(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 375 717**

(51) Int. CI.:
G06F 17/00 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05785125 .5**
(96) Fecha de presentación: **13.09.2005**
(97) Número de publicación de la solicitud: **1810177**
(97) Fecha de publicación de la solicitud: **25.07.2007**

(54) Título: **SISTEMA DE TRANSACCIÓN COMERCIAL EN LÍNEA Y PROCEDIMIENTO DE FUNCIONAMIENTO DEL MISMO.**

(30) Prioridad:
14.09.2004 GB 0420409

(45) Fecha de publicación de la mención BOPI:
05.03.2012

(45) Fecha de la publicación del folleto de la patente:
05.03.2012

(73) Titular/es:
WATERLEAF LIMITED
TOP FLOOR 14 ATHOL STREET
DOUGLAS ISLE OF MAN IM1 1JA, GB

(72) Inventor/es:
OREN, Yosi

(74) Agente: **Pons Ariño, Ángel**

DESCRIPCIÓN

Sistema de transacción comercial en línea y procedimiento de funcionamiento del mismo.

Campo de la invención

Esta invención se refiere a un sistema para realizar transacciones comerciales en línea y, más específicamente, pero no exclusivamente, a un sistema para realizar transacciones comerciales en línea iniciadas desde plataformas móviles como auriculares de telecomunicación móviles, teléfonos móviles y similares. El sistema se extiende a un procedimiento de funcionamiento de un sistema para realizar transacciones comerciales en línea iniciadas desde plataformas móviles.

Antecedentes de la invención

El uso de dispositivos de telecomunicación móviles, como teléfonos móviles, para comunicación de voz y datos ha aumentado rápidamente en los últimos años, y se espera que un crecimiento tan rápido continúe para el futuro previsible. Cada vez más, tales dispositivos de comunicación móviles se están usando no sólo para comunicación de voz y datos, sino que también se usan con propósitos de entretenimiento, como mensajería multimedia, juegos para móviles, y similares.

Los teléfonos móviles actuales son capaces de ejecutar varias tecnologías de aplicación incorporadas, como J2ME, Brew, Symbian, Linux y Windows Mobile, por nombrar sólo unas pocas. Estas de tecnologías de aplicación proporcionan plataformas adecuadas para el desarrollo de una amplia gama de aplicaciones diferentes para dispositivos de telecomunicación móviles.

Internet, que es omnipresente, proporciona una plataforma adecuada para realizar transacciones comerciales entre empresas (B2B) y entre empresa y cliente (B2C), particularmente en la World Wide Web de Internet. Un gran número de empresas comerciales dispares actualmente realizan transacciones comerciales B2C por medio de Internet. Ejemplos de tales empresas comerciales son minoristas, como Amazon™; subastadoras, como eBay™; casinos en línea; entidades de apuestas deportivas; y corredores de Bolsa, como E-trade™.

Como resultado del reciente crecimiento rápido en la telecomunicación móvil, ha surgido una necesidad de que las aplicaciones comerciales B2C basadas en la web existentes estén disponibles desde teléfonos móviles. Esto se consigue comúnmente convirtiendo un sitio web B2C existente en un formato que sea soportado por los navegadores de teléfonos móviles, como WAP, que son inherentemente de funcionalidad restringida en relación con los navegadores Web totalmente funcionales. Debido a las limitaciones inherentes de los navegadores de teléfonos móviles, a menudo no es posible convertir ciertos elementos de los sitios web B2C existentes para su uso en navegadores WAP, como, por ejemplo, componentes en Flash enriquecido, applets Java y aplicaciones o interfaces descargables. Además, la comunicación móvil representa un riesgo de seguridad ya que las señales de transmisión son susceptibles de escuchas e interceptación, necesitando la introducción de medidas de seguridad adicionales.

Por esta razón, para hacer que las aplicaciones comerciales B2C existentes estén disponibles desde teléfonos móviles, se hace necesario crear una aplicación B2C más compleja que sea compatible tanto con antiguos elementos de la aplicación comercial, así como con pantallas de dispositivos móviles de pequeño tamaño. Tal procedimiento es tedioso e innecesariamente caro. En particular, se hace necesario establecer un sistema de autenticación y seguridad que pueda usarse en navegadores para teléfonos móviles, pero siga siendo compatible con el del sitio web B2C existente, lo cual lleva mucho tiempo.

Una aplicación comercial B2C está constituida típicamente por un servidor de aplicaciones que ejecuta un programa de software servidor, y al menos un servicio de acceso de usuario que se comunica con el servidor de aplicaciones por medio de una red de comunicación como Internet, y que ejecuta un programa de software cliente. El programa de software cliente recibe solicitudes e instrucciones de un usuario y transmite estas al servidor de aplicaciones a lo largo de la red de comunicación. El programa de software servidor genera respuestas que corresponden a las solicitudes recibidas y transmite las respuestas de vuelta al servicio de acceso de usuario, donde el programa de software cliente las muestra al usuario de manera inteligible en el contexto de la aplicación comercial. El programa de software cliente puede ser descargado e instalado en la estación del usuario, o puede estar constituido por código que se ejecuta desde dentro de un navegador de Internet. La solicitud PCT Wob2 /31675 A1 “Method and system of automating Internet interactions” describe un servidor central para mantener una base de datos de información de usuario (por ejemplo, información de conexión e información de cuentas de usuarios) para uso en el suministro de información de usuario a otros sitios web.

Objeto de la invención

Un objeto de esta invención es proporcionar un sistema para realizar transacciones comerciales en línea, y un procedimiento de funcionamiento del mismo que paliará, al menos en parte, las dificultades y desventajas mencionadas anteriormente.

Un objeto adicional de esta invención es proporcionar un sistema de autenticación y seguridad para transacciones comerciales en línea realizadas desde plataformas móviles, y un procedimiento de autenticación de usuarios en transacciones comerciales en línea iniciadas desde plataformas móviles que paliará, al menos en parte, las dificultades y desventajas mencionadas anteriormente.

Resumen de la invención

De acuerdo con esta invención, se proporciona un sistema para realizar transacciones comerciales, que comprende:

un servidor de aplicaciones utilizable para alojar una aplicación de software para llevar a cabo transacciones comerciales;
una base de datos de usuarios de aplicaciones de usuarios autorizados capaces de acceder al servidor de aplicaciones para realizar transacciones comerciales en el mismo, siendo cada usuario autorizado de la base de datos de usuarios de aplicaciones identificable de manera única por medio de información de usuario correspondiente;
un servidor proxy en comunicación con el servidor de aplicaciones y accesible por una pluralidad de usuarios registrados desde terminales de acceso móviles respectivos; y
una base de datos proxy de usuarios autorizados de la base de datos de usuarios de aplicaciones que también están registrados para acceder al servidor de aplicaciones a través del servidor proxy desde sus terminales de acceso móviles respectivos, siendo cada usuario registrado en la base de datos proxy identificable de manera única por medio de un código de identificación de usuario correspondiente, proporcionando la base de datos proxy, para cada usuario registrado, una correlación del código de identificación de usuario de ese usuario y la información de usuario correspondiente del usuario contenida en la base de datos de usuarios de aplicaciones;
en el que: el servidor proxy es utilizable para proporcionar a cada uno de la pluralidad de usuarios registrados acceso al servidor de aplicaciones desde el terminal de acceso móvil respectivo de ese usuario retransmitiendo los datos recibidos por el servidor proxy desde los terminales de acceso móviles al servidor de aplicaciones y retransmitiendo los datos recibidos por el servidor proxy desde el servidor de aplicaciones a los terminales de acceso móviles; y
la información de usuario es transferible desde el servidor proxy al servidor de aplicaciones sin transferir la información de usuario entre los terminales de acceso móviles y el servidor proxy.

Características adicionales de la invención prevén que la base de datos proxy almacene la información de usuario correspondiente de cada usuario registrado en formato cifrado, que el sistema incluya un motor de cifrado capaz de cifrar cualquier dato pasado entre el servidor proxy y el terminal de acceso móvil de cada usuario registrado, que la base de datos proxy también almacene una clave de cifrado activa para cada usuario registrado, siendo usada la clave de cifrado activa por el motor de cifrado para cifrar y descifrar los datos pasados entre el servidor proxy y el terminal de acceso móvil del usuario, que el motor de cifrado sea dinámico, usando una clave de cifrado diferente durante cada sesión en la que el usuario acceda al servidor de aplicaciones desde su terminal de acceso móvil respectivo, que el motor de cifrado genere, durante cada sesión, una clave de cifrado adicional para el usuario y transfiera la clave de cifrado adicional al terminal de acceso móvil del usuario para almacenamiento en el mismo, y que el motor de cifrado haga automáticamente que la clave de cifrado adicional almacenada se convierta en la clave de cifrado activa en una sesión siguiente en la que el usuario acceda al servidor de aplicaciones desde el terminal de acceso móvil.

Otras características adicionales de la invención prevén que el terminal de acceso móvil sea un teléfono móvil que tenga un número de teléfono correspondiente, que la información de usuario sea un nombre de conexión y una contraseña, que el servidor proxy sirva de formulario de registro móvil accesible por el usuario para registrarse para acceso al servidor de aplicaciones desde el teléfono móvil respectivo del usuario, que el formulario de registro se sirva como una página HTTP accesible por medio de un navegador web totalmente funcional, y/o como una página WAP accesible por medio de un navegador de funcionalidad reducida, que el formulario de registro móvil requiera que el usuario presente un nombre de conexión y una contraseña, un número de teléfono del teléfono móvil desde el que el usuario desee acceder al servidor de aplicaciones, y un PIN de conexión seleccionado, que el servidor proxy transfiera al servidor de aplicaciones el nombre de conexión y la contraseña presentados para ser validados frente al nombre de conexión y la contraseña del usuario ya almacenados en la base de datos de usuarios de aplicaciones, que el servidor proxy asigne un código de identificación de usuario al usuario y genere una clave de cifrado cuando el nombre y la contraseña del usuario han sido validados exitosamente por el servidor de aplicaciones, que el servidor proxy combine el código de identificación de usuario y la clave de cifrado como un código de validación de dos partes y transfiera el código de validación al teléfono móvil del usuario, que el servidor proxy autentique al usuario como una función de reentrada del código de validación transferido por el usuario en el formulario de registro, que el servidor proxy cifre el nombre de conexión y la contraseña del usuario, después de la autenticación del usuario, usando una función del código PIN de conexión seleccionado del usuario como clave de cifrado, y que el servidor proxy almacene el nombre y la contraseña cifrados del usuario en la base de datos proxy por el código de identificación de usuario.

Otras características adicionales de la invención prevén que el usuario inicie el acceso al servidor de aplicaciones introduciendo su PIN de conexión en el teléfono móvil, que el teléfono móvil cifre el PIN de conexión usando la clave de cifrado activa, encabece el PIN de conexión cifrado con el código de identificación de usuario y transfiera el PIN de conexión cifrado encabezado al servidor proxy, que el servidor proxy recupere de la base de datos proxy la clave de cifrado activa como una función del código de identificación de usuario encabezado, que el servidor proxy descifre el PIN de conexión cifrado usando la clave de cifrado activa recuperada, que el servidor proxy recupere de la base de datos proxy el nombre de conexión y la contraseña cifrados del usuario, descifre el nombre de conexión y la contraseña cifrados usando una función del PIN de conexión descifrado del usuario como clave de cifrado, y transfiera al servidor de aplicaciones el nombre de conexión y la contraseña descifrados del usuario para efectuar una conexión, que el teléfono móvil cifre cualquier dato de aplicación con la clave de cifrado activa y encabece los datos de aplicación cifrados con el código de identificación de usuario antes de transferir los datos de aplicación cifrados al servidor proxy, y que el servidor proxy descifre los datos de aplicación cifrados usando la clave de cifrado activa y transfiera al servidor de aplicaciones los datos de aplicación descifrados para procesamiento.

También está previsto que el sistema permita que un usuario registre al menos un instrumento de pago para pagar las compras realizadas en el servidor de aplicaciones, que el al menos un instrumento de pago sea una tarjeta de débito o una tarjeta de crédito, que el usuario registre el al menos un instrumento de pago introduciendo en el teléfono móvil datos relacionados con el instrumento de pago, junto con un PIN de compra y el nombre de conexión y la contraseña del usuario, que el servidor proxy transfiera al servidor de aplicaciones los datos del instrumento de pago introducidos, que el servidor de aplicaciones utilice los datos del instrumento de pago transferidos para validar el instrumento de pago por medio de una pasarela de pago, que el servidor proxy cifre los datos del instrumento de pago validados usando una función del PIN de compra como clave de cifrado, y que el servidor proxy almacene en la base de datos proxy los datos del instrumento de pago validados cifrados.

Además está previsto que el sistema permita que un usuario utilice un instrumento de pago registrado previamente para pagar una compra realizada en el servidor de aplicaciones, que el servidor proxy transmita al teléfono móvil para visualización en el mismo los datos cifrados relacionados con todos los instrumentos de pago registrados previamente por el usuario, que el teléfono móvil descifre los datos de pago recibidos y visualice como un menú en el teléfono móvil los datos descifrados relacionados con todos los instrumentos de pago registrados previamente, que el usuario seleccione del menú un instrumento de pago deseado, de los instrumentos de pago registrados previamente, para usarse para el pago e introduzca un valor de la compra junto con el PIN de compra del usuario, que el terminal de acceso móvil cifre los datos introducidos usando la clave de cifrado activa y transfiera los datos cifrados al servidor proxy, que el servidor proxy obtenga de la base de datos proxy la clave de cifrado activa del usuario y descifre los datos transferidos usando la clave de cifrado activa recuperada, y que el servidor proxy transfiera los datos cifrados al servidor de aplicaciones para efectuar el pago por la transacción de compra.

