



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 330 409**

51 Int. Cl.:
G06Q 20/00 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Número de solicitud europea: **01918342 .5**

96 Fecha de presentación : **05.03.2001**

97 Número de publicación de la solicitud: **1323085**

97 Fecha de publicación de la solicitud: **02.07.2003**

54 Título: **Sistema de transacción financiera.**

30 Prioridad: **07.09.2000 US 657478**

45 Fecha de publicación de la mención BOPI:
10.12.2009

45 Fecha de la publicación del folleto de la patente:
10.12.2009

73 Titular/es: **Euronet Worldwide, Inc.**
4601 College Boulevard, Suite 300
Leawood, Kansas 66211, US

72 Inventor/es: **Chamberlin, John;**
Liles, Kevin, G. y
Clary, Jeffrey, S.

74 Agente: **Ungría López, Javier**

ES 2 330 409 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Sistema de transacción financiera.

5 **Campo de la invención**

Esta invención se refiere a un sistema de transacción financiera para el acceso a una red de datos financieros a través de dispositivos terminales alternativos.

10 **Antecedentes de la invención**

Hay una demanda creciente para soluciones versátiles, móviles y amigables a los sistemas tradicionales de transacciones y entrega de información. En ninguna industria es la demanda mayor que en la banca, sistemas financieros y en la industria de transacciones electrónicas. Las comunicaciones de Internet; la alta velocidad, alto volumen de procesamiento de datos; los avances tecnológicos exponencialmente crecientes y añadiendo la iniciativa de los consumidores para adoptar las nuevas tecnologías están aumentando la velocidad con que las industrias de servicios deben ofrecer servicios mejorados. La banca, los servicios financieros y las compañías de transacciones electrónicas cuyos negocios están crecientemente dominados por la agrupación, archivo, protección y transferencia de datos financieros electrónicos son particularmente susceptibles a estas demandas crecientes de los consumidores.

En la actualidad, las máquinas de cajeros automáticos (ATM, del inglés “automated teller machines”) proporcionan a los consumidores acceso a los servicios financieros veinticuatro horas al día, siete días a la semana y ha dado como resultado una creciente comodidad de los consumidores. Sin embargo, hay muchas limitaciones de las redes de ATM/financieras habituales en uso hoy en día lo que da como resultado barreras a una accesibilidad y uso más extendido de tales redes.

Típicamente, un terminal ATM en uso en la actualidad está cableado en una localización fija. Este cableado es necesario para proporcionar alimentación eléctrica al terminal ATM y para proporcionar accesos a las líneas de comunicación, tales como líneas telefónicas, sobre las que pueden intercambiarse los datos financieros y de la transacción con un proveedor de servicios financieros que financia el terminal ATM o a un proveedor de servicios financieros de consumo. Adicionalmente, las preocupaciones sobre la seguridad pueden jugar también un papel en la limitación de los terminales de ATM a localizaciones fijas.

Como consecuencia de la localización fija de tales terminales ATM, un proveedor de servicios financieros debe asegurar la distribución de sus terminales ATM sobre su región geográfica de forma que maximice el acceso del consumidor. Sin embargo, debido a los deseos de los consumidores de tener acceso a los servicios financieros donde quiera que viajen, las ubicaciones iniciales del proveedor de servicios financieros en la localización de sus terminales ATM pueden no satisfacer los deseos de sus clientes. El proveedor de servicios financieros puede, por supuesto, instalar un número creciente de terminales ATM en localizaciones adicionales. Sin embargo, los costes de capital asociados con una cantidad permanentemente creciente de equipos para el número creciente de terminales ATM pueden convertirlo en prohibitivo. Adicionalmente, incluso con la instalación de un número creciente de terminales ATM, un proveedor de servicios financieros puede que aún no sea capaz de satisfacer las demandas de los consumidores para terminales ATM accesibles. Algunas localizaciones, tales como en el interior de trenes, autobuses o automóviles, pueden no ser localizaciones prácticas para los terminales ATM, incluso aunque sean localizaciones razonables para los deseos de los consumidores de acceso a los servicios financieros.

Adicionalmente, puede no ser práctico proporcionar ciertos servicios financieros de valor añadido a través de terminales ATM de localización fija, a pesar del hecho de que tal terminal ATM puede proporcionar ciertas sinergias entre los servicios financieros y una diversidad de datos financieros y recursos de procesamiento de datos disponibles a través de tales terminales ATM. Por ejemplo, un proveedor de servicios para una diversidad de notificaciones de actividades contables planificadas o basadas en eventos, un servicio para la entrega de oportunidades dependientes del tiempo y otros servicios pueden perder su valor si son accesibles sólo a través de puntos de venta de localización fija tales como terminales ATM. Los consumidores desean la comodidad de la entrega de información en tiempo real, además de acceso 24 horas al día, 7 días a la semana a los servicios de sus proveedores de servicios.

Existe en la actualidad una red ATM internacional que permite a los consumidores el acceso a su información financiera en una diversidad de terminales ATM y de puntos de venta (POS del inglés “point-of-sale”) localizados por todo el mundo. Esta red internacional proporciona una base preparada para permitir el acceso del usuario a la información financiera, sin necesitar una red separada de datos financieros o un nuevo protocolo para la comunicación con una diversidad de instituciones financieras. Sin embargo, una diversidad de protocolos de seguridad que se requieren para permitir a un consumidor el acceso a los datos en la red ATM han presentado una diversidad de dificultades técnicas para proporcionar al consumidor un acceso en cualquier lado/cualquier ocasión a la red ATM a través del uso de un dispositivo de comunicaciones personal.

