el PIN es almacenado en la base de datos del módulo servidor de ticketing, junto con las claves y parámetros para calcular un resultado OTP basado en el PIN. Todo este almacenamiento es indicado en la base de datos

de la figura 1.c como datos "OTP(PIN)". De este modo, los vínculos y almacenamiento en la base de datos son ahora los siguientes: referencia de cliente ⇔ A ⇔ $VMC(A)_i$,i=1...n ⇔ CA ⇔ hash(ID&CA) ⇔ OTP(PIN).

Todavía en el paso (13), el módulo servidor de ticketing calcula un resultado OTP utilizando el PIN del usuario y las claves y parámetros OTP almacenados, y compara el resultado con el recibido desde la aplicación de ticketing del teléfono móvil. Si la validación tiene éxito, entonces se pueden enviar credenciales de ticketing a la aplicación de ticketing del teléfono móvil. De ese modo, el módulo servidor de ticketing envía credenciales al teléfono móvil del usuario registrado después de haber validado con éxito una Contraseña de un Solo Uso (OTP) recibida desde la aplicación de ticketing del teléfono móvil.

En el paso (14), se envía un primer conjunto de credenciales (por ejemplo, las credenciales desde i=1 hasta i=j, j<n) a la aplicación de ticketing del teléfono móvil; el teléfono móvil del usuario recibe las credenciales y las almacena para su uso en el sistema de ticketing para transporte sin contacto (de modo que el proceso de personalización de la tarjeta "A" para el uso de las credenciales i=1 to i=j queda entonces completado).

El usuario registrado puede, en el paso (15), utilizar el teléfono móvil para acceder a los servicios de transporte. En el paso (15), el usuario inserta su código PIN en la aplicación de ticketing del teléfono móvil antes de tratar de acceder al sistema 400 de control de acceso de ticketing; de modo que la habilitación del teléfono móvil para cada acceso a ticketing sin contacto también requiere que el usuario inserte un código de identificación personal (PIN) en la aplicación de ticketing del teléfono móvil.

En el paso (16), el módulo servidor de ticketing sabe que un primer conjunto de credenciales de ticketing han sido correctamente recibidas y almacenadas en la aplicación de ticketing del teléfono móvil (éxito en el paso 14), de modo que se envía una confirmación al distribuidor web, que realiza el cargo final del pago e informa al usuario (por ejemplo, mediante un SMS o una alerta en la página

web del distribuidor).

Se envían nuevas credenciales a la aplicación del teléfono móvil a medida que son sucesivamente solicitadas desde el dispositivo móvil del usuario, hasta el límite del derecho concedido para utilizar los servicios de ticketing sin contacto.

En el paso (17), el módulo de credenciales de la aplicación de ticketing del teléfono móvil detecta que son necesarias nuevas credenciales y envía un mensaje *request_credentials* al módulo servidor de ticketing. Este mensaje contiene un resultado Contraseña de un Solo Uso (OTP) que se ha calculado utilizando el valor del PIN (y los valores del Código de Activación y del hash(CA&ID), para poder asignar en el módulo servidor de ticketing el resultado OTP a la referencia de cliente correcta). En una realización, la aplicación calcula la OTP aprovechando que el usuario inserta su código PIN cuando trata de acceder al sistema de ticketing para transporte. En otra realización, se solicita al usuario que inserte su código PIN para poder calcular la OTP.

Al igual que en la segunda parte del paso (13), el módulo servidor de ticketing calcula un resultado OTP utilizando el PIN del usuario y las claves y parámetros OTP almacenados, y compara el resultado con el recibido desde la aplicación de ticketing del teléfono móvil. Si la validación tiene éxito, entonces se pueden enviar más credenciales de ticketing a la aplicación de ticketing del teléfono móvil. De ese modo, el módulo servidor de ticketing envía más credenciales al teléfono móvil del usuario registrado después de la validación con éxito de una Contraseña de un Solo Uso (OTP) recibida desde la aplicación de ticketing del teléfono móvil.

En el paso (18), se envía un nuevo conjunto de credenciales (por ejemplo, las credenciales desde i=j+1 hasta i=k, k<n) a la aplicación de ticketing del teléfono móvil; el teléfono móvil del usuario recibe las credenciales y las almacena para su uso en el sistema de ticketing para transporte sin contacto (de modo que el proceso de personalización de la tarjeta "A" para utilizar las credenciales i=j+1

hasta i=k queda entonces completado).

En esta realización, se repiten los pasos (17), (13) y (18) hasta que las credenciales hasta la credencial i=n se han enviado al teléfono móvil y se han recibido y almacenado en la aplicación de ticketing del teléfono móvil para su uso en el sistema de ticketing para transporte sin contacto.

Todas esas credenciales, hasta la credencial n, pueden ser utilizadas en el paso (15) por el usuario registrado para acceder a los servicios de transporte. En el paso (15), el usuario inserta su código PIN en la aplicación de ticketing del teléfono móvil antes de intentar acceder al sistema 400 de control de acceso de ticketing; así, la habilitación del teléfono móvil para cada acceso a ticketing sin contacto también requiere que el usuario inserte un código de identificación personal (PIN) en la aplicación de ticketing del teléfono móvil.

El derecho para utilizar los servicios de ticketing se puede extender si el usuario paga por ello, de modo que se pueden generar dinámicamente nuevas particiones del derecho de ticketing en el módulo servidor de ticketing. Así, por ejemplo después de una nueva ejecución del proceso de los pasos (2) y (3), se pueden generar las particiones i=n+1 hasta i=m en una nueva ejecución del proceso del paso (4), y las credenciales desde i=n+1 hasta i=m pueden ser enviadas sucesivamente al teléfono móvil y recibidas y almacenadas en la aplicación de ticketing del teléfono móvil de acuerdo con los pasos repetidos (17), (13) y (18) para su uso en el sistema de ticketing para transporte sin contacto.