La invención se extiende a un procedimiento de funcionamiento de un sistema para realizar transacciones comerciales que comprende las etapas de:

alojar, en un servidor de aplicaciones, una aplicación de software para llevar a cabo transacciones comerciales;
recopilar una base de datos de usuarios de aplicaciones de usuarios autorizados capaces de acceder al servidor de aplicaciones para realizar transacciones comerciales en el mismo e identificar de manera única cada usuario autorizado de la base de datos de usuarios de aplicaciones por medio de información de usuario correspondiente;
proporcionar un servidor proxyen comunicación con el servidor de aplicaciones y accesible por una pluralidad de usuarios registrados desde terminales de acceso móviles respectivos; y
establecer una base de datos proxy de usuarios autorizados de la base de datos de usuarios de aplicaciones que también están registrados para acceder al servidor de aplicaciones a través del servidor proxy desde sus terminales de acceso móviles respectivos, e identificar de manera única cada usuario registrado en la base de datos proxy por medio de un código de identificación de usuario correspondiente; y determinar, para cada usuario registrado en la base de datos proxy, una correlación del código de identificación de usuario de ese usuario y la información de usuario correspondiente del usuario contenida en la base de datos de usuarios de aplicaciones;
en el que: el servidor proxy proporciona a cada uno de la pluralidad de usuarios registrados acceso al servidor de aplicaciones desde el terminal de acceso móvil respectivo de ese usuario retransmitiendo los datos recibidos por el servidor proxy desde los terminales de acceso móviles al servidor de aplicaciones y retransmitiendo los datos recibidos por el servidor proxy desde el servidor de aplicaciones a los terminales de acceso móviles; y
la información de usuario es transferible desde el servidor proxy al servidor de aplicaciones sin transferir la información de usuario entre los terminales de acceso móviles y el servidor proxy.

Además está previsto que el procedimiento incluya la etapa adicional de almacenar en la base de datos proxy la información de usuario correspondiente de cada usuario registrado en formato cifrado, cifrar cualquier dato pasado entre el servidor proxy y el terminal de acceso móvil de cada usuario registrado, almacenar también en la base de datos proxy una clave de cifrado activa para cada usuario registrado, siendo usada la clave de cifrado activa para

cifrar y descifrar los datos pasados entre el servidor proxy y el terminal de acceso móvil del usuario, cifrar dinámicamente cualquier dato pasado entre el servidor proxy y el terminal de acceso móvil de cada usuario registrado usando una clave de cifrado diferente durante cada sesión en la que el usuario accede al servidor de aplicaciones desde su terminal de acceso móvil respectivo, generar, durante cada sesión, una clave de cifrado adicional para el usuario y transferir la clave de cifrado adicional al terminal de acceso móvil del usuario para almacenamiento en el mismo, y hacer automáticamente que la clave de cifrado adicional almacenada se convierta en la clave de cifrado activa en una sesión siguiente en la que el usuario acceda al servidor de aplicaciones desde el terminal de acceso móvil.

Además está previsto usar un teléfono móvil como terminal de acceso móvil, teniendo el teléfono móvil un número de teléfono correspondiente, usar un nombre de conexión y una contraseña como la información de usuario, hacer que el servidor proxy sirva de formulario de registro móvil accesible por el usuario para registrarse para acceso al servidor de aplicaciones desde el teléfono móvil respectivo del usuario, servir el formulario de registro como una página HTTP accesible por medio de un navegador web totalmente funcional, y/o como una página WAP accesible por medio de un navegador de funcionalidad reducida, requerir que el usuario presente, en el formulario de registro móvil, un nombre de conexión y una contraseña, un número de teléfono del teléfono móvil desde el que el usuario desee acceder al servidor de aplicaciones, y un PIN de conexión seleccionado, transferir el nombre de conexión y la contraseña presentados desde el servidor proxy al servidor de aplicaciones para ser validados frente al nombre de conexión y la contraseña del usuario ya almacenados en la base de datos de usuarios de aplicaciones, asignar un código de identificación de usuario al usuario y generar una clave de cifrado cuando el nombre y la contraseña del usuario han sido validados exitosamente por el servidor de aplicaciones, combinar el código de identificación de usuario y la clave de cifrado como un código de validación de dos partes y transferir el código de validación al teléfono móvil del usuario, autenticar al usuario como una función de reentrada del código de validación transferido por el usuario en el formulario de registro, cifrar el nombre de conexión y la contraseña del usuario, después de la autenticación del usuario, usando una función del código PIN de conexión seleccionado del usuario como clave de cifrado, y almacenar el nombre y la contraseña cifrados del usuario en la base de datos proxy por el código de identificación de usuario.

Además está previsto iniciar el acceso al servidor de aplicaciones introduciendo un PIN de conexión en el teléfono móvil, cifrar el PIN de conexión en el teléfono móvil usando la clave de cifrado activa, encabezar el PIN de conexión cifrado con el código de identificación de usuario y transferir el PIN de conexión cifrado encabezado al servidor proxy, recuperar de la base de datos proxy la clave de cifrado activa como una función del código de identificación de usuario encabezado, descifrar en el servidor proxy el PIN de conexión cifrado usando la clave de cifrado activa recuperada, recuperar de la base de datos proxy el nombre de conexión y la contraseña cifrados del usuario, descifrar el nombre de conexión y la contraseña cifrados usando una función del PIN de conexión descifrado del usuario como clave de cifrado, y transferir al servidor de aplicaciones el nombre de conexión y la contraseña descifrados del usuario para efectuar una conexión, cifrar en el teléfono móvil cualquier dato de aplicación con la clave de cifrado activa y encabezar los datos de aplicación cifrados con el código de identificación de usuario antes de transferir los datos de aplicación cifrados al servidor proxy, y descifrar en el servidor proxy los datos de aplicación cifrados usando la clave de cifrado activa y transferir al servidor de aplicaciones los datos de aplicación descifrados para procesamiento.

También está previsto permitir que un usuario registre al menos un instrumento de pago para pagar las compras realizadas en el servidor de aplicaciones, registrar el al menos un instrumento de pago introduciendo en el teléfono móvil datos relacionados con el instrumento de pago, junto con un PIN de compra y el nombre de conexión y la contraseña del usuario, transferir al servidor de aplicaciones los datos del instrumento de pago introducidos, utilizar los datos del instrumento de pago transferidos para validar el instrumento de pago por medio de una pasarela de pago, cifrar en el servidor proxy los datos del instrumento de pago validados usando una función del PIN de compra como clave de cifrado, y almacenar en la base de datos proxy los datos del instrumento de pago validados cifrados.

Además está previsto permitir que un usuario utilice un instrumento de pago registrado previamente para pagar una compra realizada en el servidor de aplicaciones, transferir los datos cifrados relacionados con todos los instrumentos de pago registrados previamente por el usuario desde el servidor proxy al teléfono móvil para visualización en el mismo, descifrar en el teléfono móvil los datos de pago recibidos y visualizar en el mismo como un menú los datos descifrados relacionados con todos los instrumentos de pago registrados previamente, seleccionar del menú un instrumento de pago deseado de los instrumentos de pago registrados previamente para usarse para el pago e introducir un valor de la compra junto con el PIN de compra del usuario, cifrar en el terminal de acceso móvil los datos introducidos usando la clave de cifrado activa y transferir los datos cifrados al servidor proxy, obtener de la base de datos proxy la clave de cifrado activa del usuario y descifrar los datos transferidos usando la clave de cifrado activa recuperada, y transferir los datos cifrados desde el servidor proxy al servidor de aplicaciones para efectuar el pago por la transacción de compra.

Breve descripción de los dibujos

Más adelante se describe una realización preferida de la invención, únicamente a modo de ejemplo, y con referencia a los dibujos anteriormente mencionados, en los que:

La Figura 1 es una representación funcional de un sistema para realizar transacciones comerciales en línea, según la invención.

Las Figuras 2A y 2B son organigramas de un procedimiento de registro para permitir el uso del sistema de la Figura 1 desde un teléfono móvil.

Las Figuras 3A, 3B, 3C y 3D son organigramas de un procedimiento de conexión para permitir el uso del sistema de la Figura 1 desde un teléfono móvil.

La Figura 4 es un organigrama de un procedimiento de registro de instrumentos de pago para el sistema de la Figura 1, llevado a cabo desde un teléfono móvil.

Las Figuras 5A y 5B son organigramas de una transacción de compra en el sistema de la Figura 1, realizada desde un teléfono móvil.

Descripción detallada de la invención

Haciendo referencia a las Figuras 1 a 5, en las que las características iguales de la invención están indicadas por números iguales, un sistema para realizar transacciones comerciales en línea está indicado en general por el número de referencia (1). Esta realización de la invención se describirá con referencia particular a transacciones comerciales que implican la compra y reembolso de crédito y la colocación de apuestas en juegos de azar ofrecidos por un casino en línea. Ha de entenderse claramente, sin embargo, que el uso de la invención no está limitado a esta aplicación particular, sino que también se extiende a su uso en otros tipos de transacciones comerciales en línea.

Tal como se ilustra en la Figura 1, el sistema (1) incluye un servidor de aplicaciones (2) que es accesible desde al menos un servicio de acceso del usuario en forma de una estación de trabajo informática (3) alejada del servidor de aplicaciones. La estación de trabajo informática (3), que tiene una pantalla asociada (4), se comunica con el servidor de aplicaciones (2) por medio de una red de comunicación (5) que es, en esta realización, Internet. El servidor de aplicaciones (2) aloja un sitio web B2C (6) que es accesible por un usuario, desde la estación de trabajo informática (3), por medio de un navegador Web totalmente funcional como, por ejemplo, Microsoft Internet Explorer o Mozilla Firefox. Estos navegadores web particulares son bien conocidos y son comercializados por la Microsoft Corporation de Redmond, Washington, EE.UU. y la Mozilla Foundation de California, EE.UU., respectivamente.

El sitio web B2C (6) proporciona al usuario acceso a una aplicación comercial en forma de un casino en línea que ofrece uno o más juegos de azar para ser jugados por el usuario. La estación de trabajo informática (3) ejecuta uno o más programas de software clientes, cada uno de los cuales simula el progreso de un juego de azar diferente. El funcionamiento genérico de los programas de software clientes se describirá con más detalle en la descripción que viene a continuación.

El servidor de aplicaciones (2) incluye un generador de eventos aleatorios (no mostrado) en forma de un programa informático que es ejecutable para generar eventos aleatorios en los cuales se basa el resultado de uno cualquiera de los juegos de azar. Como ilustración, uno de los programas de software clientes de la estación de trabajo informática (3) simula un juego de ruleta y, en este ejemplo, el programa de generación de eventos aleatorios (no mostrado) es ejecutable para seleccionar, aleatoriamente, un número entero entre 0 y 36 que es mostrado por el programa de software cliente en la pantalla (4) como simulación de una rueda de ruleta giratoria que se va parando y una bola de giro contrario que se detiene en una posición correspondiente de 37 posiciones demarcadas en la rueda de ruleta. Como ilustración adicional, otro de los programas de software clientes simula un juego de póquer tapado y el programa de generación de eventos aleatorios es ejecutable para generar cinco números enteros aleatorios entre 1 y 52 que son presentados al usuario por el programa de software cliente correspondiente, en la pantalla, como cinco cartas de juego que constituyen una mano particular de póquer.

Un jugador que desee usar el sistema (1) y el sitio web B2C (6) para llevar a cabo transacciones comerciales como, por ejemplo, crédito de compra, hacer una apuesta en un turno de uno cualquiera de los juegos de azar, y abonar el crédito acumulado, en primer lugar se le requiere que se registre como un usuario autorizado y que cree una cuenta en el servidor de aplicaciones (2). Para registrarse, se requiere que el usuario rellene un formulario de registro (no mostrado) que se muestra al usuario como parte del sitio web B2C. El formulario de registro requiere que el usuario facilite detalles personales como, por ejemplo, nombre, dirección de residencia, fecha de nacimiento y dirección de correo electrónico. Una vez que el usuario ha rellenado el formulario, el servidor de aplicaciones (2) asigna un nombre de conexión específico al usuario e incita al usuario a seleccionar una contraseña privada. El par de datos que está constituido por el nombre de conexión y la contraseña del usuario se denominará en esta memoria descriptiva, por comodidad, como la Información de usuario. El servidor de aplicaciones (2) almacena fuera la Información de usuario en una base de datos de usuarios de aplicaciones (7) asociada con el servidor de aplicaciones (2). Una vez que se registra de esta manera, el usuario es un usuario autorizado y es libre de usar la aplicación B2C de casino en línea simplemente introduciendo de nuevo su Información de usuario cuando accede al

sitio web B2C (6).

Se apreciará por parte de los expertos en la materia que el sistema (1) tal como se describió anteriormente permite a cualquier usuario que tenga una estación de trabajo informática con acceso a Internet (3) registrarse en el servidor de aplicaciones (2) por medio del sitio web B2C y usar la aplicación de casino en línea subordinada en el servidor de aplicaciones (2) para realizar transacciones comerciales, es decir, relacionadas con el juego. Además, la estación de trabajo informática (3) puede ser un ordenador de escritorio, un ordenador personal o un ordenador de mano ("PDA") con capacidad de acceso a Internet por medio de una red cableada o inalámbrica.

Para proporcionar acceso a la aplicación B2C desde un dispositivo de telecomunicación móvil como un teléfono móvil (9), el sistema (1) incluye un servidor proxy (10) que tiene una base de datos proxy (11) asociada. El servidor proxy (10) puede se puede comunicar con el servidor de aplicaciones (2) por medio de Internet, y aloja un sitio web proxy (12) que es accesible por el usuario para registrarse para acceder a la aplicación B2C desde el teléfono móvil (9). El teléfono móvil (9) tiene acceso a Internet, preferentemente por medio de estándares de comunicación como el Servicio General de Radio por Paquetes ("GPRS") o el Servicio Universal de Telecomunicaciones Móviles ("UMTS"), que son ambos bien conocidos en la técnica. El sitio web proxy (12) está disponible para el usuario tanto en una versión de Protocolo de Transferencia de Hipertexto ("HTTP") como en una versión de Protocolo de Aplicaciones Inalámbricas ("WAP"). Además, el sitio web proxy (12) también puede estar disponible en formato de Protocolo de Transferencia de Hipertexto (Seguro) ("HTTPS") para transacciones seguras, si es necesario. Para registrarse para acceso móvil a la aplicación B2C, el usuario debe registrarse primero en el servidor de aplicaciones (2) y la Información de usuario del usuario ya debe estar almacenada en la base de datos de usuarios de aplicaciones (7).