Un primer obstáculo técnico ha sido que muchas instituciones financieras requieren que se codifiquen una variedad de datos en una banda magnética sobre tarjetas ATM, de débito y de crédito. Estos datos codificados varían con la institución financiera, pero se usan generalmente para verificar y validar que una tarjeta particular se emitió de hecho por la institución financiera. Sin embargo, la mayoría de los dispositivos de comunicación personales, particularmente

los dispositivos de comunicación inalámbrica compactos no están equipados con un lector de tarjetas que pueda leer los datos codificados almacenados en una banda magnética. Típicamente hay al menos dos “Pistas” de información codificadas en tales bandas magnéticas. La Pista I normalmente codifica el nombre del propietario de la tarjeta y el número de tarjeta. Los datos de la Pista II varían con la institución financiera particular, pero la Pista II incluye típicamente datos codificados de un número de tarjeta, la deducción de un número de identificación personal (PIN), una fecha de caducidad y una verificación de seguridad en diferentes configuraciones dentro de la Pista II, entre otros datos. Adicionalmente, los datos de la Pista II no están impresos sobre la tarjeta y no son accesibles o verificables de modo general por el consumidor. Debido a que las instituciones financieras requieren algunos o todos estos datos en la configuración particular en la que ellos los codifican para autorizar las transacciones financieras, el acceso a la red ATM no es solamente un asunto de teclear el número de cuenta del consumidor a través de un teclado telefónico o un dispositivo de entrada similar. Se necesita transmitir los datos de la Pista II de la tarjeta ATM del consumidor, en su totalidad, a través de la red ATM para permitir que el consumidor sea autorizado y/o validado por la institución financiera para realizar las transacciones financieras a través de la red ATM. Esto es actualmente imposible usando dispositivos sin lectores de tarjeta magnética.

El segundo obstáculo técnico a superar es que la mayoría de las instituciones financieras también requieren que se envíe por el consumidor (o el usuario) un PIN para validar que el usuario de la tarjeta es realmente el poseedor de la tarjeta. En otras palabras, se usa el PIN para verificar la identidad del usuario de la tarjeta por razones de seguridad. El uso de los PIN es central para la seguridad de los datos de la red ATM y hay unas directrices estrictas impuestas por las redes de transferencia de fondos electrónicas (EFT, del inglés “electronic funds transfer”) sobre cómo puede cifrarse, almacenarse y manipularse un PIN. Los PIN se remiten a la red ATM como bloques PIN cifrados según la DES. Una máquina ATM típica cifra directamente el PIN remitido por el usuario de la tarjeta como un bloque PIN cifrado según la DES. Sin embargo, la mayoría de los dispositivos de comunicación personal y dispositivos de comunicación inalámbrica en particular, no están equipados con capacidades de cifrado DES. Más aún, la transmisión de una señal inalámbrica que contenga un PIN que no esté cifrado compromete la seguridad de la red ATM, dado que las señales inalámbricas pueden interceptarse fácilmente. Muchos fabricantes de dispositivos inalámbricos y proveedores de servicios han superado las preocupaciones de seguridad en la transmisión incluyendo capacidades de cifrado en sus redes inalámbricas. Sin embargo, la norma de cifrado inalámbrica hasta aquí, parece ser un cifrado de protocolo de capa de conexión segura (SSL, del inglés “secure socket layer”) o un cifrado de seguridad de capa de transporte inalámbrica (WTSL, del inglés “wireless socket layer”), no un cifrado DES. Existe un obstáculo adicional debido a que las normas de las redes ATM prohíben la conversión del cifrado de datos usando una norma de cifrado en datos cifrados usando otra norma de cifrado, sin el uso de un dispositivo de cifrado de hardware seguro. De ese modo, ha sido imposible para los usuarios de los dispositivos inalámbricos y de los ordenadores personales en Internet cumplir con las normas de cifrado de los PIN de la red ATM.

En consecuencia, hay una necesidad de un sistema de transacción financiera que sea móvil y disponible para el uso del consumidor independientemente de la localización del consumidor.

Adicionalmente, hay una necesidad de un sistema de transacción financiera que no necesite estar directamente conectado mediante líneas cableadas a una fuente de alimentación o a una red telefónica.

Hay una necesidad adicional de proporcionar un sistema de transacción financiera con las características anteriormente mencionadas que no comprometa la seguridad de una red ATM de los proveedores de los servicios financieros.

Hay también una necesidad de proporcionar un sistema de transacción financiera con las características descritas anteriormente que no requiera un gran desembolso de capital por el proveedor de servicios financieros, el proveedor de servicios inalámbricos o las compañías de portales de Internet.

Estos y otros inconvenientes de los sistemas de técnicas anteriores se superan mediante varias realizaciones de la intención.

El documento WO 00/31699 describe un sistema para llevar a cabo transacciones de tarjetas de créditos a través de un teléfono móvil, en donde el número de tarjeta del usuario se almacena en una tarjeta SIM del teléfono móvil y se transmite a una institución financiera en un mensaje de transacción desde el teléfono móvil.

Sumario de la invención

Por lo tanto es un objetivo de la invención superar los inconvenientes de los sistemas previos mencionados anteriormente.

Es un objetivo adicional de la invención proporcionar un sistema de transacción financiera que sea móvil y disponible para el uso de un consumidor independientemente de la localización del consumidor.

Es un objetivo adicional de la invención proporcionar un sistema de transacción financiera que no requiera una conexión cableada a una fuente de alimentación o a una red telefónica.

Es aún un objetivo adicional de la invención proporcionar un sistema de transacción financiera que no requiera un dispositivo terminal con un lector de tarjetas.

ES 2 330 409 T3

Es todavía un objetivo adicional de la invención proporcionar un sistema de transacción financiera que no comprometa la seguridad de la red ATM de un proveedor de servicios financieros y que no requiera un gran desembolso de capital por parte del proveedor de servicios.

5 Los objetivos y ventajas adicionales de la invención se expondrán en parte en la descripción que sigue y en parte serán obvios a partir de la descripción o pueden aprenderse mediante la puesta en práctica de la invención.