En un ejemplo particular, el usuario paga 50€ a través del canal web de distribución y el derecho de transporte concedido le permite acceder a una Zona A de los servicios de ticketing para transporte en autobús durante el mes de Abril (30 días). El módulo servidor de ticketing prepara la credencial 1 para su uso el primer día del mes... y la credencial 30 para su uso el último día del mes. Las primeras cinco credenciales son enviadas a la aplicación del teléfono móvil antes de empezar el mes, después de recibir un valor correcto de la OTP;

en caso de que en el teléfono móvil aún haya credenciales disponibles para cuatro días restantes, el mensaje *request_credentials* se envía para solicitar credenciales para 1 día extra, aprovechando que el usuario inserta el PIN para acceder a los servicios de ticketing móvil; en caso de que haya credenciales disponibles para tres días restantes, la solicitud será para 2 días extra, aprovechando que el usuario inserta el PIN para acceder a los servicios de ticketing móvil; en caso de que haya credenciales disponibles para 2 días o 1 solo día, se solicitará al usuario que inserte su código PIN en la aplicación de ticketing del teléfono móvil para solicitar, recibir y almacenar nuevas credenciales (hasta el límite de credenciales para 5 días, disponibles en el teléfono móvil).

En otro ejemplo particular, el usuario paga 40€ a través del canal web de distribución y el derecho de transporte concedido le permite 40 viajes en autobús dentro de la Zona A. Las primeras cinco credenciales, una por viaje, son enviadas a la aplicación del teléfono móvil después de recibir un valor de la OTP correcto; en caso de que en el teléfono móvil haya todavía credenciales disponibles para cuatro viajes restantes, el mensaje de *request_credentials* se envía para solicitar credenciales para 1 viaje extra, aprovechando que el usuario inserta el PIN para acceder a los servicios de ticketing móvil; en caso de que haya disponibles credenciales para tres viajes restantes, la solicitud será para 2 viajes extra, aprovechando que el usuario inserta el PIN para acceder a los servicios de ticketing móvil; en caso de que haya credenciales disponibles para 2 viajes o sólo 1 viaje, se solicitará al usuario que inserte su código PIN en la aplicación de ticketing del teléfono móvil para solicitar, recibir y almacenar nuevas credenciales (hasta el límite de credenciales para 5 viajes, disponibles en el teléfono móvil).

De modo que la aplicación del teléfono móvil limita la solicitud de nuevas credenciales basándose en información acerca de las credenciales que están ya almacenadas en el teléfono móvil. Ventajosamente, esta característica permite al proveedor de servicios de ticketing monitorizar y controlar el número de credenciales disponibles en el teléfono móvil del usuario, manteniendo así

parte del derecho concedido en el módulo servidor de ticketing.

El módulo de operaciones (o el de seguridad) en el módulo servidor de ticketing puede solicitar que al menos una credencial sea deshabilitada (o eliminada) de la aplicación del teléfono móvil mediante el envío de un mensaje de deshabilitación (o eliminación) desde el módulo de servidor de ticketing a la aplicación del teléfono móvil del usuario. De ese modo, el proveedor de servicios de ticketing todavía puede gestionar el ciclo de vida de las credenciales cuando ya están disponibles en la aplicación del teléfono móvil.

En una realización, las credenciales de ticketing se bloquean en la aplicación del teléfono móvil después de que se haya producido un número determinado de inserciones erróneas del Número de Identificación Personal, y se envía un mensaje de advertencia al módulo servidor de ticketing. En otra realización, el modulo servidor de ticketing bloquea el derecho de ticketing concedido después de que se produzca un número determinado de verificaciones erróneas de una OTP recibida desde la aplicación del teléfono móvil, y se envía un mensaje de bloqueo de credenciales a la aplicación del teléfono móvil. Así, el proveedor de servicios de ticketing tiene disponibles herramientas de gestión de seguridad y del PIN, tanto en la aplicación como en el lado del módulo servidor de ticketing.

El módulo de seguridad comprueba periódicamente la validez de los códigos de activación y las credenciales, de modo que no se pueden utilizar después de la expiración. En un ejemplo, si se utiliza un código de activación o credencial después de su fecha de caducidad, se envía un mensaje al sistema legacy de transporte para informar de este evento.

La Figura 2.a es un diagrama esquemático que ilustra generalmente los principales bloques funcionales de la invención como una extensión de un sistema legacy de pagos ; esta figura muestra un sistema 3000a legacy de pagos de un de un banco (/entidad de medios de pago) proveedor de servicios, que soporta tarjetas inteligentes de contacto & sin contacto para pagos (de

modo que un usuario de este sistema puede tener disponible una tarjeta inteligente financiera de contacto / sin contacto para pagar en establecimientos comerciales equipados con un Terminal 4000a Punto de Venta de contacto / sin contacto). Los usuarios 1000a pueden solicitar, a través de un canal 2000a web de distribución, tarjetas inteligentes financieras para pagos a débito/crédito/prepago. En este ejemplo, el canal web de distribución pertenece al banco que posee el sistema legacy de pagos y el usuario también es cliente de este banco, de modo que puede confirmar el pago de tarjetas financieras solicitadas y más tarde activarlas a través de la página web, utilizando un medio de firma electrónica proporcionado por el banco.

Cuando el usuario solicita, a través del canal web de distribución, los servicios móviles de pago relacionados con la presente invención (es decir, la capacidad para utilizar al menos una tarjeta financiera móvil para pagos móviles sin contacto) y paga por ellos (el usuario paga por la capacidad que solicita) utilizando el medio de firma electrónica del banco, el sistema legacy de pagos reenvía la solicitud al módulo 5000a servidor de pagos de la invención. Los principales bloques funcionales de este módulo se ilustran en esta figura.

La figura 2.b proporciona más detalles acerca de los bloques funcionales de la figura 2.a y es un diagrama esquemático que ilustra una realización de un sistema de pagos de acuerdo con la invención, para habilitar pagos móviles sin contacto a través de una aplicación de teléfono móvil; la figura 2b muestra el proceso desde el registro del usuario para los servicios móviles de pago hasta la provisión de dichos servicios.

En el paso (1), el usuario descarga en su teléfono móvil dotado de tecnología sin contacto la aplicación de pagos para teléfono móvil, desde una tienda 7000 de aplicaciones.