Se desea permitir a los usuarios acceder a la aplicación B2C desde teléfonos móviles (9) sin necesitar ninguna modificación de la propia aplicación B2C ni de ningún subsistema de la misma, como un subsistema de identificación de usuario y seguridad (no mostrado). Este objetivo se consigue interponiendo el servidor proxy (10) como elemento intermediario entre el teléfono móvil (9) y el servidor de aplicaciones (2), con todos los datos recibidos por el servidor proxy desde el teléfono móvil siendo retransmitidos por el servidor proxy al servidor de aplicaciones y viceversa, y sin tener que transferir la Información de usuario entre un teléfono móvil y el servidor proxy por el aire.

Registro para uso móvil

El procedimiento de registro se describe a continuación con referencia a las Figuras 2A y 2B. Para registrarse para acceso móvil en la aplicación B2C, un usuario accede selectivamente a la versión HTTP o la versión WAP del sitio web proxy (12) por medio de la estación de trabajo informática (3) o el teléfono móvil (9), respectivamente. El sitio web proxy (12) presenta al usuario un formulario de registro móvil (no mostrado) en el que se requiere que el usuario introduzca, en la etapa 100, su Información de usuario, es decir, el nombre de usuario y la contraseña tal como se registró previamente en el servidor de aplicaciones (2), junto con la siguiente información adicional:

1. un número de teléfono del teléfono móvil (9) desde el cual se desea el acceso a la aplicación B2C; y

2. un Número de Identificación Personal ("código PIN de conexión") seleccionado por el usuario en un formato que sea cómodo para introducir en un teclado numérico del teléfono móvil (9) como, por ejemplo, un código numérico de 4 dígitos.

El servidor proxy (10) pasa, en la etapa 101, la Información de usuario al servidor de aplicaciones (2), que comprueba la validez de la Información de usuario frente al contenido de la base de datos de usuarios de aplicaciones (7), tal como se indica por la etapa 102. El servidor de aplicaciones (2) notifica luego al servidor proxy (10) si la Información de usuario ha resultado ser válida o inválida. Si la Información de usuario es inválida, el servidor proxy (10) genera una respuesta de error en la etapa 103 y muestra un mensaje de error al usuario en el sitio web proxy (12). Si la Información de usuario resulta ser válida, el registro móvil pasa a la siguiente fase, en la que el servidor proxy (10):

- primero asigna, en la etapa 104, un código de identificación de usuario ("UIC") al usuario y almacena el UIC en la base de datos proxy (11);
- luego construye un código de validación, en la etapa 105, en forma de un código de dos partes separadas por un carácter separador que, en esta realización, es un carácter "guión". La primera parte del código de validación es el UIC, mientras que la segunda parte del código de validación es un código de cifrado de cuatro caracteres que es generado automáticamente por el servidor proxy (10) y almacenado alejado en la base de datos proxy (11), indexado por el UIC; y
- también cifra, en la etapa 106, el código PIN de conexión y la Información de usuario usando una función HASH del código de cifrado de cuatro caracteres como clave de cifrado.

Para cerciorarse de que el usuario que está usando el teléfono móvil (9) es, de hecho, el mismo usuario que se registró en el servidor de aplicaciones (2), un mensaje que cumple con el bien conocido estándar del Servicio de Mensajes Cortos ("SMS") es enviado, en la etapa 107, al número de teléfono del teléfono móvil (9) proporcionado por el usuario en la etapa 100 anterior. El mensaje enviado incluye el código de validación tal como es construido

por el servidor proxy (10), así como una dirección de hiperenlace.

Si el usuario está registrándose para acceso móvil desde la estación de trabajo informática (3) mediante la versión HTTP del sitio web proxy (12), simplemente se le requiere que introduzca el código de validación contenido en el mensaje enviado dentro del formulario de registro móvil para completar el procedimiento de registro móvil. Si, por otra parte, el usuario está registrándose desde la versión WAP del sitio web proxy (12) por medio del teléfono móvil (9), se requiere que el usuario active el hiperenlace contenido en el mensaje enviado, lo cual hace que el navegador WAP del teléfono móvil (9) muestre un nuevo formulario de registro en el teléfono. Luego se requiere que el usuario vuelva a introducir, en la etapa 108, su Información de usuario una vez más en este formulario de registro, junto con el código de validación. En esta parte del procedimiento de registro, el servidor proxy (10):

1. usa el UIC contenido en la primera parte del código de validación como índice para recuperar la Información de usuario cifrada de la base de datos proxy (11) en la etapa 109;

2. luego descifra la Información de usuario cifrada del usuario procedente de la base de datos proxy (11), usando el código de validación introducido como clave de cifrado, en la etapa 110;

3. compara, en la etapa 111, la Información de usuario descifrada con la información de usuario introducida;

4. transmite una respuesta de error para su presentación al usuario en el navegador del usuario si la Información de usuario descifrada e introducida no es idéntica; y

5. almacena con seguridad la Información de usuario introducida en la base de datos proxy (11) si la Información de usuario descifrada e introducida es idéntica.

Se apreciará por parte de los expertos en la materia que el procedimiento anterior de: generar el código de validación, cifrar la Información de usuario y almacenarla en la base de datos proxy (11), enviar el código de validación al teléfono móvil (9), requerir que el usuario vuelva a introducir la Información de usuario y el código de validación enviado, usar el código de validación reintroducido para descifrar la Información de usuario almacenada, cifrada procedente de la base de datos proxy, y comparar la Información de usuario descifrada con la Información de usuario reintroducida es tanto necesario como suficiente para asegurar que el usuario que ha solicitado acceso móvil a la aplicación B2C es, de hecho, el mismo usuario que el registrado en el servidor de aplicaciones (2).

Una vez que la correcta identidad del registrante ha sido verificada como se esbozó anteriormente, el servidor proxy (10):

1. genera automáticamente, en la etapa 112, una clave de cifrado de 16 caracteres y almacena la clave de cifrado en la base de datos proxy (11). El servidor proxy (10) usa el UIC como índice para localizar la clave de cifrado en la base de datos proxy (11) que corresponde al usuario;

2. construye, en la etapa 113, un código de activación de dos partes en el que las dos partes están separadas por un carácter separador, en esta realización un carácter “guión”. La primera parte del código de activación es el UIC tal como fue asignado al usuario por el servidor proxy (10) y que está almacenado en la base de datos proxy (11), mientras que la segunda parte del código de activación es la clave de cifrado de 16 caracteres generada en la etapa 112;

3. cifra la Información de usuario usando una función Hash del PIN seleccionado por el usuario como clave de cifrado y almacena la información de usuario cifrada en la base de datos proxy (11) indexada por el UIC; y

4. envía un mensaje WAP al teléfono móvil (9) que contiene un reconocimiento de que la Información de usuario descifrada y reintroducida es idéntica, un enlace de descarga a una página web dedicada desde la cual un programa de software cliente móvil asociado con la aplicación B2C puede ser descargado al teléfono móvil (9), y el código de activación generado en la etapa 113 anterior para el programa de software cliente móvil.

La clave de cifrado de 16 caracteres tal como está contenida en la segunda parte del código de activación se convertirá en una clave activa usada para cifrar los datos de aplicación que son enviados por el teléfono móvil (9) al servidor proxy (10) durante la primera sesión del usuario en la que él accede a la aplicación B2C desde el teléfono móvil (9). El funcionamiento de la clave de cifrado de 16 caracteres se describirá con mayor detalle en la descripción que viene a continuación.

Después de la recepción del mensaje WAP enviado, el usuario accede a la página web dedicada para solicitar, en la etapa 114, una descarga del programa de software cliente móvil. El servidor proxy (10) adjunta, en la etapa 115, el código de activación al archivo de descarga para asegurarse de que el usuario no tiene que introducir el código de activación en el teclado numérico del teléfono móvil (9), lo cual puede ser tedioso y llevar mucho tiempo. Se

apreciará por parte de los expertos en la materia que el código de activación actúa como identificador único que es inyectado dentro de la descarga del programa de software cliente móvil y que es único para esa aplicación B2C específica y para ese usuario específico.

Una vez descargado desde el servidor proxy (10), el programa de software cliente móvil puede instalarse en el teléfono móvil (9), en la etapa 116, y la aplicación B2C está entonces lista para que el usuario acceda a ella. La instalación del programa de software cliente móvil tiene como resultado que se visualiza un icono de aplicación (no mostrado) en el teléfono móvil (9). La función del programa de software cliente móvil es análoga a la del programa de software cliente en la estación de trabajo informática (3) descrito anteriormente, concretamente, en esta realización, simular el progreso de un juego de azar ofrecido por el casino en línea.

Conexión a la aplicación

El procedimiento de conexión a la aplicación se describe con referencia a las Figuras 3A a 3D. El usuario lanza el programa de software cliente móvil activando el icono de aplicación correspondiente (no mostrado) en el teléfono móvil (9) en la etapa 200. La activación del icono de aplicación (no mostrado) por primera vez después del registro para uso móvil de la aplicación B2C hace que se visualice una pantalla de inicio de aplicación en el teléfono móvil (9). La pulsación de cualquier tecla en el teléfono móvil (9) hace que la pantalla de inicio sea sustituida por un formulario que tiene un campo en el que el usuario debe introducir el código de activación. Para ayudar al usuario, este campo muestra, en 201, el código de activación generado por el servidor proxy, que simplemente se requiere que el usuario lo confirme. Después de que el código de activación ha sido confirmado, se requiere que el usuario introduzca, en la etapa 202, su PIN de 4 dígitos preseleccionado por medio de un teclado numérico (no mostrado) asociado con el teléfono móvil (9).

En la descripción que viene a continuación, la clave de cifrado de 16 caracteres que forma la segunda parte del código de activación se denominará, por comodidad, la “clave de cifrado activa”.

El programa de software cliente móvil instalado en el teléfono móvil (9) cifra, en 203, el PIN introducido por el usuario, junto con llamadas de funciones específicas del juego, usando la clave de cifrado activa. El teléfono móvil (9) encabeza el PIN cifrado con el UIC y el carácter separador y transmite el resultado como un paquete al servidor proxy (10). El servidor proxy (10) quita el UIC del paquete y usa el UIC como índice para recuperar, en 204, la clave de cifrado correspondiente del usuario procedente de la base de datos proxy (11), que es idéntica a la clave de cifrado activa en el teléfono móvil (9) como resultado de una finalización exitosa del procedimiento de registro para uso del móvil descrito en la sección previa. Luego el servidor proxy (10) descifra, en la etapa 205, el PIN cifrado recibido desde el teléfono móvil (9), usando la clave de cifrado activa recuperada. El código PIN descifrado resultante es cifrado mediante una función HASH en la etapa 206 y el resultado se usa como nueva clave de cifrado para descifrar, en 207, la Información de usuario cifrada correspondiente del usuario (es decir, el nombre de conexión y la contraseña del usuario) que se almacena en la base de datos proxy (11). El servidor proxy (10) transmite la Información de usuario descifrada al servidor de aplicaciones (2) para efectuar una transacción de conexión de usuario en la aplicación B2C en la etapa 208.

Si la transacción de conexión de usuario es exitosa, el servidor de aplicaciones (2) obtiene un identificador de sesión de la aplicación B2C, en la etapa 209, y devuelve el identificador de sesión al servidor proxy (10). El servidor proxy (10) almacena el identificador de sesión en la base de datos proxy (11), en la etapa 210, y transmite una respuesta cifrada al teléfono móvil (9), que se construye de la siguiente manera:

1. el servidor proxy (10) cifra una confirmación de “conexión correcta” usando la clave de cifrado activa del usuario almacenada en la base de datos proxy (11);

2. el servidor proxy (10) genera una nueva clave de cifrado de 16 caracteres, en la etapa 211, y la almacena en la base de datos proxy (11) bajo la UIC del usuario; y

3. la nueva clave de cifrado se cifra usando la clave de cifrado activa y se concatena, en 212, con la confirmación de “conexión correcta” descrita en el párrafo 1.) anterior.

La cadena concatenada constituye la respuesta a la transacción de conexión llevada a cabo por el usuario en el teléfono móvil (9).

El programa de software cliente móvil del teléfono móvil (9) descifra la respuesta a la transacción de conexión, en la etapa 213, usando la clave de cifrado activa. Si el programa de software cliente móvil detecta la respuesta de “conexión correcta”, en la etapa 214, la nueva clave de cifrado de 16 caracteres contenida en la respuesta se almacena, en 215, en la memoria no volátil (no mostrada) en el teléfono móvil (9), junto con el UIC, como nueva clave de activación. Esta nueva clave de cifrado se convertirá en la clave de cifrado activa para la siguiente sesión del usuario de la aplicación B2C. Durante la siguiente sesión del usuario, se enviará una nueva clave de cifrado adicional al teléfono móvil (9) de la misma manera para uso en la sesión subsiguiente del usuario, y así sucesivamente, de manera recurrente.

Una vez que la fase de conexión de la transacción comercial se ha completado exitosamente tal como se describió anteriormente, cualquier dato de aplicación que haya de ser transmitido por el teléfono móvil (9) al servidor de aplicaciones (2) en primer lugar es cifrado, en la etapa 216, con la clave de cifrado activa para la sesión actual en el servidor de aplicaciones. La clave de cifrado para la siguiente sesión del usuario en el servidor de aplicaciones (2), que ya ha sido almacenada en el teléfono móvil (9) permanece inactiva y sin usar hasta que el usuario inicia la siguiente sesión en el servidor de aplicaciones, lo cual podría ser después de un periodo de tiempo considerable. De esta manera, el código de activación actúa como clave de cifrado en curso para la transferencia de datos de aplicación al servidor proxy (10).