De acuerdo con un aspecto de la presente invención, se proporciona un sistema de transacción financiera para proporcionar servicios bancarios y financieros que comprenden:

10

(a) una red de datos financieros que utiliza un protocolo de seguridad de datos predeterminado para recibir y transmitir los datos financieros del usuario;

15

(b) un sistema de gestión de la transacción en comunicación con dicha red de datos financieros para ejecutar transacciones seguras de servicios financieros a través de dicha red de datos financieros de acuerdo con el protocolo de seguridad de datos predeterminado en respuesta a las solicitudes de servicio de los usuarios; y

20

(c) un dispositivo de comunicaciones para transmitir y recibir las solicitudes de servicio de los usuarios, siendo procesadas las solicitudes de servicio de los usuarios por dicho sistema de gestión de la transacción usando los datos financieros recuperados desde dicha red de datos financieros;

25

en el que dicho sistema de transacción recibe la solicitud de servicio del usuario en una primera norma de cifrado y remite al menos una parte de los datos desde la solicitud de servicio del usuario a dicha red de datos financieros en una segunda norma de cifrado; y

en el que el protocolo de seguridad de datos de dicha red de datos financieros incluye datos de validación embebidos en una ficha de seguridad específica del usuario que es una tarjeta;

30

caracterizado por que:

dicho sistema de gestión de la transacción incluye una fuente de datos de dichos datos de validación enlazados al menos a una identificación del usuario, por lo que dicho sistema de transacción puede remitir los datos de validación a dicha red de datos financieros en respuesta a la solicitud de servicio del usuario que no contiene los datos de validación.

35

De acuerdo con otro aspecto de la presente invención, se proporciona una fuente de datos para el uso en la remisión de transacciones financieras a una red de datos financieros que comprende:

40

(a) un identificador del usuario para un usuario; y

(b) datos de validación de la cuenta para al menos una cuenta de usuario asociada con dicho identificador del usuario, correspondiendo dichos datos de validación de la cuenta a datos de una ficha de seguridad que es una tarjeta que requiere que se tenga acceso a un lector de tarjetas;

45

caracterizado por que:

la fuente de datos se dispone para permitir el acceso desde un sistema de transacción para formular una solicitud de servicios financieros para el usuario a través de la red de datos financieros en respuesta a una solicitud de servicio del usuario que no contiene los datos de validación de la cuenta.

50

Lo anterior y otros objetos de las realizaciones preferidas se alcanzan particularmente mediante un sistema y un método de transacción financiera para proporcionar servicios bancarios y financieros usando una red de datos financieros que tenga un protocolo de seguridad de datos predeterminado para recibir y transmitir los datos financieros del usuario. El sistema incluye un sistema de gestión de la transacción en comunicación con la red de datos financieros para ejecutar transacciones de servicios financieros seguras a través de la red de datos financieros de acuerdo con el protocolo de seguridad de datos predeterminado. El sistema de gestión de la transacción maneja las solicitudes de servicio del usuario originadas desde dispositivos terminales alternativos, tales como dispositivos de comunicación inalámbricos y dispositivos de Internet. El sistema de gestión de la transacción puede incluir un sistema criptográfico para convertir SSL, WTSLS u otros formatos de cifrado en cifrado DES y puede incluir una fuente de datos que incluye los datos de la Pista II a partir de las tarjetas bancarias y/o de crédito del usuario de forma que el sistema puede accederse desde un dispositivo que carezca de lector de tarjetas magnéticas o dispositivos similares. El sistema y el método permiten transacciones similares a las ATM a través de dispositivos inalámbricos y de Internet no equipados con lectores de tarjetas magnéticas ni con cifrado DES.

65

Los dibujos adjuntos, que se incorporan en y constituyen una parte de esta especificación, ilustran una realización de la invención y, junto con la descripción, sirven para explicar los principios de la invención.

Breve descripción de los dibujos

La Figura 1 es una vista esquemática de un sistema inalámbrico de transacción financiera para proporcionar servicios bancarios y financieros por medio de un dispositivo de comunicaciones inalámbricas de acuerdo con una realización de la invención.

La Figura 2 es una vista esquemática de un sistema inalámbrico de transacción financiera para proporcionar servicios bancarios y financieros por medio de un dispositivo de comunicaciones inalámbricas de acuerdo con una realización de la invención.

La Figura 3 es una vista esquemática de la arquitectura de software del sistema inalámbrico de transacción financiera para proporcionar servicios bancarios y financieros por medio de un dispositivo de comunicaciones inalámbricas de acuerdo con una realización de la invención.

La Figura 4 es un diagrama de flujo que ilustra las etapas en el proceso de registro para el uso del sistema inalámbrico de transacción financiera de acuerdo con una realización de la invención.

La Figura 5 es un diagrama de flujo que ilustra las etapas en el proceso del uso de servicios inalámbricos de transacción bancaria y financiera de acuerdo con una realización de la invención.

La Figura 6 es un diagrama de flujo que ilustra las etapas en el proceso de proporcionar servicios inalámbricos de transacción bancaria y financiera de acuerdo con una realización de la invención.

La Figura 7 es una vista esquemática de una diversidad de terminales de servicio y métodos de interfase para el uso con un sistema inalámbrico de transacción financiera de acuerdo con una realización de la invención.

Descripción detallada de las realizaciones preferidas

Se hará referencia ahora en detalle a las realizaciones preferidas actuales de la invención, de las que se ilustran ejemplos en los dibujos adjuntos, en los que caracteres de referencia similares se refieren a elementos que se corresponden.