En el contexto de la invención, el usuario paga por ciertos servicios de pago solicitados al proveedor de servicios. En el paso (2) de esta realización, el usuario solicita servicios de pago (es decir, solicita la capacidad para utilizar al

menos una tarjeta financiera móvil para pagos móviles sin contacto) a través de un canal web de distribución y confirma el pago a través de ese medio (el usuario paga por la capacidad solicitada). En esta realización aplica el mismo escenario que el descrito en la figura 2.a: el canal web de distribución pertenece al banco. En el paso (3), la solicitud es enviada al sistema legacy de pagos y luego reenviada al módulo servidor de pagos.

Asociado al pago y al correspondiente derecho concedido para utilizar ciertos servicios de pago, un módulo servidor de pagos prepara credenciales de pago para su uso por el usuario registrado y las envía al teléfono móvil del usuario registrado, como se detalla a continuación. En esta realización, el módulo servidor de pagos divide el derecho de pagos concedido en varias particiones y genera una credencial independiente para cada una de dichas particiones.

En el paso (4), el módulo servidor de pagos asigna un derecho de pagos al usuario (representado en la fig. 2.b como tarjeta "A" en el módulo servidor), vinculado a un conjunto de credenciales (representadas en la fig. 2.b como tarjetas "$VMC(A)_1$" a "$VMC(A)_n$" en el módulo servidor) y a una referencia de cliente de pagos, y almacena estos vínculos en la base de datos del módulo servidor de pagos (referencia de cliente $\Leftrightarrow$ A $\Leftrightarrow$ $VMC(A)_i$,i=1...n).

En el paso (5), se genera un código de activación y se almacena en la base de datos del módulo servidor de pagos (referencia de cliente $\Leftrightarrow$ A $\Leftrightarrow$ $VMC(A)_i$,i=1...n $\Leftrightarrow$ CA). En el paso (6), el Código de Activación es enviado al sistema legacy de pagos, reenviado al canal web de distribución y mostrado al usuario.

En el paso (7), el usuario inserta el código de activación en la aplicación de pagos del teléfono móvil, y en el paso (8) el teléfono móvil envía al módulo servidor de pagos, por ejemplo vía https, el [código de activación y el hash(número de identificación del teléfono móvil & código de activación)].

En el paso (9), el valor del hash es almacenado en el módulo servidor de pagos, de modo que los vínculos quedan ahora como sigue: referencia de

cliente ⇔ A ⇔ $VMC(A)_i$,i=1...n ⇔ CA ⇔ hash(ID&CA).

En el paso (10) se pre-personaliza la tarjeta "A" en la aplicación del teléfono móvil.

La pre-personalización hace referencia al paso anterior a la personalización; y la pre-personalización/personalización de la tarjeta "A" hace referencia a la pre-personalización/personalización de la aplicación de pagos móvil sin contacto de la invención para que funcione en "modo de emulación de tarjeta" para servicios de pagos móviles sin contacto, de un modo equivalente a una aplicación de pagos basada en tarjeta SIM funcionando en "modo de emulación de tarjeta" para servicios de pagos móviles sin contacto (como por ejemplo pagos de tipo EMV chip & PIN). La personalización completa de la tarjeta "A" en la aplicación de pagos del teléfono móvil requiere la descarga de credenciales desde el módulo servidor de pagos a la aplicación de pagos del teléfono móvil, como se describe a continuación.

Cuando termina el paso (10), el usuario ya está registrado en el sistema de la invención, pero aún está pendiente la recepción de credenciales en la aplicación de pagos del teléfono móvil. En esta etapa, cada credencial está asociada unívocamente al teléfono móvil del usuario registrado y a un código de activación, y habilita parcialmente el teléfono móvil para servicios de pago sin contacto en establecimientos comerciales.

En el paso (11), se solicita al usuario que seleccione un Número de Identificación Personal (PIN) para servicios de pago móviles sin contacto. El valor del PIN no es almacenado en la aplicación de pagos del teléfono móvil, sino que es enviado de manera segura en el paso (12) al módulo servidor de pagos, junto con una Contraseña de un Solo Uso (OTP) calculada utilizando el valor el PIN (y los valores del Código de Activación y del hash(CA&ID), para poder asignar en el módulo servidor de pagos el PIN seleccionado y el resultado OTP a la correcta referencia de cliente).

En el paso (13) el PIN se almacena en la base de datos del módulo servidor de pagos, junto con las claves y parámetros para calcular una OTP basada en el PIN. Todo este almacenamiento es indicado en la base de datos de la figura 1.c como datos "OTP(PIN)". De modo que los vínculos y almacenamiento en la base de datos son ahora los siguientes: referencia de cliente ⇔ A ⇔ $VMC(A)_i$,i=1...n ⇔ CA ⇔ hash(ID&CA) ⇔ OTP(PIN).

Todavía en el paso (13), el módulo servidor de pagos calcula un resultado OTP utilizando el PIN del usuario y las claves y parámetros OTP almacenados, y compara el resultado con el recibido de la aplicación de pagos del teléfono móvil. Si la validación tiene éxito, entonces se pueden enviar credenciales de pago a la aplicación de pagos del teléfono móvil. De modo que el módulo servidor de pagos envía credenciales al teléfono móvil del usuario registrado después de la correcta validación de una Contraseña de un Solo Uso (OTP) recibida desde la aplicación de pagos del teléfono móvil.

En el paso (14), un primer conjunto de credenciales (por ejemplo, las credenciales desde i=1 hasta i=j, j<n) son enviadas a la aplicación de pagos del teléfono móvil; el teléfono móvil del usuario recibe las credenciales y las almacena para su uso en establecimientos comerciales dotados de Terminales Punto de Venta sin contacto (de modo que el proceso de personalización de la tarjeta "A" para el uso de las credenciales i=1 hasta i=j queda entonces completado).

El usuario registrado puede, en el paso (15), utilizar el teléfono móvil para pagar en comercios dotados de Terminales Punto de Venta sin contacto. En el paso (15), el usuario inserta su código PIN en la aplicación de pagos del teléfono móvil antes de intentar pagar en el Terminal 4000 Punto de Venta sin contacto; de modo que la habilitación completa del teléfono móvil para cada pago móvil sin contacto requiere además que el usuario inserte un código de identificación personal (PIN) en la aplicación de pagos del teléfono móvil.