Los datos de aplicación cifrados son adjuntados al UIC y transmitidos por el teléfono móvil (9) al servidor proxy (10) para su descifrado. Una vez recibidos por el servidor proxy (10), los datos son descifrados, en 217, y convertidos y procesados para pasar al servidor de aplicaciones (2) como parámetros de estilo web convencional como si el usuario hubiese interactuado directamente con la aplicación B2C en el servidor de aplicaciones, sin la presencia del servidor proxy (10).

Registro para comprar

El procedimiento de registro para comprar se describe con referencia a la Figura 4. Una transacción común que se llevará a cabo por la mayoría de los usuarios autorizados en la aplicación B2C es una transacción de compra para comprar bienes y/o servicios. En la realización actual, el usuario lleva a cabo una transacción de compra para adquirir crédito para hacer apuestas en cualquiera de los juegos de azar ofrecidos por el casino en línea.

Para comprar bienes o servicios, en primer lugar se requiere que el usuario registre previamente uno o más instrumentos de pago, como tarjetas de crédito, tarjetas de débito y similares, de uno en uno. Este registro puede realizarse desde una página HTTP, una página WAP o, más comúnmente, una página HTTPS, en la que se requiere que el usuario introduzca, en la etapa 300, su Información de usuario, junto con datos relacionados con el instrumento de pago deseado como, por ejemplo, un número de tarjeta de crédito, un tipo de tarjeta de crédito, una moneda de pago y una dirección de facturación. También se requiere que el usuario seleccione e introduzca un código PIN de compra, en particular, un código numérico de cuatro dígitos que sea cómodo de introducir desde el teclado numérico del teléfono móvil (9).

El servidor proxy (10) pasa, en la etapa 301, la Información de usuario al servidor de aplicaciones (2), que comprueba la validez de la Información de usuario frente al contenido de la base de datos de usuarios de aplicaciones (7), como se representa en la etapa 302. Cuando se ha finalizado la comprobación de validez de la Información de usuario, el servidor de aplicaciones (2) notifica al servidor proxy (10) si la Información de usuario ha resultado ser válida o inválida. Si la Información de usuario es inválida, el servidor proxy (10) genera una respuesta de error en la etapa 303 y muestra un error al usuario en la página HTTP o WAP. Si la Información de usuario resulta ser válida, el registro de pago pasa a la siguiente fase en la que:

- el servidor de aplicaciones (2) valida, en 304, el instrumento de compra con una pasarela de pago (no mostrada); y
- si el instrumento de compra es validado por la pasarela de pago (no mostrada) los datos del instrumento de pago son cifrados por el servidor proxy (10) en la etapa 305, y almacenados en la base de datos proxy (11), en 306. Los datos del instrumento de pago suministrados por el usuario son cifrados, en la etapa 307, usando una función Hash del código PIN de compra seleccionado por el usuario.

Se apreciará que el usuario puede registrar más de un instrumento de pago y puede utilizar cualquier instrumento de pago registrado para efectuar el pago en una transacción de compra particular.

Transacción de compra

La transacción de compra se describe con referencia a las Figuras 5A y 5B. Una vez que el jugador ha lanzado el programa de software cliente móvil activando el icono de aplicación (no mostrado) en el teléfono móvil (9) y se ha conectado exitosamente a la aplicación B2C en el servidor de aplicaciones (2), el usuario puede seleccionar, de un menú de aplicación, una opción para comprar, como se ilustra en la etapa 400. El teléfono del programa de software de aplicación móvil (9) transmite una solicitud de compra, cifrada con la clave de cifrado activa y encabezada con el UIC, al servidor proxy (10). Luego, el servidor proxy (10), a su vez, descifra la solicitud de compra usando la clave de cifrado activa obtenida de la base de datos proxy (11) y recupera, en 401, los datos del instrumento de pago cifrados relacionados con todos los instrumentos de pago registrados previamente del usuario y devuelve estos datos al teléfono móvil (9). Los datos del instrumento de pago recibidos son descifrados por el programa de software cliente móvil en el teléfono móvil (9) y luego son presentados al usuario, en la etapa 402, como un menú de todos los instrumentos de pago a disposición del usuario.

El usuario es incitado a seleccionar un instrumento de pago preferido de los que figuran en la lista del menú, a

introducir una cantidad de compra, y a introducir su PIN de compra, como se muestra en la etapa 403. Estos datos introducidos por el usuario, junto con un identificador para una transacción de compra, son cifrados, en 404, usando la clave de cifrado activa y encabezados con el UID y el carácter separador, como se describió anteriormente, antes de ser transmitidos al servidor proxy (10). En el momento de recibir los datos introducidos por el usuario, el servidor proxy (10) quita el UIC y usa este para recuperar la clave de cifrado activa del usuario de la base de datos proxy (11), como se ilustra en la etapa 405. Los datos recibidos son descifrados, en 406, usando la clave de cifrado activa recuperada de la base de datos proxy (11). Al PIN de compra descifrado se le aplica una función Hash, en 407, y el resultado se usa para descifrar los datos del instrumento de pago cifrados que corresponden al instrumento de pago preferido seleccionado por el usuario para pagar la compra, que están almacenados en la base de datos proxy (11), como se muestra en la etapa 408. Luego, el servidor proxy (10) reenvía los datos los datos del instrumento de pago preferido descifrados y la cantidad de compra descifrada al servidor de aplicaciones (2) donde se usan para completar un pago en línea, normalmente por medio de una pasarela de pago, de una manera que es bien conocida en la técnica y que, por esta razón, no se describirá detalladamente aquí.

Se apreciará por parte de los expertos en la materia de la invención que toda comunicación entre el teléfono móvil (9) y el servidor proxy (10) está cifrada. Además, la comunicación entre el servidor proxy (10) y el servidor de aplicaciones (2) no requiere que se haga ningún cambio en el servidor de aplicaciones (2), dejando inalterada la antigua aplicación en el servidor de aplicaciones.

Durante el registro para uso móvil, el sistema (1) verifica que el usuario es la misma persona que una que está registrada en la base de datos de usuarios de aplicaciones (7) como un usuario autorizado de la aplicación B2C. El servidor proxy (10) cifra el nombre de conexión y la contraseña del usuario y los almacena en la base de datos proxy (11), permitiendo así que el usuario se conecte al servidor de aplicaciones (2) sin tener que volver a introducir el nombre de conexión y la contraseña y transmitir el nombre de conexión y la contraseña por el aire - sólo es necesario el PIN preseleccionado por el usuario para efectuar la conexión. El código PIN seleccionado por el usuario, como parte del procedimiento de registro, constituye la única información que se requerirá para acceso posterior a la aplicación B2C desde el teléfono móvil (9).

El servidor proxy (10) descarga una versión única, personalizada, de la aplicación B2C al teléfono móvil del usuario (9), que posteriormente es instalada en el teléfono móvil, siendo personalizada la aplicación B2C por medio de un código de activación incorporado que sirve como motor de cifrado dinámico para transferencia de datos en curso, segura, desde el teléfono móvil al servidor proxy (10), y desde allí al servidor de aplicaciones (2).

Se apreciará, además, por parte de los expertos en la materia que el uso de un servidor proxy y una base de datos proxy (11) de una manera descrita anteriormente no requiere que se haga ningún cambio o modificación en el servidor de aplicaciones (2) o la base de datos de usuarios de aplicaciones (7) para acceder a la aplicación B2C desde el teléfono móvil (9). Esta característica permite que las aplicaciones B2C existentes sean migradas a dispositivos de telecomunicación móviles son afectar a los antiguos sistemas intermediarios existentes.

Son posibles numerosas modificaciones de esta realización sin apartarse del ámbito de la invención. En particular, la comunicación entre el servidor proxy (10) y el servidor de aplicaciones también puede ser cifrada, como cuando se usa HTTPS para comunicación segura. Además, la descarga del programa de software cliente móvil puede tener lugar, no desde el servidor proxy (10), sino, en cambio, desde un servidor de descarga separado (no mostrado) que esté en comunicación con el servidor proxy, desconectando así las funciones intermediarias de descarga y comunicación del servidor de descarga. Aún más, la aplicación comercial puede ser una aplicación entre empresas (“B2B”) en contraposición a una aplicación B2C.

Aún más, el sistema (1) también puede permitir que múltiples aplicaciones B2C y B2B sean descargadas e instaladas en el teléfono móvil (9), teniendo cada aplicación comercial un icono de aplicación correspondiente (no mostrado). En esta variación particular de la invención, el servidor proxy (10) almacena en la base de datos proxy (11) una clave de cifrado y un PIN seleccionado por el usuario que corresponden a cada una de las múltiples aplicaciones B2C y B2B instaladas en el teléfono móvil (9). Cada aplicación B2C y B2B tendrá un UIC diferente, ya que cada aplicación no tiene que cooperar con el mismo servidor proxy (10). En esta topología, cada aplicación B2C y B2B incorporará una dirección de servidor proxy diferente. Además, cada servidor proxy (10) puede usar una base de datos proxy (11) diferente, o todos los servidores proxy pueden utilizar una base de datos proxy común. Igualmente, las múltiples aplicaciones B2C y B2B pueden ser atendidas por el mismo servidor de aplicaciones (2), o pueden ser atendidas por diferentes servidores de aplicaciones.

Por lo tanto, la invención proporciona un sistema para llevar a cabo transacciones comerciales móviles que proporciona acceso de usuario seguro desde dispositivos de telecomunicación móviles por medio de un procedimiento de conexión simplificado. El sistema no requiere modificación de los antiguos sistemas intermediarios.

REIVINDICACIONES

1. Un sistema (1) para realizar transacciones comerciales, que comprende:

un servidor de aplicaciones (2) utilizable para alojar una aplicación de software para llevar a cabo transacciones comerciales;
una base de datos de usuarios de aplicaciones (7) de usuarios autorizados capaces de acceder al servidor de aplicaciones (2) para realizar transacciones comerciales en el mismo, siendo cada usuario autorizado de la base de datos de usuarios de aplicaciones (7) identificable de manera única por medio de información de usuario correspondiente;
un servidor proxy (10) en comunicación con el servidor de aplicaciones (2) y accesible por una pluralidad de usuarios registrados desde terminales de acceso móviles (9) respectivos; y
una base de datos proxy (11) de usuarios autorizados de la base de datos de usuarios de aplicaciones (7) que también están registrados para acceder al servidor de aplicaciones (2) a través del servidor proxy (10) desde sus terminales de acceso móviles (9) respectivos, siendo cada usuario registrado en la base de datos proxy (11) identificable de manera única por medio de un código de identificación de usuario correspondiente, proporcionando la base de datos proxy (11), para cada usuario registrado, una correlación del código de identificación de usuario de ese usuario y la información de usuario correspondiente del usuario contenida en la base de datos de usuarios de aplicaciones (7);
caracterizado porque:
el servidor proxy (10) es utilizable para proporcionar a cada uno de la pluralidad de usuarios registrados acceso al servidor de aplicaciones (2) desde el terminal de acceso móvil respectivo (9) de ese usuario retransmitiendo los datos recibidos por el servidor proxy (10) desde los terminales de acceso móviles (9) al servidor de aplicaciones (2) y retransmitiendo los datos recibidos por el servidor proxy (10) desde el servidor de aplicaciones (2) a los terminales de acceso móviles (9); y
la información de usuario es transferible desde el servidor proxy (10) al servidor de aplicaciones (2) sin transferir la información de usuario entre los terminales de acceso móviles (9) y el servidor proxy (10).

2. Un sistema (1) según la reivindicación 1 en el que la base de datos proxy (11) almacena la información de usuario correspondiente de cada usuario registrado en formato cifrado.

3. Un sistema (1) según la reivindicación 2 que incluye un motor de cifrado capaz de cifrar cualquier dato pasado entre el servidor proxy (10) y el terminal de acceso móvil (9) de cada usuario registrado.

4. Un sistema (1) según la reivindicación 3 en el que la base de datos proxy (11) también almacena una clave de cifrado activa para cada usuario registrado, siendo usada la clave de cifrado activa por el motor de cifrado para cifrar y descifrar los datos pasados entre el servidor proxy (10) y el terminal de acceso móvil (9) del usuario.

5. Un sistema (1) según la reivindicación 4 en el que el motor de cifrado es dinámico, usando una clave de cifrado diferente durante cada sesión en la que el usuario accede al servidor de aplicaciones (2) desde su terminal de acceso móvil (9) respectivo.

6. Un sistema (1) según la reivindicación 5 en el que el motor de cifrado genera, durante cada sesión, una clave de cifrado adicional para el usuario y transfiere la clave de cifrado adicional al terminal de acceso móvil (9) del usuario para almacenamiento en el mismo.

7. Un sistema (1) según la reivindicación 6 en el que el motor de cifrado hace automáticamente que la clave de cifrado adicional almacenada se convierta en la clave de cifrado activa en una sesión siguiente en la que el usuario accede al servidor de aplicaciones (2) desde el terminal de acceso móvil (9).

8. Un sistema (1) según la reivindicación 1 en el que el terminal de acceso móvil (9) es un teléfono móvil que tiene un número de teléfono correspondiente.

9. Un sistema (1) según la reivindicación 8 en el que la información de usuario es un nombre de conexión y una contraseña.

10. Un sistema (1) según la reivindicación 9 en el que el servidor proxy (10) sirve de formulario de registro móvil accesible por el usuario para registrarse para acceso al servidor de aplicaciones (2) desde el teléfono móvil respectivo del usuario.

11. Un sistema (1) según la reivindicación 10 en el que el formulario de registro móvil se sirve como una página HTTP accesible por medio de un navegador web totalmente funcional, y/o como una página WAP accesible por medio de un navegador de funcionalidad reducida.

12. Un sistema (1) según la reivindicación 10 en el que el formulario de registro móvil requiere que el usuario presente un nombre de conexión y una contraseña, un número de teléfono del teléfono móvil desde el que el usuario

desea acceder al servidor de aplicaciones (2), y un PIN de conexión seleccionado.