Con referencia a las figuras en general y particularmente a la Figura 1, se muestra un sistema inalámbrico de transacción financiera 100 para proporcionar servicios bancarios y financieros por medio de dispositivos inalámbricos. El sistema 100 permite a un usuario acceder a los servicios bancarios y financieros incluyendo, sin limitarse a, aquellos servicios ofrecidos a través de las ATM tradicionales de localización fija, a través de un dispositivo de comunicación inalámbrica 110, tal como el teléfono móvil del usuario, un asistente personal digital (PDA) con un módem inalámbrico, un buscapersonas alfanumérico u otros dispositivos de comunicaciones inalámbricas. El sistema 100 incluye un Sistema de Transacción 130, que conecta una diversidad de servicios de comunicaciones proporcionados por un Proveedor de Servicios Inalámbricos 120 y una diversidad de información financiera proporcionada por al menos un Proveedor de Servicios Financieros 140 usando protocolos de datos de red ATM. El Sistema de Transacción 130 puede proporcionar el procesado de los datos, almacenamiento de los datos, conversión de los datos y seguridad de los datos para un usuario que accede a los servicios financieros y bancarios. Para usar el sistema 100, el usuario puede iniciar una transacción de solicitud de servicios a través del dispositivo de comunicaciones inalámbricas del usuario 110, tal como mediante la marcación de un número de teléfono particular o un código de acceso. El usuario puede entonces navegar por uno o más menús u opciones simples para iniciar y transmitir una solicitud de servicio particular, tal como una solicitud de los saldos actuales de una o más de las cuentas financieras del usuario. La solicitud de servicio se recibe mediante el Proveedor de Servicios Inalámbricos 120 y se pasa al Sistema de Transacción 130. El Sistema de Transacción 130 extrae una diversidad de informaciones relevantes de seguridad y de la transacción a partir de la solicitud de servicio transmitida e inicia la ejecución de al menos una aplicación para cumplir con la solicitud de servicio transmitida. La aplicación puede incluir la consulta a uno o más proveedores de servicios financieros para el acceso a los datos financieros usando los protocolos de transmisión de datos de la red ATM. Una parte de la aplicación para el acceso a los datos financieros puede incluir la recepción de los PIN cifrados con una norma de cifrado distinta de la DES (por ejemplo, SSL) y el uso de cifrado por hardware para convertirla a bloques PIN cifrados según la DES de acuerdo con las normas de la red ATM. Una vez se ejecuta la aplicación, se devuelve una respuesta adecuada, tal como los saldos actuales solicitados u otra notificación, al usuario a través del Proveedor de Servicios Inalámbricos 120 y el dispositivo de comunicaciones inalámbricas 110. El Sistema de Transacción 130 puede permitir también la comunicación con otros sistemas, redes, o terminales de servicio, tales como una diversidad de dispositivos terminales 150. Los dispositivos terminales 150 pueden utilizarse por el usuario para registrarse en, mantener, o acceder de otra forma a los servicios financieros y bancarios proporcionados a través del Sistema de Transacción 130. Los dispositivos terminales 150 se equipan cada uno con un lector de tarjeta magnética para permitir que el usuario registre inicialmente una tarjeta que tenga datos de Pista II codificados en una banda magnética de la misma, con el Sistema de Transacción 130 para permitir transacciones sin tarjeta similares a las ATM.

El dispositivo de comunicaciones inalámbricas 110 puede incluir cualquier dispositivo habilitado para comunicaciones inalámbricas, tales como teléfonos móviles, pequeños ordenadores con módems inalámbricos (por ejemplo, PDA, Palm Top, etc.), buscas, radios bidireccionales, comunicadores y otros dispositivos de comunicación personal. En una realización preferida, el dispositivo inalámbrico 110 puede incluir un teléfono móvil que utilice una tecnología

ES 2 330 409 T3

5 GSM, una CDMA o una UMTS. En una realización, el dispositivo inalámbrico 110 incluye una pantalla 111 (por ejemplo, una pantalla LCD, una pantalla de plasma, etc.) y uno o más dispositivos de entrada 112 (por ejemplo, un teclado numérico, uno más botones de navegación, etc.). El dispositivo de comunicaciones inalámbricas 110 puede ser compatible con un formato de comunicaciones para permitir la visualización de los datos transmitidos al dispositivo de comunicaciones inalámbricas 110 sobre una pantalla 110 u otros dispositivos de salida. Tales formatos de comunicación pueden incluir un formato tal como un formato de servicio de mensajes cortos (SMS, del inglés “Short Message Service”), formato de protocolo de aplicaciones inalámbricas (WAP, del inglés “Wireless Application Protocol”) u otro protocolo de comunicación de datos.

10 El Proveedor del Servicio Inalámbrico 120 puede usar uno o más sistemas de cualquier proveedor de servicios de comunicaciones inalámbricas, tal como compañías que proporcionan servicios de comunicaciones móviles (por ejemplo, AT&T, Bell Atlantic Mobile, EuroTel, etc.). El Proveedor del Servicio Inalámbrico 120 puede o no estar asociado con un responsable del mantenimiento del Sistema de Transacción 130 y todo o parte de los sistemas de comunicación inalámbricas del Proveedor del Servicio Inalámbrico 120 pueden o no estar integrados con el Sistema de Transacción 130. En una realización preferida, una diversidad de sistemas de proveedores de servicios inalámbricos, tal como el sistema del Proveedor del Servicio Inalámbrico 120, comunican con y permiten los servicios de transacción financiera y bancaria del Sistema de Transacción 130 para proporcionar aquellos servicios a través de los dispositivos de comunicación inalámbricas 110 de los clientes del Proveedor del Servicio Inalámbrico 120.

20 El Sistema de Transacción 130 incluye un sistema de ordenadores para recibir una solicitud de servicio, procesar la solicitud de servicio y devolver un resultado a partir del procesamiento de la solicitud de servicio. El procesamiento de la solicitud de servicio puede involucrar contactar y/o intercambiar datos con uno o más proveedores de servicios financieros, tal como el Proveedor de Servicios Financieros 140; interactuar con una o más bases de datos de información del usuario (por ejemplo, una base de datos que contenga datos de la Pista II de una diversidad de usuarios); y llevar a cabo una o más operaciones lógicas utilizando los datos remitidos por el usuario, de los proveedores de servicios financieros o de la base de datos.

30 La solicitud de servicio manejada por el Sistema de Transacción 130 puede incluir una variedad de servicios financieros y bancarios. En una realización preferida, estos servicios financieros y bancarios incluyen al menos un servicio de Consulta de Saldo 131, un servicio de Movimientos 132, un servicio de Transferencias 130, un servicio de Cambio de Claves 134, un servicio de Pérdida de Tarjetas 135, un servicio de Aviso 136, un servicio de Petición de Justificantes 137, un servicio de Petición de Cheques 138 y un servicio de Registro 139. El servicio de Aviso 136 incluye un servicio de Lista de Avisos 136a, un servicio de Añadir Aviso 136b y un servicio de Borrar Aviso 136c. Los servicios adicionales pueden incluir el pago de facturas, presentación del monto de las facturas, cargo y recargo de cuentas de prepago, y servicios y solicitud de información diversa.