En el paso (16), el módulo servidor de pagos sabe que un primer conjunto de

credenciales de pago ha sido correctamente recibido y almacenado en la aplicación de pagos del teléfono móvil (éxito en el paso 14), de modo que se envía una confirmación al distribuidor web, que realiza el cargo final del pago e informa al usuario (por ejemplo, a través de un SMS o una alerta en la página web del distribuidor).

Se envían nuevas credenciales a la aplicación del teléfono móvil a medida que son sucesivamente solicitadas desde el dispositivo móvil del usuario, hasta el límite del derecho concedido para el uso de los servicios de pago sin contacto.

En el paso (17), la aplicación de pagos del teléfono móvil detecta que son necesarias nuevas credenciales y envía un mensaje de *request_credentials* al módulo servidor de pagos. Este mensaje contiene un resultado Contraseña de un Solo Uso (OTP), que ha sido calculada utilizando el valor PIN (y los valores del Código de Activación y el hash(CA&ID), para ser capaz de asignar en el módulo servidor de pagos el resultado OTP a la referencia de cliente correcta). En una realización, la aplicación calcula la OTP aprovechando que el usuario inserta su código PIN cuando trata de realizar un pago móvil sin contacto en un establecimiento comercial. En otra realización, se solicita al usuario que inserte su código PIN para poder calcular la OTP.

Al igual que en la segunda parte del paso (13), el módulo servidor de pagos calcula un resultado OTP utilizando el PIN del usuario y las claves y parámetros OTP almacenados, y compara el resultado con el recibido desde la aplicación de pagos del teléfono móvil. Si la validación tiene éxito, entonces se pueden enviar más credenciales de pago a la aplicación de pagos del teléfono móvil. De modo que el módulo servidor de pagos envía más credenciales al teléfono móvil del usuario registrado después de la validación con éxito de una Contraseña de un Solo Uso (OTP) recibida desde la aplicación de pagos del teléfono móvil.

En el paso (18), se envía un nuevo conjunto de credenciales (por ejemplo, las credenciales desde i=j+1 hasta i=k, k<n) a la aplicación de pagos del teléfono

móvil; el teléfono móvil del usuario recibe las credenciales y las almacena para su uso en pagos móviles sin contacto (de modo que el proceso de personalización de la tarjeta "A" para el uso de las credenciales i=j+1 hasta i=k queda entonces completado).

En esta realización, los pasos (17), (13) y (18) se repiten hasta que las credenciales hasta la credencial i=n son enviadas al teléfono móvil, y son recibidas y almacenadas en la aplicación de pagos del teléfono móvil para su uso en pagos móviles sin contacto.

Todas estas credenciales, hasta la credencial n, pueden ser utilizadas en el paso (15) por el usuario registrado para pagos móviles sin contacto. En el paso (15), el usuario inserta su código PIN en la aplicación de pagos del teléfono móvil antes de intentar pagar en un Terminal Punto de Venta de un establecimiento comercial; de modo que la habilitación del teléfono móvil para cada pago móvil sin contacto también requiere que el usuario inserte un código de identificación personal (PIN) en la aplicación de pagos del teléfono móvil.

El derecho a utilizar los servicios de pagos puede ser extendido si el usuario paga por ello, de modo que se pueden generar dinámicamente nuevas particiones del derecho de pagos en el módulo servidor de pagos. Por tanto, después de una nueva ejecución de los pasos (2) y (3), se pueden generar particiones desde i=n+1 hasta i=m en un nuevo proceso de ejecución del paso (4), y las credenciales desde i=n+1 hasta i=m pueden ser sucesivamente enviadas al teléfono móvil y recibidas y almacenadas en la aplicación de pagos del teléfono móvil de acuerdo con los pasos repetidos (17), (13) y (18) para su uso en pagos móviles sin contacto.

En un ejemplo particular, el usuario paga 20€ a través del canal web de distribución y el derecho de pagos concedido le habilita para llevar a cabo operaciones de pago sin contacto, a través de su aplicación móvil sin contacto, de acuerdo con un esquema tradicional de producto de crédito, en Terminales Punto de Venta de comercios durante un año. El módulo servidor de pagos

prepara credenciales para su uso durante el periodo anual, cada una de las cuales es válida para un único intento de pago. En primer lugar, se envían cinco credenciales a la aplicación del teléfono móvil al comenzar el período, después de recibir un valor OTP correcto; en caso de que en el teléfono móvil haya todavía credenciales disponibles para cuatro operaciones de pago restantes, se envía el mensaje *request_credentials* para solicitar credenciales para 1 pago extra, aprovechando que el usuario inserta el PIN para un intento de pago móvil sin contacto en un establecimiento comercial; en caso de que haya credenciales disponibles para tres operaciones de pago restantes, se hará una solicitud de 2 pagos extra, aprovechando que el usuario inserta el PIN para un intento de pago móvil sin contacto en un establecimiento comercial; en caso de que haya disponibles credenciales para 2 o sólo para una operación de pago, se solicitará al usuario que inserte su código PIN en la aplicación de pagos del teléfono móvil para solicitar, recibir y almacenar nuevas credenciales (hasta el límite de 5 credenciales de pago, disponibles en el teléfono móvil).

De modo que la aplicación del teléfono móvil limita la solicitud de nuevas credenciales basándose en información acerca de las credenciales que ya están almacenadas en el teléfono móvil. Ventajosamente, esta característica permite al proveedor de servicios de pago monitorizar y controlar el número de credenciales disponibles en el teléfono móvil del usuario, manteniendo así parte del derecho concedido en el módulo servidor de pagos.

El módulo de seguridad (o el de operaciones) del módulo servidor de pagos puede solicitar que al menos una credencial sea deshabilitada (o eliminada) de la aplicación del teléfono móvil mediante el envío de un mensaje de deshabilitación (o eliminación) desde el módulo servidor de pagos a la aplicación del teléfono móvil del usuario. De ese modo, el proveedor de servicios de pagos todavía puede gestionar el ciclo de vida de las credenciales cuando ya están disponibles en la aplicación del teléfono móvil.