13. Un sistema (1) según la reivindicación 11 en el que el servidor proxy (10) transfiere al servidor de aplicaciones (2) el nombre de conexión y la contraseña presentados para ser validados frente al nombre de conexión y la contraseña del usuario ya almacenados en la base de datos de usuarios de aplicaciones (7).

14. Un sistema (1) según la reivindicación 13 en el que el servidor proxy (10) asigna un código de identificación de usuario al usuario y genera una clave de cifrado cuando el servidor de aplicaciones (2) ha validado exitosamente el nombre y la contraseña del usuario.

15. Un sistema (1) según la reivindicación 14 en el que el servidor proxy (10) combina el código de identificación de usuario y la clave de cifrado como un código de validación de dos partes y transfiere el código de validación al teléfono móvil del usuario.

16. Un sistema (1) según la reivindicación 15 en el que el servidor proxy (10) autentica al usuario como una función de reentrada del código de validación transferido por el usuario en el formulario de registro.

17. Un sistema (1) según la reivindicación 16 en el que el servidor proxy (10) cifra el nombre de conexión y la contraseña del usuario, después de la autenticación del usuario, usando una función del código PIN de conexión seleccionado del usuario como clave de cifrado.

18. Un sistema (1) según la reivindicación 17 en el que el servidor proxy (10) almacena el nombre y la contraseña cifrados del usuario en la base de datos proxy (11) por el código de identificación de usuario.

19. Un sistema (1) según la reivindicación 18 en el que el usuario inicia el acceso al servidor de aplicaciones (2) introduciendo su PIN de conexión en el teléfono móvil.

20. Un sistema (1) según la reivindicación 19 en el que el teléfono móvil cifra el PIN de conexión usando la clave de cifrado activa, encabeza el PIN de conexión cifrado con el código de identificación de usuario y transfiere el PIN de conexión cifrado encabezado al servidor proxy (10).

21. Un sistema (1) según la reivindicación 20 en el que el servidor proxy (10) recupera de la base de datos proxy (11) la clave de cifrado activa como una función del código de identificación de usuario encabezado.

22. Un sistema (1) según la reivindicación 21 en el que el servidor proxy (10) descifra el PIN de conexión cifrado usando la clave de cifrado activa recuperada.

23. Un sistema (1) según la reivindicación 22 en el que el servidor proxy (10) recupera de la base de datos proxy (11) el nombre de conexión y la contraseña cifrados del usuario, descifra el nombre de conexión y la contraseña cifrados usando una función del PIN de conexión descifrado del usuario como clave de cifrado, y transfiere al servidor de aplicaciones (2) el nombre de conexión y la contraseña descifrados del usuario para efectuar una conexión.

24. Un sistema (1) según la reivindicación 23 en el que el teléfono móvil cifra cualquier dato de aplicación con la clave de cifrado activa y encabeza los datos de aplicación cifrados con el código de identificación de usuario antes de transferir los datos de aplicación cifrados al servidor proxy (10).

25. Un sistema (1) según la reivindicación 24 en el que el servidor proxy (10) descifra los datos de aplicación cifrados usando la clave de cifrado activa y transfiere al servidor de aplicaciones (2) los datos de aplicación descifrados para procesamiento.

26. Un sistema (1) según la reivindicación 25 que permite que un usuario registre al menos un instrumento de pago para pagar las compras realizadas en el servidor de aplicaciones (2).

27. Un sistema (1) según la reivindicación 26 en el que el al menos un instrumento de pago es una tarjeta de débito o una tarjeta de crédito.

28. Un sistema (1) según la reivindicación 26 en el que el usuario registra el al menos un instrumento de pago introduciendo en el teléfono móvil datos relacionados con el instrumento de pago, junto con un PIN de compra y el nombre de conexión y la contraseña del usuario.

29. Un sistema (1) según la reivindicación 28 en el que el servidor proxy (10) transfiere al servidor de aplicaciones (2) los datos del instrumento de pago introducidos.

30. Un sistema (1) según la reivindicación 29 en el que el servidor de aplicaciones (2) utiliza los datos del instrumento de pago transferidos para validar el instrumento de pago por medio de una pasarela de pago.

31. Un sistema (1) según la reivindicación 30 en el que el servidor proxy (10) cifra los datos del instrumento de pago validados usando una función del PIN de compra como clave de cifrado.

32. Un sistema (1) según la reivindicación 31 en el que el servidor proxy (10) almacena en la base de datos proxy (11) los datos del instrumento de pago validados cifrados.

33. Un sistema (1) según la reivindicación 32 que permite que un usuario utilice un instrumento de pago registrado previamente para pagar una compra realizada en el servidor de aplicaciones (2).

34. Un sistema (1) según la reivindicación 33 en el que el servidor proxy (10) transmite al teléfono móvil para visualización en el mismo los datos cifrados relacionados con todos los instrumentos de pago registrados previamente por el usuario.

35. Un sistema (1) según la reivindicación 34 en el que el teléfono móvil descifra los datos de pago recibidos y visualiza como un menú en el teléfono móvil los datos descifrados relacionados con todos los instrumentos de pago registrados previamente.

36. Un sistema (1) según la reivindicación 35 en el que el usuario selecciona del menú un instrumento de pago deseado, de los instrumentos de pago registrados previamente, para usarse para el pago, e introduce un valor de la compra junto con el PIN de compra del usuario.

37. Un sistema (1) según la reivindicación 36 en el que el terminal de acceso móvil (9) cifra los datos introducidos usando la clave de cifrado activa y transfiera los datos cifrados al servidor proxy (10).

38. Un sistema (1) según la reivindicación 37 en el que el servidor proxy (10) obtiene de la base de datos proxy (11) la clave de cifrado activa del usuario y descifra los datos transferidos usando la clave de cifrado activa recuperada.

39. Un sistema (1) según la reivindicación 38 en el que el servidor proxy (10) transfiere los datos cifrados al servidor de aplicaciones (2) para efectuar el pago por la transacción de compra.

40. Un procedimiento de funcionamiento de un sistema (1) para realizar transacciones comerciales, que comprende las etapas de:

alojar, en un servidor de aplicaciones (2), una aplicación de software para llevar a cabo transacciones comerciales;
recopilar una base de datos de usuarios de aplicaciones (7) de usuarios autorizados capaces de acceder al servidor de aplicaciones (2) para realizar transacciones comerciales en el mismo e identificar de manera única cada usuario autorizado de la base de datos de usuarios de aplicaciones (7) por medio de información de usuario correspondiente;
proporcionar un servidor proxy (14)en comunicación con el servidor de aplicaciones (2) y accesible por una pluralidad de usuarios registrados desde terminales de acceso móviles (9) respectivos;
establecer una base de datos proxy (11) de usuarios autorizados de la base de datos de usuarios de aplicaciones (7) que también están registrados para acceder al servidor de aplicaciones (2) a través del servidor proxy (10) desde sus terminales de acceso móviles (9) respectivos, e identificar de manera única cada usuario registrado en la base de datos proxy (11) por medio de un código de identificación de usuario correspondiente; y determinar, para cada usuario registrado en la base de datos proxy (11), una correlación del código de identificación de usuario de ese usuario y la información de usuario correspondiente del usuario contenida en la base de datos de usuarios de aplicaciones (7);
caracterizado porque:
el servidor proxy (10) proporciona a cada uno de la pluralidad de usuarios registrados acceso al servidor de aplicaciones (2) desde el terminal de acceso móvil respectivo (9) de ese usuario retransmitiendo los datos recibidos por el servidor proxy (10) desde los terminales de acceso móviles (9) al servidor de aplicaciones (2) y retransmitiendo los datos recibidos por el servidor proxy (10) desde el servidor de aplicaciones (2) a los terminales de acceso móviles (9); y
la información de usuario es transferible desde el servidor proxy (10) al servidor de aplicaciones (2) sin transferir la información de usuario entre los terminales de acceso móviles (9) y el servidor proxy (10).

41. Un procedimiento según la reivindicación 40 que incluye la etapa adicional de almacenar en la base de datos proxy (11) la información de usuario correspondiente de cada usuario registrado en formato cifrado.

42. Un procedimiento según la reivindicación 41 en el que cualquier dato pasado entre el servidor proxy (10) y el terminal de acceso móvil (9) de cada usuario registrado es cifrado.

43. Un procedimiento según la reivindicación 42 en el que una clave de cifrado activa para cada usuario registrado

también es almacenada en la base de datos proxy (11), siendo usada la clave de cifrado activa para cifrar y descifrar los datos pasados entre el servidor proxy (10) y el terminal de acceso móvil (9) del usuario.

44. Un procedimiento según la reivindicación 43 en el que cualquier dato pasado entre el servidor proxy (10) y el terminal de acceso móvil (9) de cada usuario registrado es cifrado dinámicamente usando una clave de cifrado diferente durante cada sesión en la que el usuario accede al servidor de aplicaciones (2) desde su terminal de acceso móvil (9) respectivo.

45. Un procedimiento según la reivindicación 44 que incluye la etapa de generar, durante cada sesión, una clave de cifrado adicional para el usuario y transferir la clave de cifrado adicional al terminal de acceso móvil (9) del usuario para almacenamiento en el mismo.

46. Un procedimiento según la reivindicación 45 en el que se hace automáticamente que la clave de cifrado adicional almacenada se convierta en la clave de cifrado activa en una sesión siguiente en la que el usuario accede al servidor de aplicaciones (2) desde el terminal de acceso móvil (9).

47. Un procedimiento según la reivindicación 46 que incluye la etapa de usar un teléfono móvil como terminal de acceso móvil (9), teniendo el teléfono móvil un número de teléfono correspondiente.

48. Un procedimiento según la reivindicación 47 que incluye la etapa de usar un nombre de conexión y una contraseña como la información de usuario.

49. Un procedimiento según la reivindicación 48 que incluye la etapa de hacer que el servidor proxy (10) sirva de formulario de registro móvil accesible por el usuario para registrarse para acceso al servidor de aplicaciones (2) desde el teléfono móvil respectivo del usuario.

50. Un procedimiento según la reivindicación 49 en el que el formulario de registro se sirve como una página HTTP accesible por medio de un navegador web totalmente funcional, y/o como una página WAP accesible por medio de un navegador de funcionalidad reducida.

51. Un procedimiento según la reivindicación 49 en el que se requiere que el usuario presente, en el formulario de registro móvil, un nombre de conexión y una contraseña, un número de teléfono del teléfono móvil desde el que el usuario desea acceder al servidor de aplicaciones (2), y un PIN de conexión seleccionado.

52. Un procedimiento según la reivindicación 51 en el que el nombre de conexión y la contraseña presentados son transferidos desde el servidor proxy (10) al servidor de aplicaciones(2) para ser validados frente al nombre de conexión y la contraseña del usuario ya almacenados en la base de datos de usuarios de aplicaciones (7).

53. Un procedimiento según la reivindicación 52 en el que se asigna un código de identificación de usuario al usuario y se genera una clave de cifrado cuando el servidor de aplicaciones (2) ha validado exitosamente el nombre y la contraseña del usuario.

54. Un procedimiento según la reivindicación 53 en el que el código de identificación de usuario y la clave de cifrado son combinados como un código de validación de dos partes y el código de validación es transferido al teléfono móvil del usuario.

55. Un procedimiento según la reivindicación 54 en el que el usuario es autenticado como una función de reentrada del código de validación transferido por el usuario en el formulario de registro.

56. Un procedimiento según la reivindicación 55 en el que el nombre de conexión y la contraseña del usuario son cifrados en el servidor proxy (10), después de la autenticación del usuario, usando una función del código PIN de conexión seleccionado del usuario como clave de cifrado.

57. Un procedimiento según la reivindicación 56 en el que el nombre y la contraseña cifrados del usuario son almacenados en la base de datos proxy (11) por el código de identificación de usuario.

58. Un procedimiento según la reivindicaciones 57 que incluye la etapa iniciar el acceso al servidor de aplicaciones (2) introduciendo un PIN de conexión en el teléfono móvil.

59. Un procedimiento según la reivindicación 58 en el que el PIN de conexión es cifrado en el teléfono móvil usando la clave de cifrado activa, el PIN de conexión cifrado es encabezado con el código de identificación de usuario y el PIN de conexión cifrado encabezado es transferido al servidor proxy (10).

60. Un procedimiento según la reivindicación 59 en el que la clave de cifrado activa es recuperada de la base de datos proxy (11) como una función del código de identificación de usuario encabezado.

61. Un procedimiento según la reivindicación 60 en el que el PIN de conexión cifrado es descifrado en el servidor proxy (10) usando la clave de cifrado activa recuperada.

62. Un procedimiento según la reivindicación 61 en el que el nombre de conexión y la contraseña cifrados del usuario son recuperados de la base de datos proxy (11), el nombre de conexión y la contraseña cifrados son descifrados usando una función del PIN de conexión descifrado del usuario como clave de cifrado, y el nombre de conexión y la contraseña descifrados del usuario son transferidos al servidor de aplicaciones (2) para efectuar una conexión.

63. Un procedimiento según la reivindicación 62 en el que cualquier dato de aplicación es cifrado en el teléfono móvil con la clave de cifrado activa y los datos de aplicación cifrados son encabezados con el código de identificación de usuario antes de transferir los datos de aplicación cifrados al servidor proxy (10).

64. Un procedimiento según la reivindicación 63 en el que los datos de aplicación cifrados son descifrados en el servidor proxy (10) usando la clave de cifrado activa y los datos de aplicación descifrados son transferidos al servidor de aplicaciones (2) para procesamiento.

65. Un procedimiento según la reivindicación 64 que incluye la etapa de permitir que un usuario registre al menos un instrumento de pago para pagar las compras realizadas en el servidor de aplicaciones (2).

66. Un procedimiento según la reivindicación 65 en el que el al menos un instrumento de pago es registrado introduciendo en el teléfono móvil datos relacionados con el instrumento de pago, junto con un PIN de compra y el nombre de conexión y la contraseña del usuario.