40 Cada uno de los servicios financieros y bancarios puede incluir uno o más objetos de aplicación para ejecutar el servicio financiero/bancario. Uno o más de los servicios financieros y bancarios pueden incluir una consulta u otro intercambio de datos con uno o más proveedores de servicios financieros usando los protocolos de datos de la red ATM. Para facilitar cada una de tales transacciones de servicio financiero y bancario, un objeto de aplicación puede interrogar una base de datos que contenga información del usuario incluyendo los datos de la Pista II para remitir los datos de la Pista II de un usuario al Proveedor de Servicios Financieros 140. Un objeto de la aplicación puede recibir entonces un PIN no cifrado según la DES (por ejemplo un PIN cifrado según SSL), enviar el PIN cifrado a un sistema de criptografía por hardware para la conversión a un bloque PIN cifrado según la DES. Algunas transacciones de servicio financiero y bancario pueden no utilizar la red de datos ATM y sus objetos de aplicación pueden usar predominantemente datos recuperados desde la base de datos de información del usuario u otras fuentes de datos.

50 El servicio de Consulta de Saldo 131 permite a un usuario acceder al saldo actual de una o más cuentas financieras del usuario. En una realización, el usuario remite un mensaje cifrado según SSL conteniendo un número de tarjeta y un PIN a través de un dispositivo de comunicaciones inalámbrico 110 al Sistema de Transacción 130; el Sistema de Transacción 130 convierte el PIN remitido a un formato de cifrado DES y recupera la información de la Pista II del usuario a partir de la base de datos de información del usuario; dirige la consulta y la información de seguridad de la Pista II del usuario al Proveedor de Servicios Financieros 140 apropiado para el usuario; recibe los datos de vuelta desde el Proveedor de Servicios Financieros 140 correspondientes al saldo actual en la cuenta financiera del usuario; y da formato y devuelve la información del saldo o saldos actuales para una o más de las cuentas del usuario al dispositivo de comunicaciones inalámbricas 110 del usuario.

60 El servicio de Movimientos 132 permite al usuario acceder a una diversidad de detalles de una o más transacciones pasadas para una o más cuentas financieras del usuario. El servicio de Movimientos 132 incluye un número fijo o variable de transacciones o todas las transacciones durante un período de tiempo fijo o variable que afecta al saldo de las cuentas del usuario para mostrarlas al usuario. El servicio de Movimientos 132 puede permitir al usuario buscar una transacción particular mediante uno o más campos (por ejemplo, fecha, beneficiario, cantidad, etc.). El servicio de Movimientos 132 puede usar la información de los datos de PIN convertidos y los datos del registro de la Pista II del usuario para remitir una consulta para una transacción de información desde el Proveedor de Servicios Financieros 140 usando los protocolos de la red ATM.

El servicio de Transferencias 133 permite a un usuario transferir fondos desde al menos una de las cuentas del usuario con un Proveedor de Servicios Financieros 140 a otra de las cuentas del usuario con el Proveedor de Servicios

ES 2 330 409 T3

Financieros 140 o con otro de los Proveedores de Servicios Financieros 140. El servicio de Transferencias 133 puede usar la información de los datos del PIN convertidos y los datos del registro de la Pista II del usuario para remitir una petición para una transacción de información desde el Proveedor de Servicios Financieros 140 usando los protocolos de la red ATM.

5

El servicio de Cambio de Claves 134 permite a un usuario cambiar la clave del usuario, si el usuario ha elegido usar una característica de seguridad adicional o una clave bancaria inalámbrica. Alternativamente, el usuario puede registrar su PIN en la base de datos de información del usuario y usar una clave para iniciar las transacciones a través del Sistema de Transacción 130. Esto evita que el PIN real del usuario haya de ser transmitido a través del sistema 100. Debido a que la clave del usuario es una clave específica para el Sistema de Transacción 130, no es necesario acceder a cualquier Proveedor de Servicios Financieros 140 o utilizar la información de los datos del PIN convertidos o de la Pista II del sistema 100.

15

El servicio de Pérdida de Tarjetas 135 permite al usuario informar de una pérdida o robo de una tarjeta ATM, una pérdida o robo de una tarjeta de débito, o una pérdida o robo de una tarjeta de crédito al Proveedor de Servicios Financieros 140 que emitió la tarjeta perdida o robada de forma que puedan tomarse las acciones apropiadas para bloquear el uso de la tarjeta perdida o robada. El servicio de Pérdida de Tarjetas 135 puede usar la información de los datos del PIN convertidos y los datos del registro de la Pista II del usuario para permitir al Proveedor de Servicios Financieros 140 verificar la identidad del usuario tras recibir del usuario el informe de tarjeta perdida o robada.

20

El servicio de Avisos 136 permite a un usuario ver, suscribirse a y borrar la suscripción a uno o más avisos de información financiera planificados o condicionales y servicios de gestión de mensajes a través del dispositivo de comunicaciones inalámbricas 110. Algunos ejemplos de los tipos de avisos que pueden proporcionarse al usuario incluyen: un aviso planificado de modo regular del saldo de la cuenta (por ejemplo, proporcionar una información de aviso actualizada planificada regularmente informando al usuario del saldo de la cuenta de cheques actual del usuario); un aviso para supervisar los cambios condicionales en el saldo de la cuenta (por ejemplo, un aviso advirtiendo al usuario cuando una transacción lleva al saldo de la cuenta por debajo de un saldo mínimo requerido); un aviso para informar de una transacción al usuario cuando tiene lugar una transacción, tal como una notificación de un débito en un POS o ATM por encima de 100 \$ o una notificación de la finalización de una transacción ACH o cualquier otra información de entrega planificada o condicional. El servicio de Avisos 136 puede incluir un aviso que contenga un contenido informativo no relacionado directamente con la información de la cuenta financiera personal del usuario, tal como un aviso de una subida o una caída en las tasas de interés de mercado actuales, un aviso de un precio para una acción particular, un aviso incluyendo puntuaciones deportivas, un aviso incluyendo información meteorológica, un aviso incluyendo anuncios e información mercantil y otra información de conveniencia general. El servicio de Avisos 136 puede usarse para establecer uno o más recordatorios personales del usuario, tal como un aviso para las próximas vacaciones, un aviso de cumpleaños, un aviso incluyendo al menos una fecha de vencimiento de un pago de una factura de productos o servicios y un aviso de otro evento. El servicio de la Lista de Avisos 136a permite al usuario acceder a una lista completa de todos los avisos a los que se ha suscrito. El servicio de Añadir Aviso 136b permite al usuario añadir una suscripción para un nuevo aviso. El servicio de Borrar Aviso 136c permite a un usuario borrar una suscripción de aviso existente. Debido a que el servicio de Avisos 136 puede mantenerse dentro del Sistema de Transacción 130, no es necesario acceder a ningún Proveedor de Servicios Financieros 140 o utilizar las características de la información de los datos del PIN convertidos o de la Pista II del sistema 100 para modificar los avisos para los que se ha suscrito el usuario en el servicio de Avisos 136.