En una realización, las credenciales de pago son bloqueadas en la aplicación del teléfono móvil después de un número determinado de intentos erróneos de

introducir el Número de Identificación Personal, y se envía un mensaje de advertencia al módulo servidor de pagos. En otra realización, el módulo servidor de pagos bloquea el derecho de pagos concedido después de un número determinado de verificaciones incorrectas de una OTP recibida desde la aplicación del teléfono móvil, y se envía un mensaje de bloqueo de credenciales a la aplicación del teléfono móvil. Por tanto, el proveedor de servicios de pago tiene herramientas de gestión de la seguridad y del PIN disponibles tanto en la aplicación como en el lado del módulo servidor de pagos.

La figura 2.c es un diagrama de flujo que ilustra parcialmente una realización de un método de acuerdo con la invención.

En esta realización, para transacciones on-line de pagos móviles sin contacto, una segunda parte de la credencial de pago es calculada por la propia aplicación de pagos del teléfono móvil, utilizando el valor de la transacción y el PIN del usuario como entradas para generar un resultado OTP (que constituye la segunda parte de la credencial). La primera y la segunda partes de la credencial se utilizan para la transacción de pago móvil sin contacto y la verificación de dicha OTP por el módulo servidor de pagos es necesaria para aceptar o denegar la transacción.

En un entorno EMV chip & PIN, se asigna un número PAN a una tarjeta EMV proporcionada al usuario (tarjeta (A)). Esta tarjeta incluye otro conjunto de datos que son parte de la propia credencial: fecha de caducidad (FC), CVV y clave derivada para el cálculo del criptograma.

En esta realización, la credencial de pagos para la tarjeta $VMC(A)_i$ es generada primero en el módulo servidor de pagos, de modo que el PAN, FC, CVV y la clave derivada son calculados en el lado del servidor y enviados, junto con el BIN, a la aplicación de pagos móvil. En un ejemplo particular, el número PAN es generado utilizando el hash(ID&CA) y la referencia de cliente como datos de entrada.

Durante el proceso de pago online que utiliza esta credencial de pago $VMC(A)_i$, el PIN es insertado en la aplicación de pagos del teléfono móvil. En esta realización, el valor de la transacción (la cantidad a pagar) también es insertado por el usuario en la aplicación de pagos del teléfono móvil, de modo que tanto el valor de la transacción como el PIN del usuario son entradas que se usan para generar un resultado OTP (que constituye la segunda parte de la credencial). En un ejemplo particular, la OTP es un resultado de 7 dígitos, FC' (4 dígitos) y CVV' (3 dígitos). La FC' será una fecha de caducidad válida en el sistema de medios de pago.

El intento de transacción de pago sin contacto se lleva a cabo utilizando el BIN/PAN/FC'/CVV' y el criptograma como credenciales, de modo que la primera parte de la credencial ha sido calculada en el lado del servidor y la segunda parte en la aplicación de pagos del teléfono móvil, utilizando el PIN y el valor de la transacción como datos de entrada.

El módulo servidor de pagos procesa el PAN recibido y obtiene datos de referencia de cliente & dispositivo, de modo que puede asignar la transacción a una cuenta particular (PIN, claves OTP, etc.). En el contexto de una transacción online, el valor de la transacción es conocido en el lado del servidor y el PIN está almacenado en el módulo servidor de pagos, de modo que la OTP puede ser verificada por el módulo servidor de pagos. Si la verificación de la OTP tiene éxito, se validan las credenciales y se puede autorizar la transacción en el host del banco como si fuese una transacción con tarjeta (A). Los mensajes de respuesta al banco adquiriente, sin embargo, se referirán a una transacción $VMC(A)_i$.

Ventajosamente, calcular parte de la credencial en la aplicación de pagos del teléfono móvil dota al usuario y al sistema de un nivel de seguridad más elevado en el ciclo de vida de las credenciales de pago.

Aunque la presente invención se ha descrito con detalle por motivos de

ilustración, se entiende que dichos detalles se muestran únicamente con ese objeto, y que los expertos en la materia podrán realizar variaciones en el mismo sin salirse del ámbito de la invención. Por tanto, aunque las realizaciones preferidas del método y del sistema móvil se han descrito con referencia al entorno en el que fueron desarrollados, son simplemente ilustrativos de los principios de la invención. Se pueden concebir otras realizaciones y configuraciones sin salirse del ámbito de las reivindicaciones adjuntas.

Además, aunque las realizaciones de la invención descritas con referencia a las figuras comprenden aparatos de ordenador (se entiende por "ordenador" cualquier medio de procesamiento electrónico capaz de ejecutar una secuencia de operaciones codificadas como un programa) y procesos llevados a cabo en aparatos de ordenador, la invención también se extiende a programas de ordenador, en particular programas de ordenador en o sobre una portadora, adaptados para llevar a la práctica la invención. El programa puede estar en la forma de código fuente, código objeto, o un código intermedio entre objeto y fuente, como por ejemplo en forma parcialmente compilada, o en cualquier otra forma adecuada para su uso en la implementación de procesos de acuerdo con la invención. La portadora puede ser una entidad o dispositivo capaz de almacenar el programa. Por ejemplo, la portadora puede comprender un medio de almacenamiento, como un ROM, por ejemplo un CD ROM o un ROM semiconductor, o un medio de almacenamiento magnético, por ejemplo un disco flexible o un disco duro. Además, la portadora puede ser una portadora transmisible, como una señal eléctrica u óptica que pueda transportarse a través de un cable eléctrico u óptico o por radio u otros medios. Cuando el programa está incorporado en una señal que pueda transportarse directamente por cable o por otro dispositivo o medio, la portadora puede estar constituida por dicho cable o dicho otro dispositivo o medio. Alternativamente, la portadora puede ser un circuito integrado en el que está embebido el programa, estando adaptado el circuito para llevar a cabo, o para su uso llevar a cabo, los procesos correspondientes.