67. Un procedimiento según la reivindicación 66 en el que los datos del instrumento de pago introducidos son transferidos al servidor de aplicaciones (2).

68. Un procedimiento según la reivindicación 67 en el que los datos del instrumento de pago transferidos son utilizados para validar el instrumento de pago por medio de una pasarela de pago.

69. Un procedimiento según la reivindicación 68 en el que los datos del instrumento de pago validados son cifrados en el servidor proxy (10) usando una función del PIN de compra como clave de cifrado.

70. Un procedimiento según la reivindicación 69 en el que los datos del instrumento de pago validados cifrados son almacenados en la base de datos proxy (11).

71. Un procedimiento según la reivindicación 70 que incluye la etapa de permitir que un usuario utilice un instrumento de pago registrado previamente para pagar una compra realizada en el servidor de aplicaciones (2).

72. Un procedimiento según la reivindicación 71 en el que los datos cifrados relacionados con todos los instrumentos de pago registrados previamente por el usuario son transferidos desde el servidor proxy (10) al teléfono móvil para visualización en el mismo.

73. Un procedimiento según la reivindicación 72 en el que los datos de pago recibidos son descifrados en el teléfono móvil y los datos descifrados relacionados con todos los instrumentos de pago registrados previamente son visualizados en el mismo como un menú.

74. Un procedimiento según la reivindicación 73 en el que se selecciona del menú un instrumento de pago deseado de los instrumentos de pago registrados previamente para usarse para el pago y se introduce un valor de la compra junto con el PIN de compra del usuario.

75. Un procedimiento según la reivindicación 74 en el que los datos introducidos son cifrados en el terminal de acceso móvil (9) usando la clave de cifrado activa y los datos cifrados son transferidos al servidor proxy (10).

76. Un procedimiento según la reivindicación 75 en el que la clave de cifrado activa del usuario es obtenida de la base de datos proxy (11) y los datos transferidos son descifrados usando la clave de cifrado activa recuperada.

77. Un procedimiento según la reivindicación 76 en el que los datos cifrados son transferidos desde el servidor proxy (10) al servidor de aplicaciones (2) para efectuar el pago por la transacción de compra.

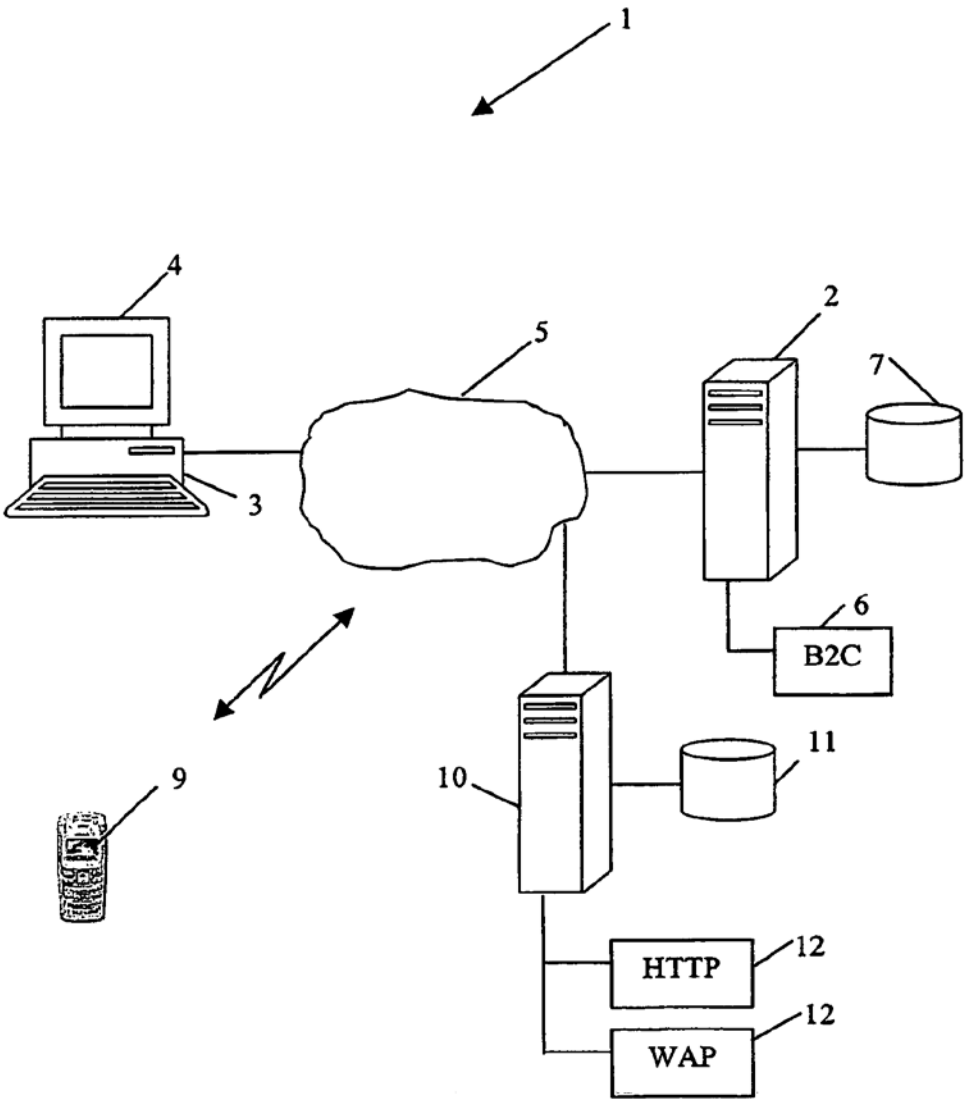

Figura 1

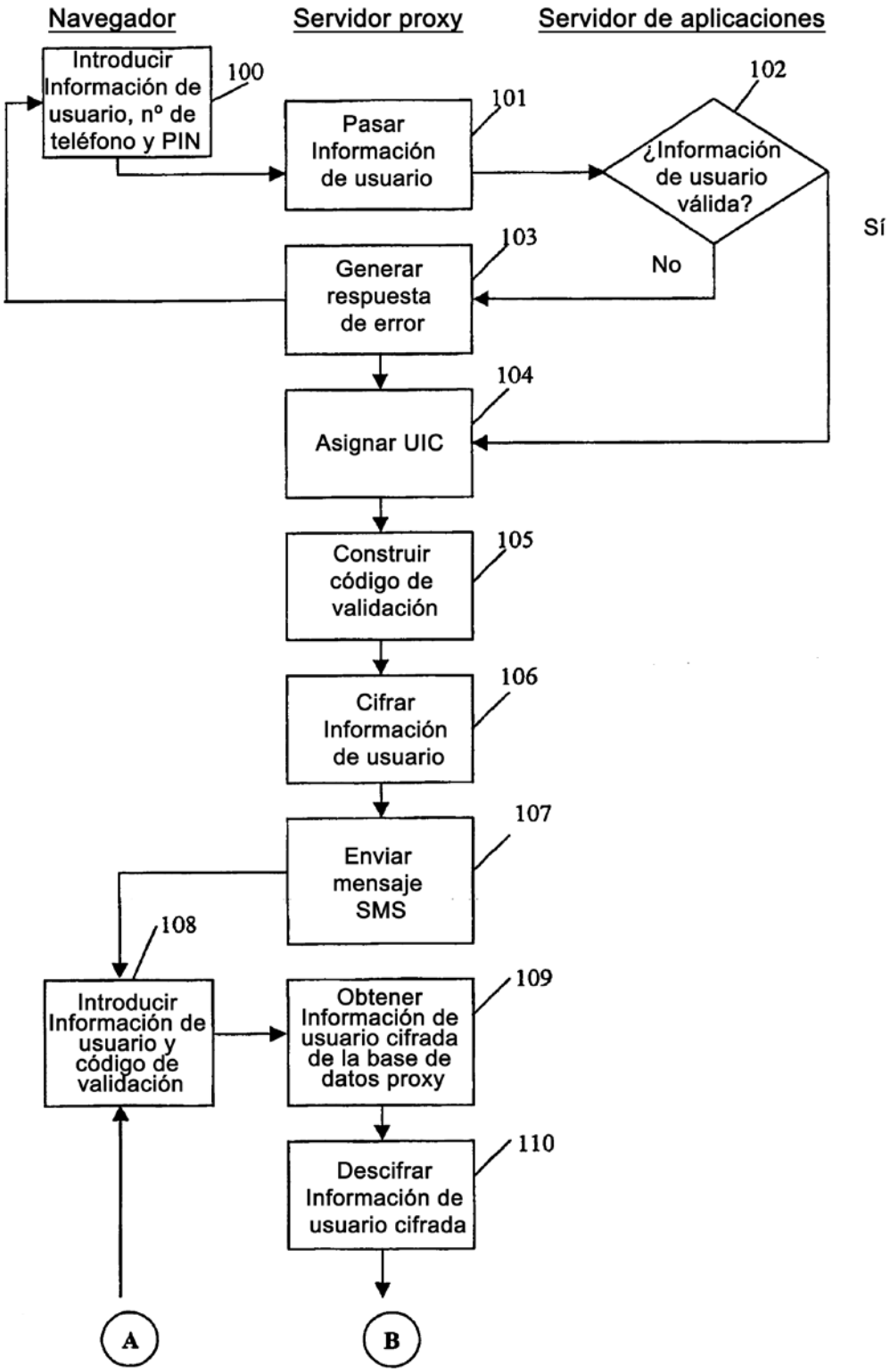
Navegador
Servidor proxy
Servidor de aplicaciones
Introducir Información de usuario, nº de teléfono y PIN
100
Pasar Información de usuario
101
¿Información de usuario válida?
102
Sí
No
Generar respuesta de error
103
Asignar UIC
104
Construir código de validación
105
Cifrar Información de usuario
106
Enviar mensaje SMS
107
Introducir Información de usuario y código de validación
108
Obtener Información de usuario cifrada de la base de datos proxy
109
Descifrar Información de usuario cifrada
110
A
B

Figura 2A

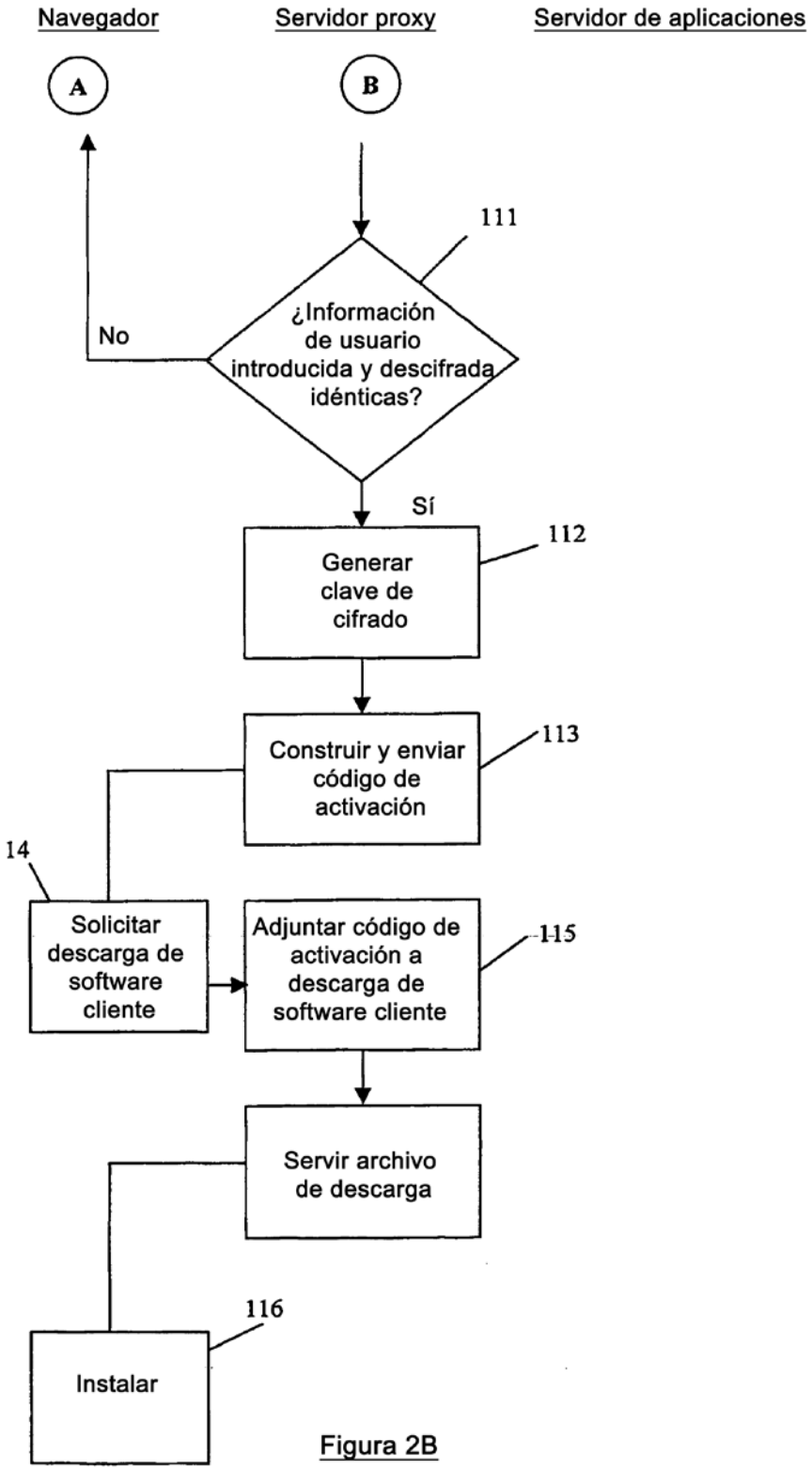
Navegador
Servidor proxy
Servidor de aplicaciones
A
B
111
¿Información de usuario introducida y descifrada idénticas?
No
Sí
112
Generar clave de cifrado
113
Construir y enviar código de activación
14
Solicitar descarga de software cliente
Adjuntar código de activación a descarga de software cliente
115
Servir archivo de descarga
116
Instalar