45

El servicio de Petición de Justificantes 137 permite a un usuario solicitar una copia o justificante de la banca electrónica o la tarjeta de crédito del Proveedor de Servicios Financieros 140 apropiado para el registro del usuario o para sustituir a un justificante perdido. El servicio de Petición de Justificantes 137 puede usar la información de los datos del PIN convertidos y los datos del registro de la Pista II para permitir al Proveedor de Servicios Financieros 140 verificar la identidad del usuario tras recibir una solicitud de petición de justificantes.

50

El servicio de Petición de Cheques 138 permite a un usuario pedir fácilmente una diversidad de cheques de sustitución para una diversidad de cheques emitidos originalmente por el Proveedor de Servicios Financieros 140 del usuario. El servicio de Petición de Cheques 138 puede usar la información de los datos del PIN convertidos y los datos del registro de la Pista II para permitir al Proveedor de Servicios Financieros 140 verificar la identidad del usuario tras recibir una solicitud de petición de cheques. Alternativamente, el Sistema de Transacción 130 puede usar un tercer proveedor para satisfacer una petición de cheques y puede acceder a la información disponible desde la base de datos de información del usuario, tal como un nombre, una dirección, un número de teléfono, un número de cuenta, información del banco y un número de ruta para el usuario.

60

El servicio de Registro 139 permite al usuario establecer inicialmente un archivo de información de usuario en la base de datos de información del usuario y, específicamente, almacenar los datos de la Pista II a partir de la tarjeta ATM del usuario. No se accede al servicio de Registro 139 a través del dispositivo de comunicaciones inalámbricas 110. Por el contrario, se accede al servicio de Registro 139 a través de un terminal alternativo en comunicación con el Sistema de Transacción 130, tal como un dispositivo terminal 150. El usuario inicia el servicio de Registro 139 mediante el paso de la tarjeta ATM del usuario a través de un lector de tarjetas magnéticas en comunicación con el dispositivo terminal 150 y el Sistema de Transacción 130 registra al menos los datos de la Pista II transmitidos por medio del lector de tarjeta en el dispositivo terminal 150 dentro de un archivo de registro en la base de datos de información del usuario. El servicio de Registro 139 puede preguntar también al usuario por otra información o puede

65

ES 2 330 409 T3

ser capaz de acceder a información adicional, tal como una diversidad de información de contacto del usuario, a través de los registros del usuario del Proveedor de Servicios Inalámbricos 120 o del Proveedor de Servicios Financieros 140. Puede accederse al servicio de Registro 139 a través de las ATM (por ejemplo, de la ATM 151), del sistema POS 152 en un distribuidor al por menor del Proveedor de Servicios Inalámbricos 120 sobre Internet desde un terminal o un
5 ordenador personal equipado con un lector de tarjetas magnéticas (por ejemplo, el ordenador personal 153, o un lector de tarjetas magnéticas (no mostrado)) o en un banco (por ejemplo, el Banco 154 usando un sistema de establecimiento del PIN) con un lector de tarjetas magnéticas u otros dispositivos de la red del banco que esté equipado con un lector de tarjetas magnéticas.

10 El Proveedor de Servicios Financieros 140 puede incluir cualquier número de instituciones financieras y de redes de datos financieros. El Proveedor de Servicios Financieros 140 puede comprender una diversidad de uno cualquiera o más de los bancos físicos tradicionales, bancos (“virtuales”) en Internet, una diversidad de compañías de ahorro y préstamos, una diversidad de entidades de créditos, una diversidad de casas de corredores, una diversidad de compañías de tarjetas de créditos, una diversidad de compañías al por menor de crédito extendido, una diversidad de compañías
15 hipotecarias, una diversidad de compañías de servicios de préstamos, una diversidad de compañías de facturación y una diversidad de otros negocios e instituciones que mantienen cuentas financieras seguras y otros datos. El Sistema de Transacción 130 permite a los servicios financieros y bancarios utilizar datos intercambiados con el Proveedor de Servicios Financieros 140 apoyándose sobre los protocolos de la red ATM. El Sistema de Transacción 130 puede utilizar también otras formas de intercambio de datos con el Proveedor de Servicios Financieros 140 para permitir
20 alguno o todos los servicios financieros y bancarios disponibles.

Los Dispositivos Terminales 150 pueden incluir una diversidad de dispositivos, redes y/o sistemas habilitados para acceder a uno o más servicios proporcionados por el Sistema de Transacción 130. El Sistema de Transacción 130 puede permitir una amplia variedad de tipos de acceso y formatos de comunicación, además del acceso inalámbrico
25 a los servicios bancarios y financieros descritos en este documento. Por ejemplo, el Sistema de Transacción 130 puede permitir el acceso a los servicios sobre Internet, el acceso a los servicios vía sistemas telefónicos, el acceso a los servicios a través de los sistemas de POS y las ATM y el acceso a los servicios a través de otros medios de comunicación y configuraciones de dispositivos. Los dispositivos terminales 150 equipados cada uno con al menos un lector de tarjetas magnéticas permiten el registro de los datos de la Pista II del usuario a través del servicio de
30 Registro 139.