REIVINDICACIONES

1. Un método para habilitar ticketing/pagos móviles sin contacto mediante una aplicación de teléfono móvil, comprendiendo el método los siguientes pasos:

(a) un usuario paga a un proveedor de servicios por unos servicios de ticketing/pagos, obteniendo un código de activación ;

(b) asociado al pago y a un correspondiente derecho concedido para utilizar los servicios de ticketing/pagos correspondientes, un módulo servidor de ticketing/pagos prepara credenciales de ticketing/pagos para su uso por el usuario y las envía al teléfono móvil del usuario;

(c) el teléfono móvil del usuario recibe las credenciales y las almacena para su uso en un sistema de ticketing para transporte sin contacto, en caso de credenciales de ticketing, o para su uso en pagos móviles sin contacto, en el caso de credenciales de pago;

estando dicho método **caracterizado porque** cada credencial preparada está unívocamente asociada al teléfono móvil del usuario registrado a través de uno o varios identificadores del dispositivo y a un código de activación, y habilita parcialmente el teléfono móvil para el acceso a ticketing sin contacto, en caso de credenciales de ticketing, o para pagos móviles sin contacto, en caso de credenciales de pagos; donde la habilitación del teléfono móvil para cada acceso a ticketing sin contacto o pago móvil sin contacto también requiere que el usuario inserte un número de identificación personal en la aplicación de ticketing/pagos del teléfono móvil; y donde el módulo servidor de ticketing/pagos envía credenciales al teléfono móvil del usuario registrado después de la validación con éxito de una Contraseña de un Solo Uso (OTP) recibida desde la aplicación de ticketing/pagos del teléfono móvil.

2. Un método de acuerdo con la reivindicación 1, donde el módulo servidor de ticketing/pagos divide el derecho de ticketing/pagos concedido en varias particiones y genera una credencial independiente para cada una de dichas particiones.

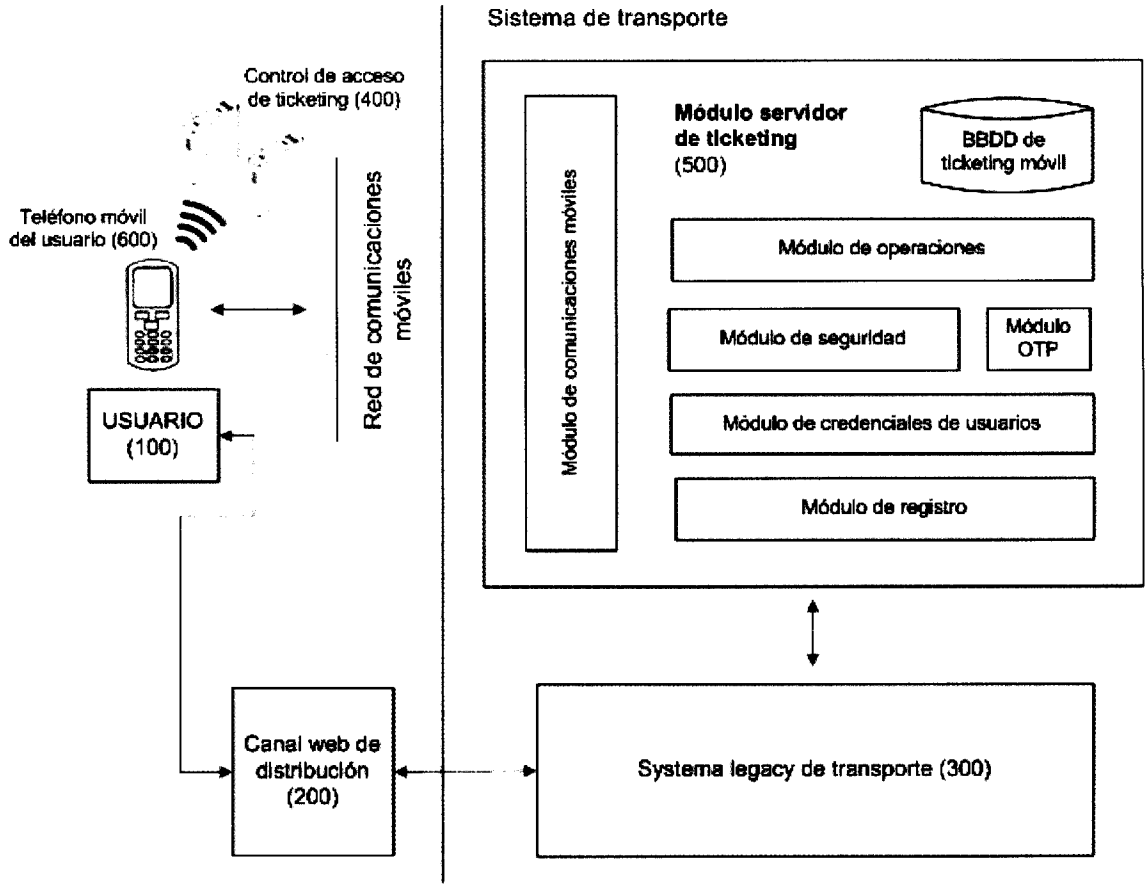
Sistema de transporte
Control de acceso de ticketing (400)
Teléfono móvil del usuario (600)
Red de comunicaciones móviles
USUARIO (100)
Módulo de comunicaciones móviles
Módulo servidor de ticketing (500)
BBDD de ticketing móvil
Módulo de operaciones
Módulo de seguridad
Módulo OTP
Módulo de credenciales de usuarios
Módulo de registro
Canal web de distribución (200)
Systema legacy de transporte (300)