Figura 2B

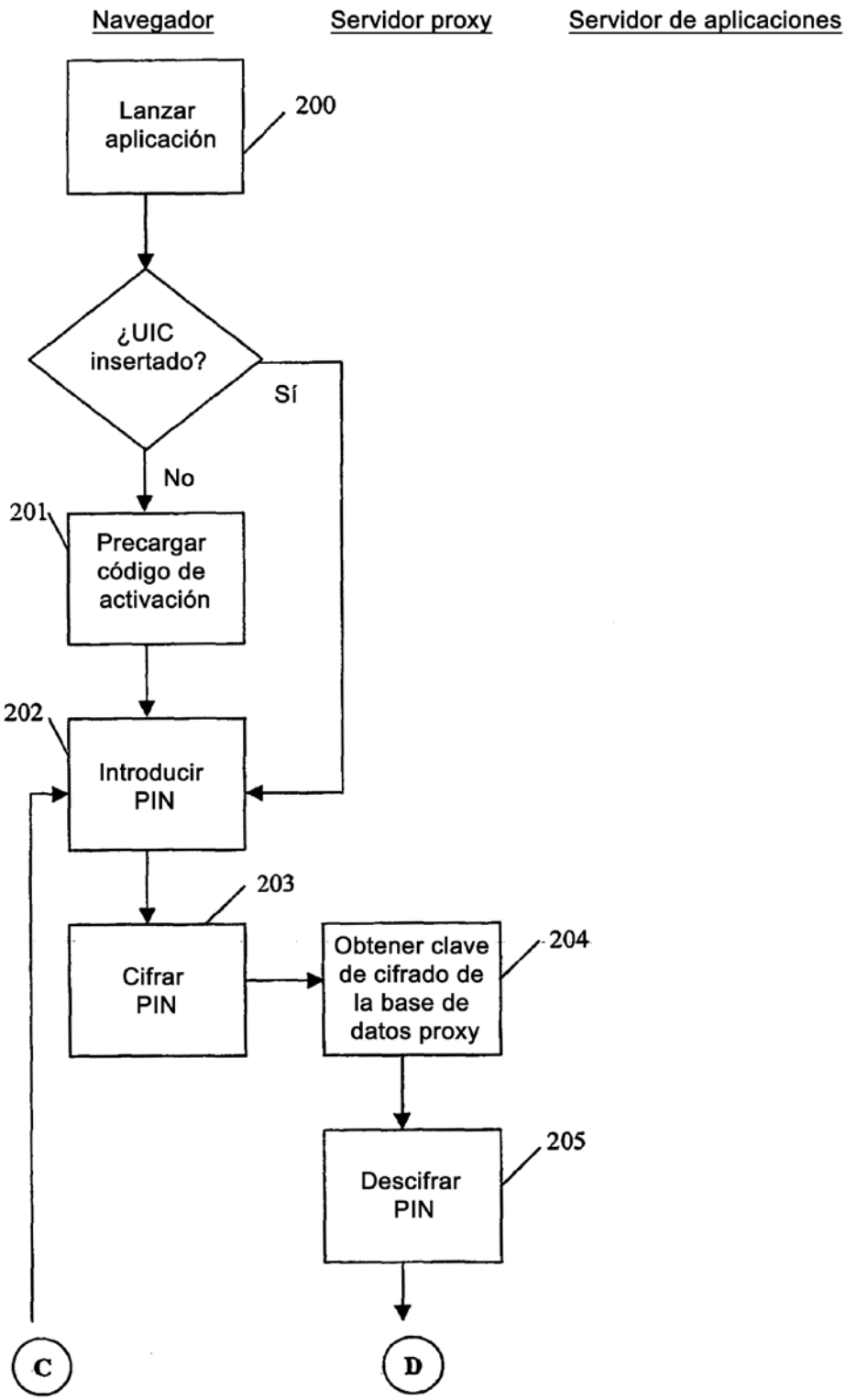
Navegador
Servidor proxy
Servidor de aplicaciones
Lanzar aplicación
200
¿UIC insertado?
Sí
No
201
Precargar código de activación
202
Introducir PIN
203
Cifrar PIN
Obtener clave de cifrado de la base de datos proxy
204
Descifrar PIN
205
C
D

Figura 3A

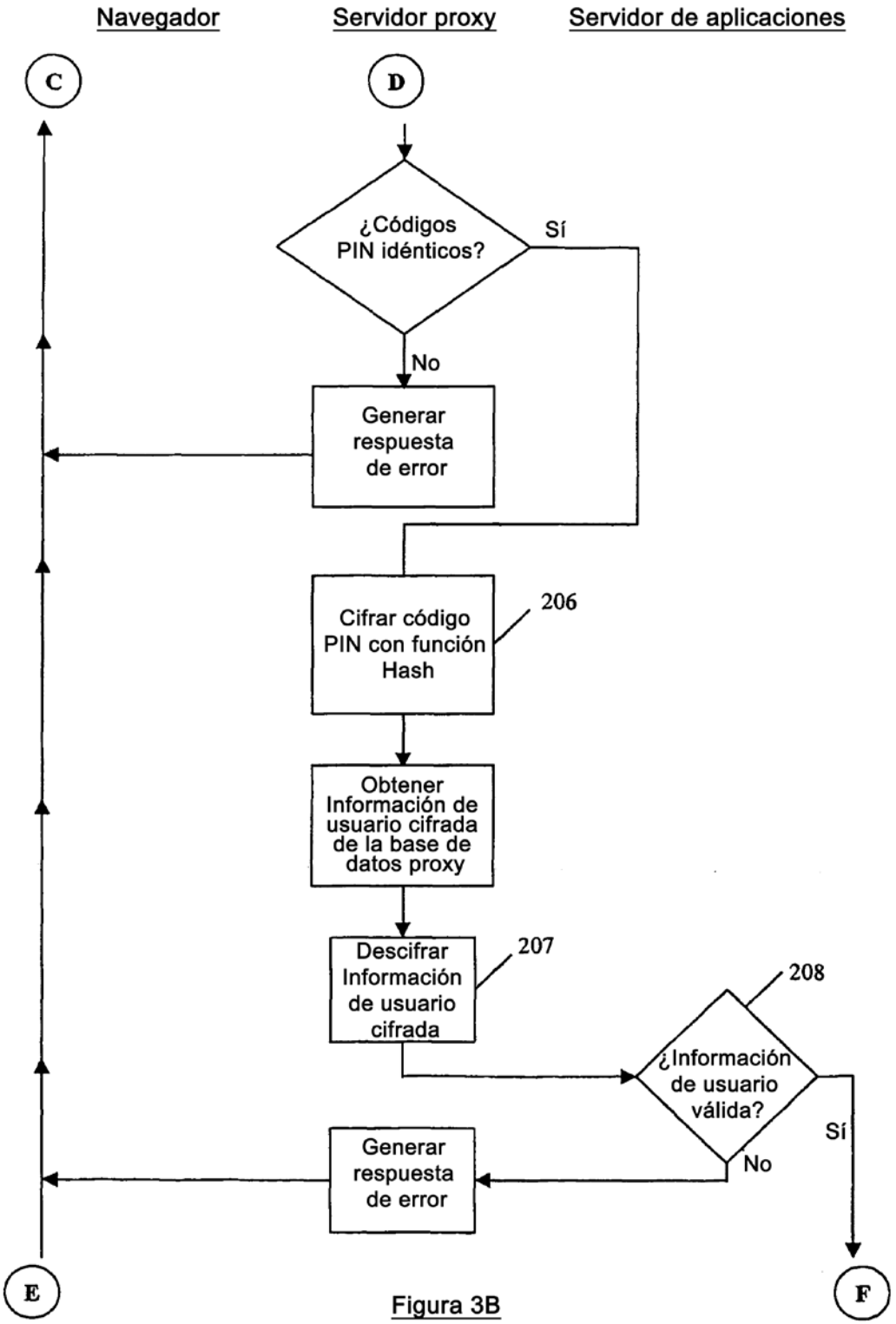
Navegador
Servidor proxy
Servidor de aplicaciones
C
D
¿Códigos PIN idénticos?
Sí
No
Generar respuesta de error
Cifrar código PIN con función Hash
206
Obtener Información de usuario cifrada de la base de datos proxy
Descifrar Información de usuario cifrada
207
208
¿Información de usuario válida?
Sí
No
Generar respuesta de error
E
F

Figura 3B

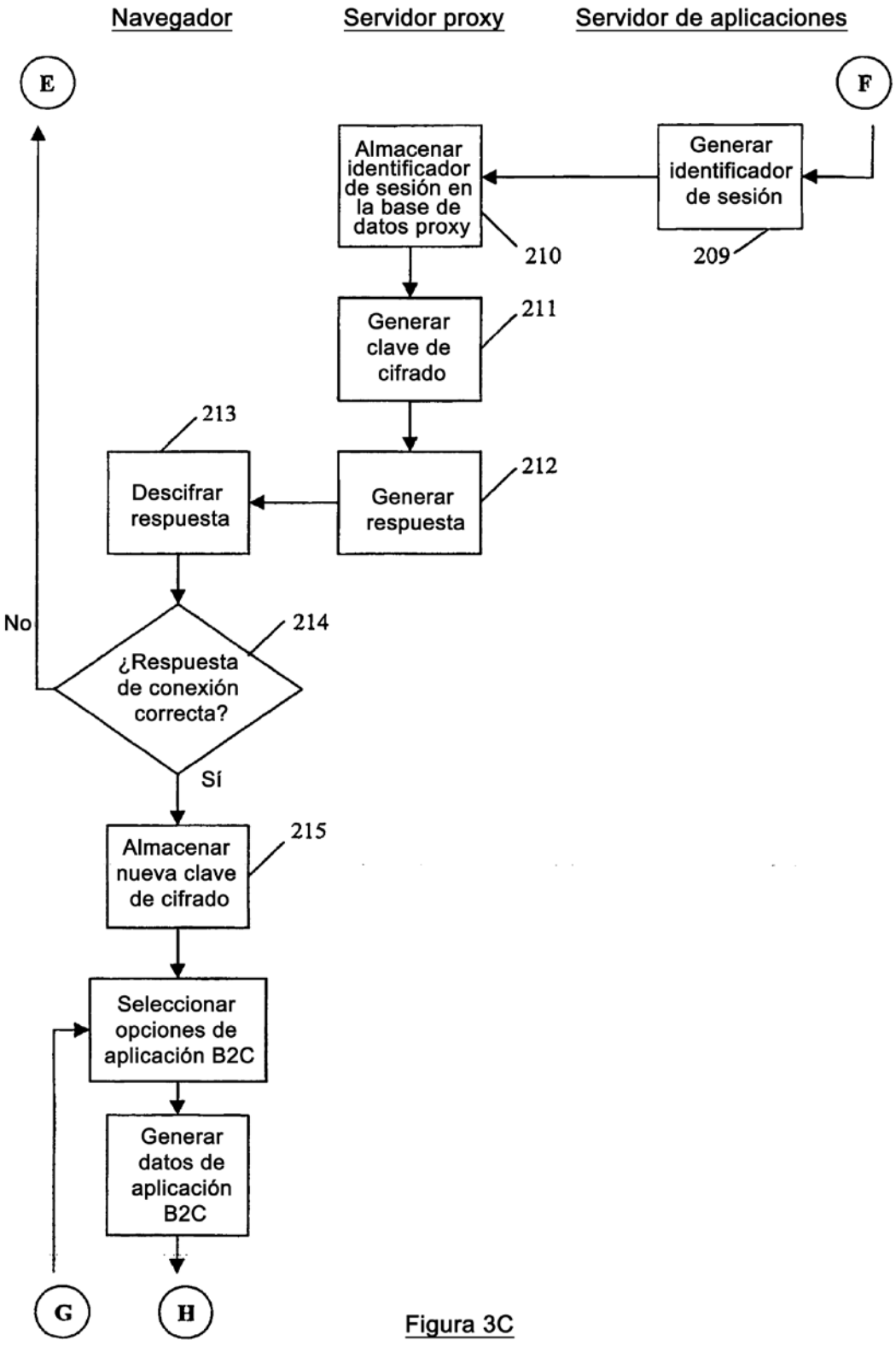
Navegador
Servidor proxy
Servidor de aplicaciones
E
F
Almacenar identificador de sesión en la base de datos proxy
Generar identificador de sesión
210
209
Generar clave de cifrado
211
213
Descifrar respuesta
Generar respuesta
212
No
214
¿Respuesta de conexión correcta?
Sí
Almacenar nueva clave de cifrado
215
Seleccionar opciones de aplicación B2C
Generar datos de aplicación B2C
G
H