En la Figura 2, se muestra un sistema de transacción 200 para proveer de servicios bancarios y financieros. El sistema de transacción 200 incluye una Pasarela de Comunicaciones 210, un Servidor de Aplicaciones 220 y un Servidor de Interfase 230. El sistema de transacción 200 actúa como un intermediario entre: una diversidad de sistemas
35 de redes financieras mantenidas por los proveedores de servicios financieros, tales como los Proveedores de Servicios Financieros 140 descritos anteriormente con relación a la Figura 1; una diversidad de puntos de acceso a redes financieras tales como los terminales POS 152 y las ATM 151; uno o más sistemas de comunicaciones inalámbricas, tal como el sistema del Proveedor de Servicios Inalámbricos 120 descrita anteriormente en relación con la Figura 1; y una diversidad de otros puntos de acceso a los sistemas de transacción, tal como los dispositivos terminales 150 descritos anteriormente con relación a la Figura 1. El Servidor de Interfase 230 permite al usuario acceder a una diversidad de servicios financieros y bancarios a través de una variedad de terminales de servicio, tales como un asistente digital personal (PDA), un teléfono móvil o celular, una ATM, un terminal POS y otros dispositivos. El Servidor de Interfase
40 230 puede incluir una diversidad de servidores de interfase para soportar una diversidad de diferentes protocolos de comunicación y normas de interfase para permitir uno o más tipos de terminales de servicio o de dispositivos terminales para comunicar con la diversidad de proveedores de servicios financieros. El Servidor de Aplicaciones 220, en comunicación con Servidor de Interfase 230, incluye una variedad de aplicaciones modulares para proporcionar una diversidad de servicios financieros y bancarios, tales como los servicios descritos anteriormente con relación a la Figura 1. El Servidor de Aplicaciones 220 puede conectarse a un Sistema Criptográfico 240 para proporcionar conversión de los datos cifrados en una o más de otras normas de cifrado al cifrado DES. El Servidor de Aplicaciones
45 220 puede dirigir una diversidad de comunicaciones con relación a los servicios financieros y bancarios del usuario, tales como una consulta del saldo de la cuenta, una transferencia de fondos electrónicos y otras las acciones con una diversidad de sistemas de redes financieras exteriores, a través de la Pasarela de Comunicaciones 210. La Pasarela de Comunicaciones 210 actúa para dirigir o enrutar adecuadamente la diversidad de comunicaciones a uno o más sistemas y puntos de acceso dentro de una red financiera, tal como la red ATM internacional. Un repositorio de datos
50 250 contiene una diversidad de información de cuentas personalizadas para una diversidad de usuarios, permitiendo por ello que se proporcionen servicios financieros y bancarios adicionales a tal diversidad de usuarios. Por ejemplo, el repositorio de datos 250 puede incluir una base de datos de usuario con una diversidad de datos de la Pista II y bloques PIN cifrados de cada uno de la diversidad de usuarios de tarjetas ATM, de débito y de crédito.

60 Para enrutar la diversidad de comunicaciones, como se ha referenciado anteriormente, la Pasarela de Comunicaciones 210 incluye una diversidad de hardware y software de conmutación y supervisión para dirigir la diversidad de comunicaciones con relación a los servicios financieros y bancarios del usuario (tal como datos financieros electrónicos) a un destino predeterminado (el Proveedor de Servicios Financieros 140) de acuerdo con los protocolos de comunicaciones apropiados para el Proveedor de Servicios Financieros 140. Incluye adicionalmente un nodo central para dirigir el tráfico en los datos financieros electrónicos entre una diversidad de redes de comunicaciones y sistemas de datos financieros de otra manera incompatibles. La Pasarela de Comunicaciones 210 puede incluir también
65 una diversidad de canales de comunicación y conexiones de redes para comunicar los datos financieros electrónicos usando normas de cifrado de datos ATM, normas de cifrado de datos de transferencias de fondos electrónicas (EFT),

ES 2 330 409 T3

normas de cifrado de datos basadas en Internet, normas de cifrado de datos propietarias y otras normas de cifrado de datos para transferencia segura de datos. Por ejemplo, la Pasarela de Comunicaciones 210 puede recibir transacciones desde una ATM, una institución financiera, otra pasarela EFT, un terminal POS o un Servidor de Aplicaciones 220 (por ejemplo una transacción desde una red bancaria o un usuario de teléfono inalámbrico habilitado por el banco).

5 Tras la recepción de la transacción, la Pasarela de Comunicaciones 207 determina el remitente usando un Número de Identificación Bancaria (BIN, del inglés “Bank Identification Number”) incluido en los datos recibidos, tales como los datos de la Pista II de la tarjeta de débito del usuario. Si el BIN pertenece a un banco local, la transacción se enrutará al banco local para autorización. Si el BIN no pertenece a un banco local, entonces la decisión de enrutado se tomará dependiendo del número BIN de la tarjeta. Esta decisión de enrutado se determinará mediante la comparación del BIN
10 con las tablas de enrutado mantenidas en el software de la Pasarela de Comunicaciones 210. Cuando se encuentra el BIN o algunos dígitos apropiados del bin, la transacción se enruta a otra pasarela adecuada o institución financiera para autorización. Si no se halla el BIN en las tablas de enrutado entonces se usará una pasarela por omisión para autorizar las transacciones. En una realización, puede recibirse un mensaje del servidor de aplicaciones en un formato propietario y convertirse a un formato apropiado para el envío al terminal tras la toma de la decisión de enrutado.
15 Se recibirá una autorización desde el emisor de autorizaciones y la transición será aprobada o rechazada basándose en la respuesta del emisor. La Pasarela de Comunicaciones 210 puede realizar también balances y apuntes con la autorización del emisor, así como con el proveedor de servicios de adquisiciones.

Para realizar las funciones anteriormente descritas, la Pasarela de Comunicaciones 210 incluye preferiblemente una plataforma AS/400 con un sistema operativo OS/400. La Pasarela de Comunicaciones 210 puede incluir adicionalmente un software ITM 2.2 para el acceso contable y anotaciones asociadas.