FIGURA 1.a

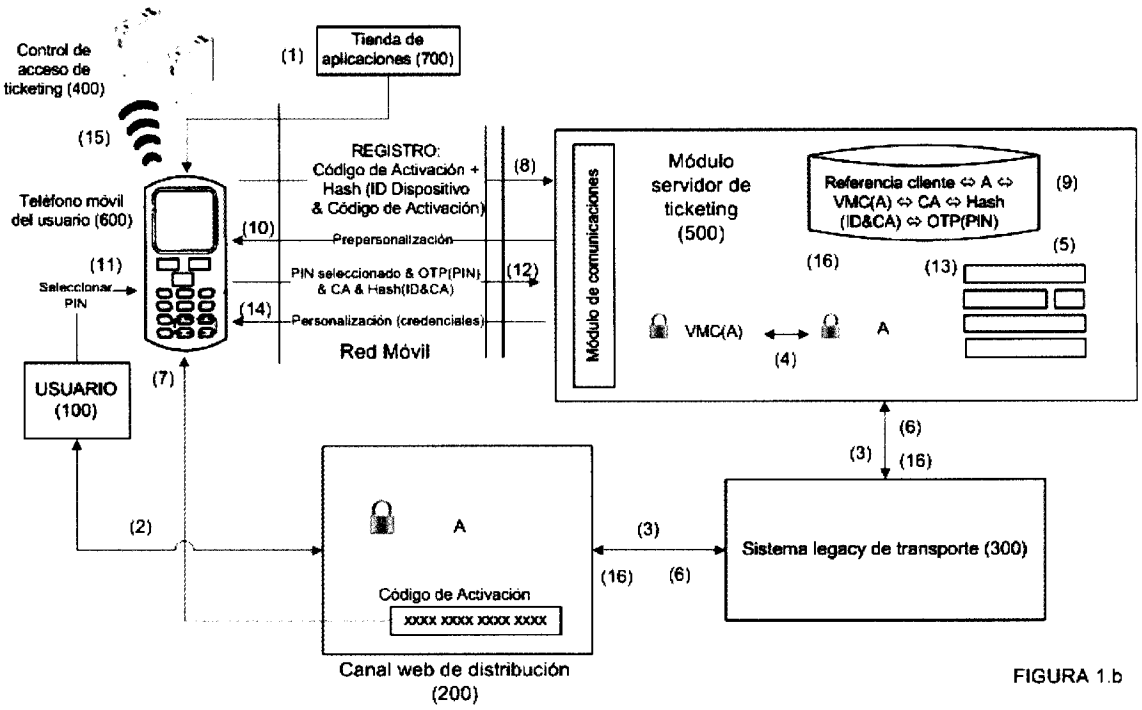

FIGURA 1.b

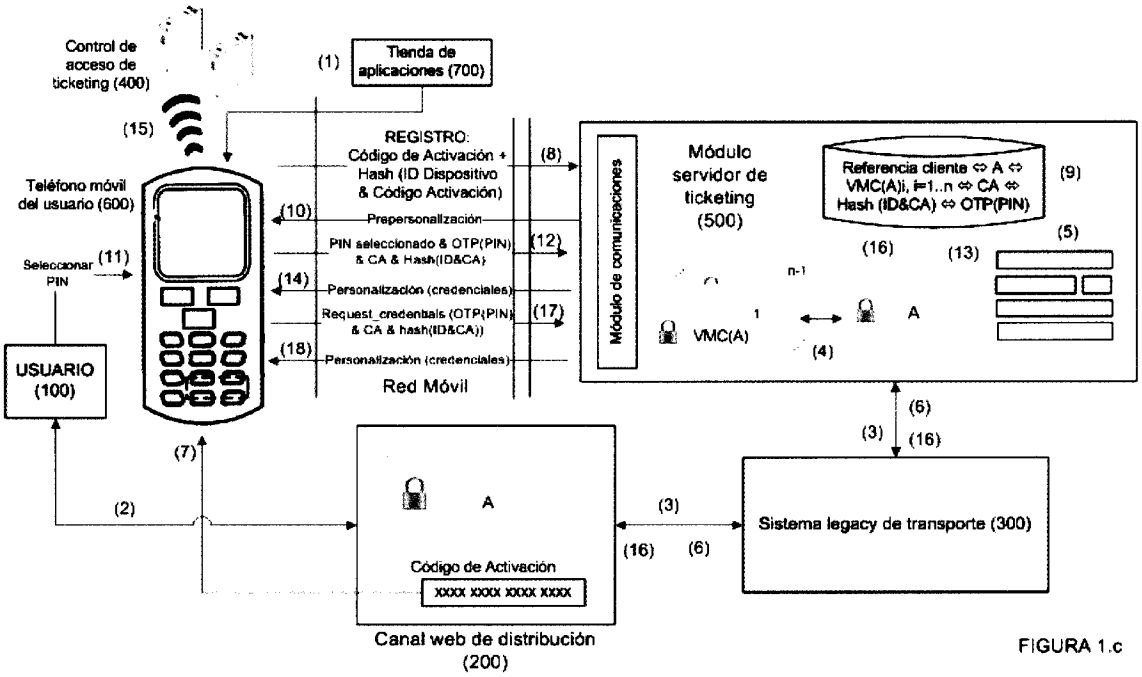

FIGURA 1.c

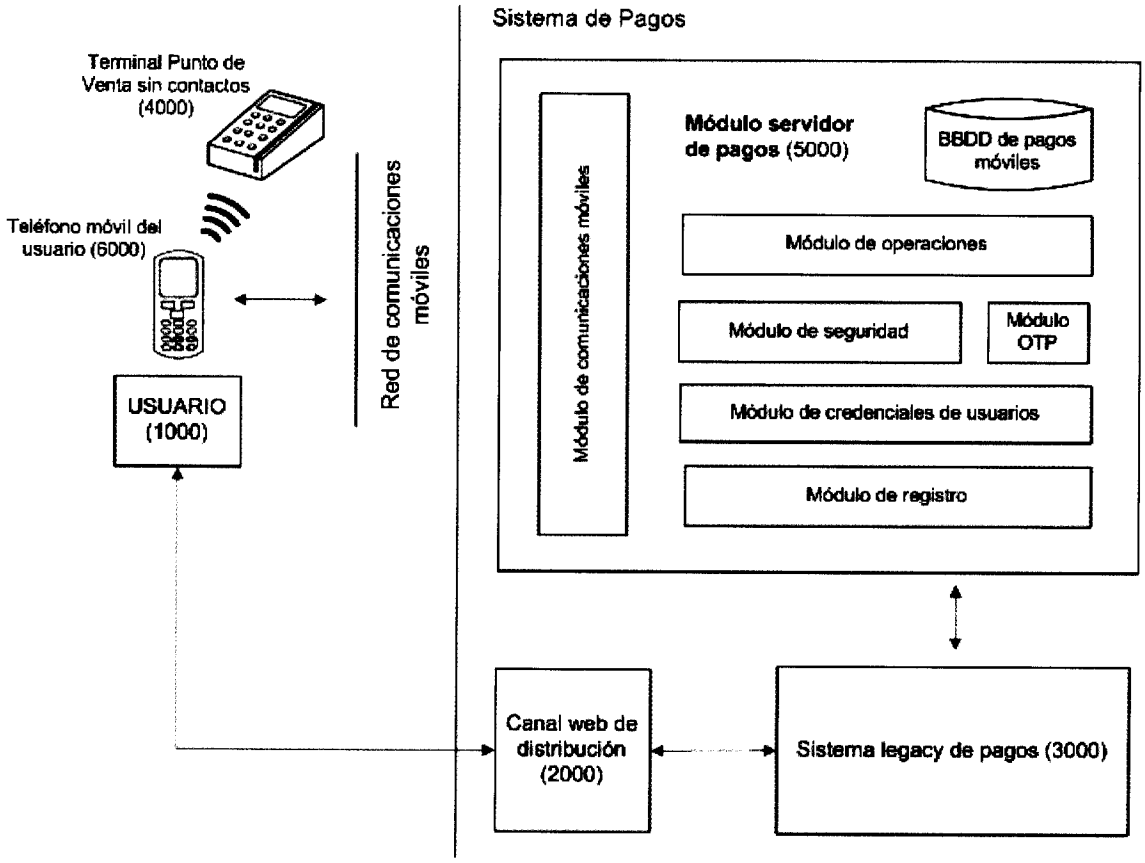
Sistema de Pagos
Terminal Punto de Venta sin contactos (4000)
Teléfono móvil del usuario (6000)
USUARIO (1000)
Red de comunicaciones móviles
Módulo de comunicaciones móviles
Módulo servidor de pagos (5000)
BBDD de pagos móviles
Módulo de operaciones
Módulo de seguridad
Módulo OTP
Módulo de credenciales de usuarios
Módulo de registro
Canal web de distribución (2000)
Sistema legacy de pagos (3000)