Figura 3C

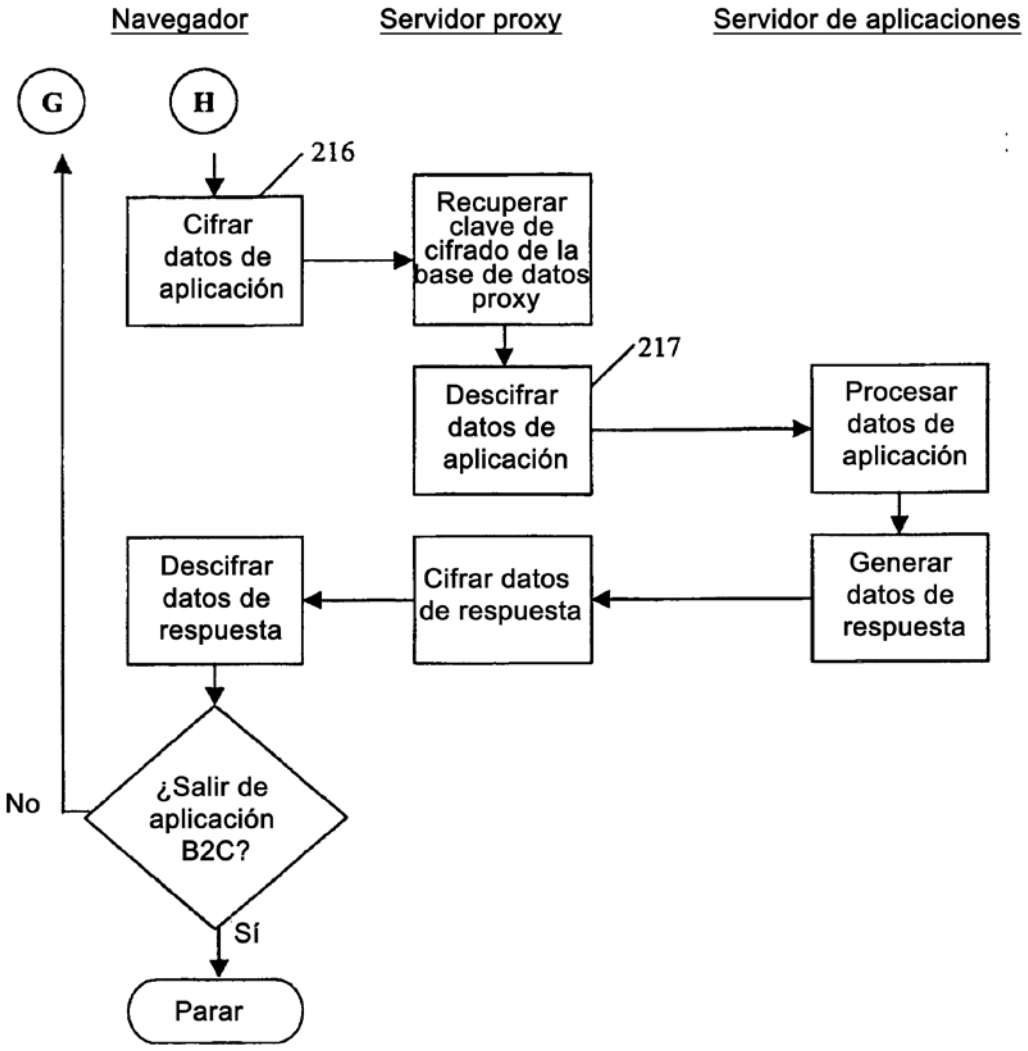
Navegador
Servidor proxy
Servidor de aplicaciones
G
H
216
Cifrar datos de aplicación
Recuperar clave de cifrado de la base de datos proxy
217
Descifrar datos de aplicación
Procesar datos de aplicación
Generar datos de respuesta
Cifrar datos de respuesta
Descifrar datos de respuesta
¿Salir de aplicación B2C?
No
Sí
Parar

Figura 3D

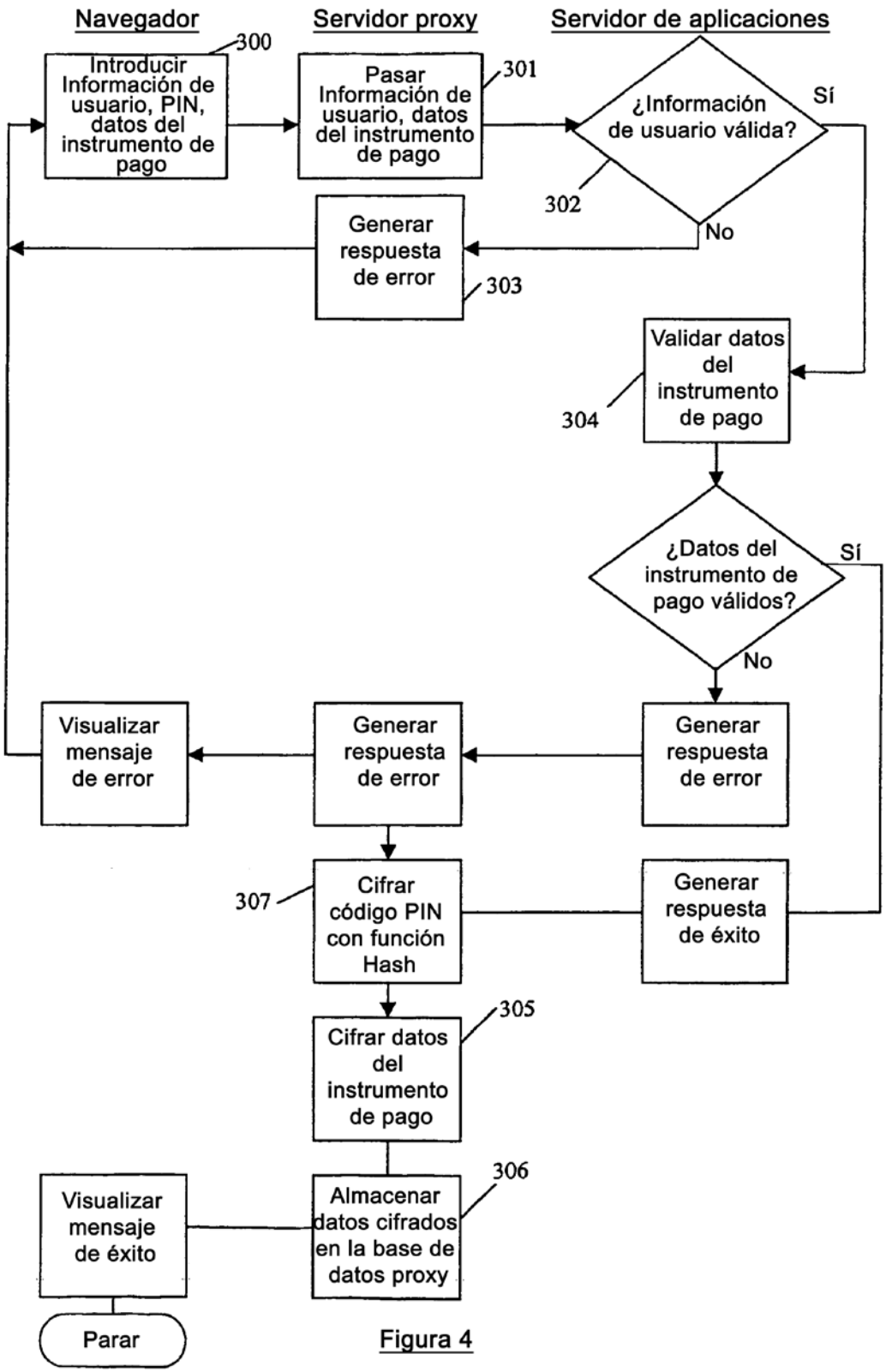
Navegador
Servidor proxy
Servidor de aplicaciones
300
Introducir Información de usuario, PIN, datos del instrumento de pago
301
Pasar Información de usuario, datos del instrumento de pago
¿Información de usuario válida?
Sí
302
No
Generar respuesta de error
303
Validar datos del instrumento de pago
304
¿Datos del instrumento de pago válidos?
Sí
No
Visualizar mensaje de error
Generar respuesta de error
Generar respuesta de error
307
Cifrar código PIN con función Hash
Generar respuesta de éxito
305
Cifrar datos del instrumento de pago
306
Visualizar mensaje de éxito
Almacenar datos cifrados en la base de datos proxy
Parar

Figura 4

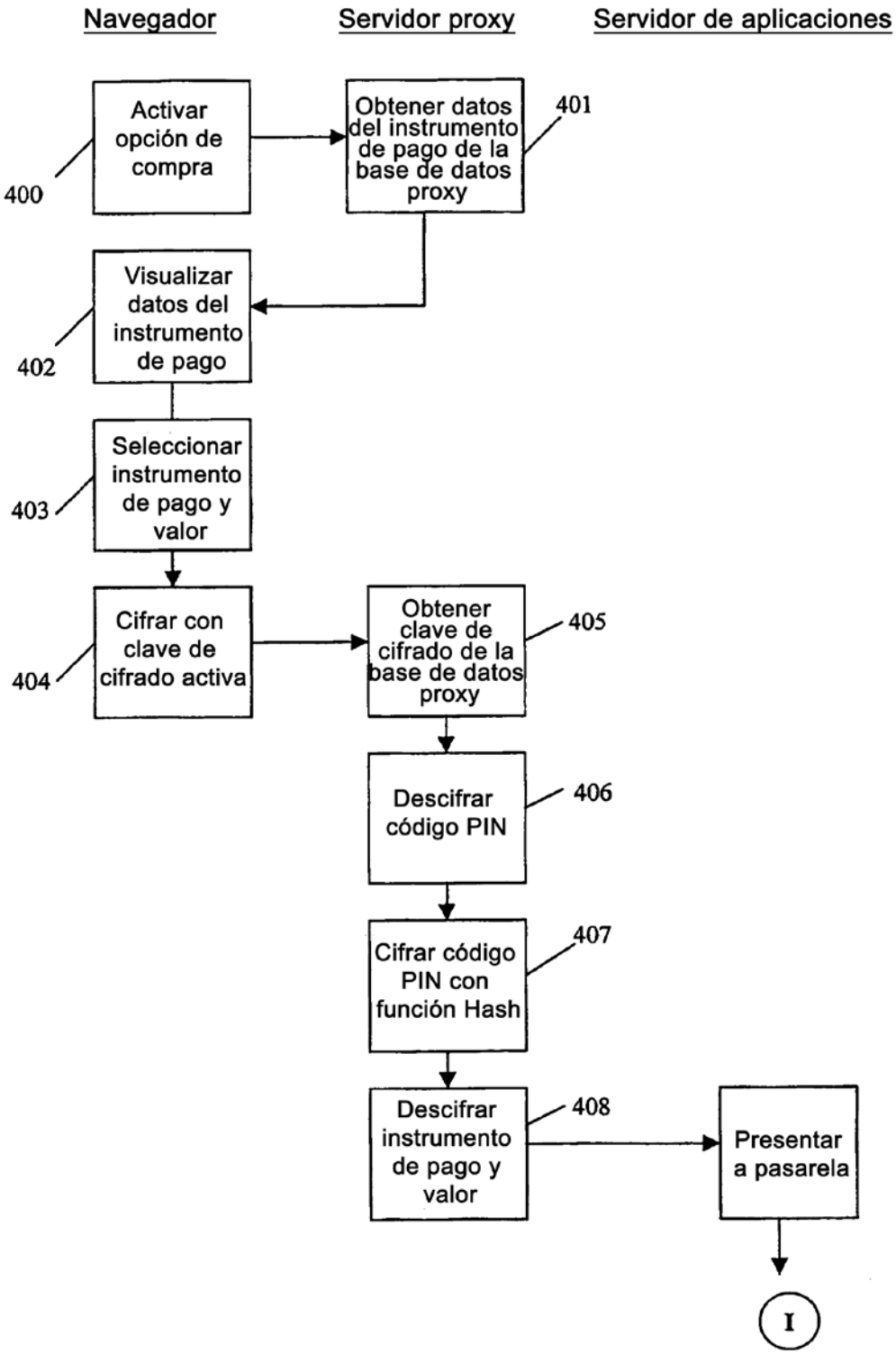
Navegador
Servidor proxy
Servidor de aplicaciones
Activar opción de compra
400
Obtener datos del instrumento de pago de la base de datos proxy
401
Visualizar datos del instrumento de pago
402
Seleccionar instrumento de pago y valor
403
Cifrar con clave de cifrado activa
404
Obtener clave de cifrado de la base de datos proxy
405
Descifrar código PIN
406
Cifrar código PIN con función Hash
407
Descifrar instrumento de pago y valor
408
Presentar a pasarela
I

Figura 5A

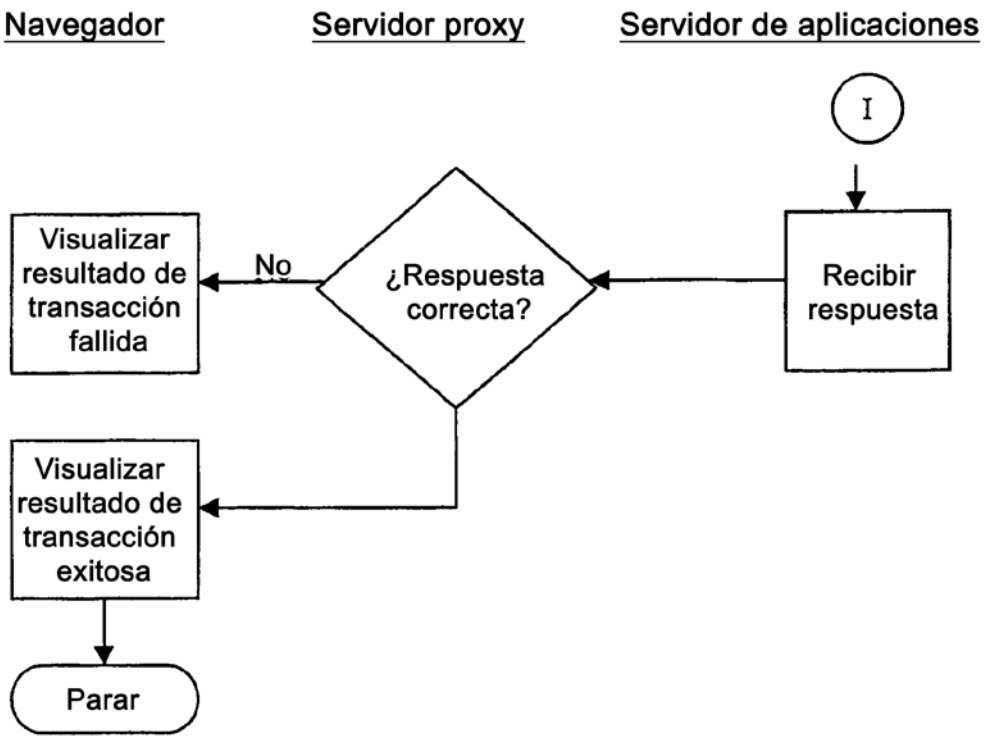
Navegador
Servidor proxy
Servidor de aplicaciones
I
Recibir respuesta
¿Respuesta correcta?
No
Visualizar resultado de transacción fallida
Visualizar resultado de transacción exitosa
Parar

Figura 5B