FIGURA 2.a

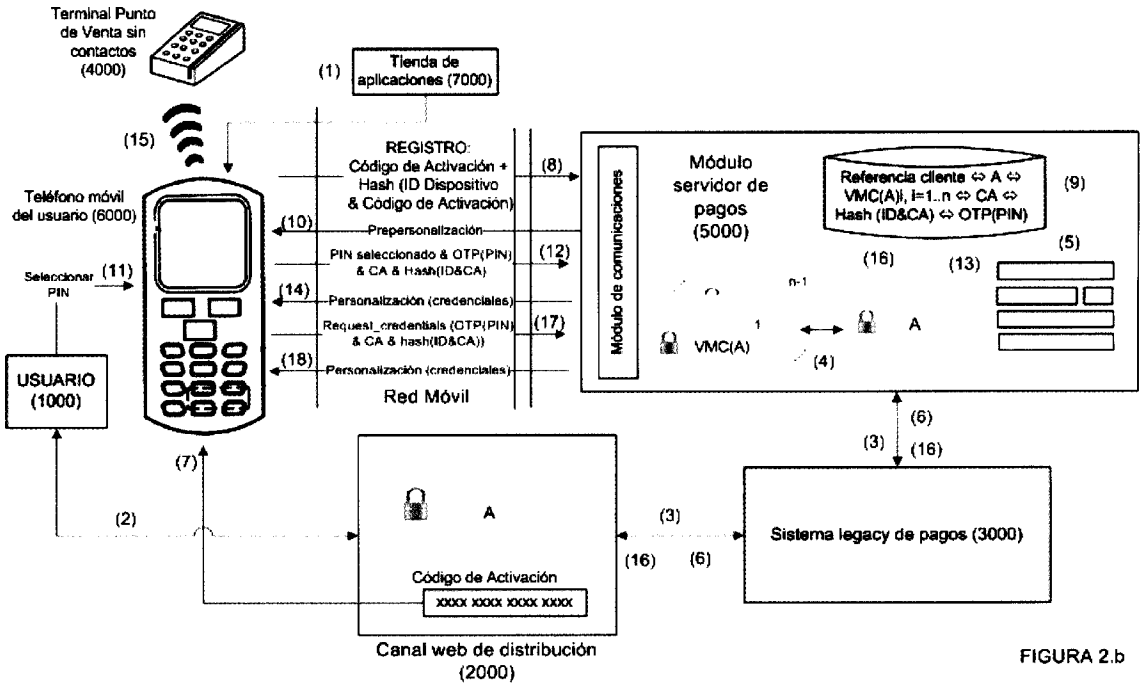

FIGURA 2.b

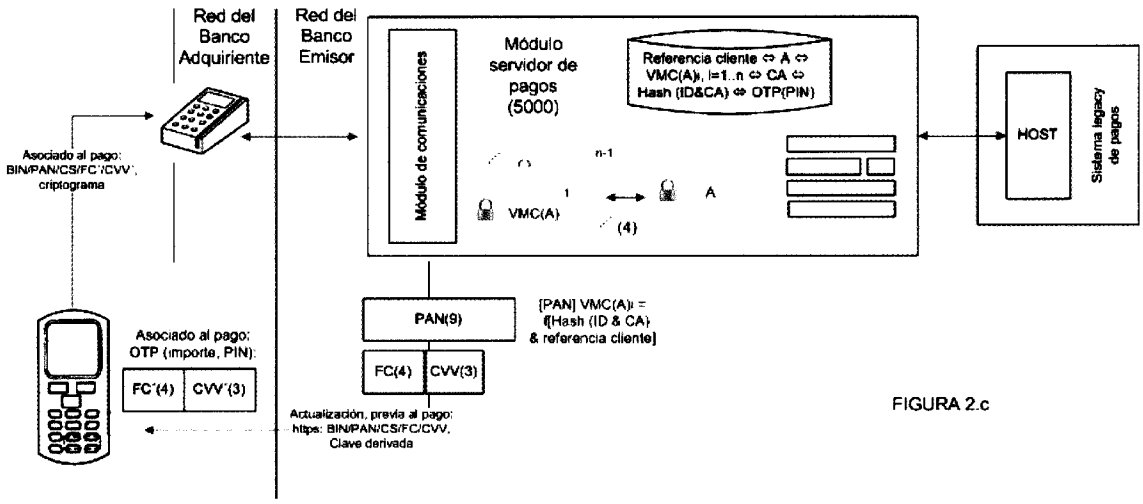

FIGURA 2.c