El Servidor de Aplicaciones 220 incluye uno o más servidores para el alojamiento de una diversidad de aplicaciones de servicios financieros y bancarios. Tales aplicaciones de servicios financieros y bancarios pueden incluir cualquier servicio en relación a banca personalizada, finanzas, gestión monetaria, transacciones de pago o inversiones. El Servidor de Aplicaciones 220 incluye adicionalmente una plataforma para la ejecución de una diversidad de aplicaciones financieras y bancarias. El Servidor de Aplicaciones 220 utiliza un diseño de aplicación modular soportando objetos de interfase estándar para proporcionar un sistema flexible, fácilmente extensible y ampliamente independiente del hardware para proporcionar las aplicaciones de servicios financieros. Por ejemplo, el Servidor de Aplicaciones
30 220 puede ser un servidor de aplicaciones de empresa ejecutando una diversidad de aplicaciones compuestas de una diversidad de módulos de aplicación intercambiables (por ejemplo, Enterprise JavaBeans). Puede usarse un tal módulo de aplicación intercambiable para permitir al Servidor de Aplicaciones 220 ofrecer servicios financieros y bancarios a través de él y responder a las solicitudes de servicio desde el servidor de interfase 230. Otro puede permitir al Servidor de Aplicaciones 220 iniciar transacciones (por ejemplo transferencias y consultas) con sistemas de redes financieras externas o con repositorios de datos 250.

En una realización, el Servidor de Aplicaciones 220 puede componerse por un servidor Microsoft NT 4.0 que tiene un sistema de CPU de 500 MHz o más rápida con al menos 1 - 2 gigabytes de memoria, ejecutando software WebLogic y SQL de Microsoft, y que tiene una diversidad de discos SCSI con un controlador RAID. En una realización alternativa, el servidor de aplicaciones 220 puede incluir un servidor Microsoft NT 4.0 que tiene al menos un sistema de CPU de 500 MHz con al menos 0,5 a 1 gigabyte de memoria, ejecutando software SQL 7.0 de Microsoft, y que tiene una diversidad de discos SCSI con un controlador RAID. La realización alternativa puede enlazarse a un segundo servidor con memoria adicional ejecutando el software WebLogic. Adicionalmente, es preferible incluir una diversidad de tarjetas ethernet y una red capaz de procesar 100 megabits por segundo para comunicación con otras
45 zonas del sistema.

El Servidor de Aplicaciones 220 se conecta, y se comunica con, un Sistema Criptográfico 240 para permitir el cifrado de datos en bloques PIN cifrados según la DES compatibles con las normas de cifrado de datos de la red ATM. Por ejemplo, el Sistema Criptográfico 240 puede estar formado por un componente de hardware para el descifrado de un PIN recibido desde el Servidor de Aplicaciones 220 en un formato de cifrado distinto del DES (por ejemplo, SSL, WTSL, etc.). Se pasa un mensaje cifrado, junto con un marcador para indicar la localización del PIN dentro del mensaje, al componente de hardware. Dentro del componente de hardware, el mensaje se descifra desde el cifrado SSL o WTSL y se extrae el PIN y se convierte al cifrado DES. El bloque de PIN cifrado según la DES se pasa de vuelta saliendo del componente de hardware para añadirse al mensaje de cifrado para la entrega a la pasarela. El componente de hardware es a prueba de sabotaje de modo que cualquier intento de abrir la carcasa del componente inhabilita al componente. De esta manera, el PIN nunca está presente en una forma visible o electrónica sin cifrar lo que le podría dejar sujeto a apropiación indebida a través de una supervisión física o electrónica.

El Servidor de Interfase 230, conectado al Servidor de Aplicaciones 220, proporciona una diversidad de interfaces de usuario para el acceso a una o más aplicaciones de servicios financieros y bancarios alojados en el Servidor de Aplicaciones 220. El Servidor de Interfase 230 puede incluir una diversidad de alojamientos de servidores una diversidad de interfaces para uno o más protocolos de comunicación y terminales dirigidos. Por ejemplo, el Servidor de Interfase 230 puede incluir un servidor de servicios de mensajes cortos (SMS), un servidor de protocolo de aplicaciones inalámbricas (WAP), un servidor Web, un servidor ATM, un servidor de un sistema POS, un servidor de teléfonos automatizado, etc. El servidor de SMS proporciona uno o más mensajes de texto cortos para intercambiar información interactivamente con el usuario y puede accederse por el usuario usando cualquier dispositivo habilitado para SMS, tal como un teléfono móvil, un buscapersonas alfanumérico u otro dispositivo inalámbrico con capacidades de pantalla limitadas. El servidor WAP puede proporcionar una o más páginas de interfase, tales como páginas escritas

ES 2 330 409 T3

en el lenguaje de marcado inalámbrico (WML, del inglés “Wireless Markup Language”, una aplicación del lenguaje de marcado extensible (XML)), para intercambiar información interactivamente con el usuario y es accesible para el usuario usando cualquier dispositivo que soporte WAP, tal como un teléfono móvil, un buscapersonas, una radio bidireccional, un teléfono inteligente, un comunicador y otro dispositivo inalámbrico portátil. Al menos una parte del contenido disponible a través del Servidor de Interfase 230 puede proporcionarse mediante una o más aplicaciones desde el Servidor de Aplicaciones 220.

Un repositorio de datos 250 puede incluir cualquier número de repositorios de datos individuales que contengan datos financieros o información relacionada. El repositorio de datos 250 puede ser una fuente de datos localizada, tal como una base de datos o un grupo de bases de datos, o puede ser una fuente distribuida, tal como un lote de archivos localizables distribuidos a través de la red. El repositorio de datos 250 incluye un repositorio de información de cuentas financieras y bancarias específicas del usuario e información de acceso de cuentas asociadas, tal como una tarjeta bancaria o información de la banda magnética de la tarjeta de crédito, incluyendo los datos de la Pista II, para uno o más usuarios. El repositorio de datos 250 puede incluir un archivo de registro para cada usuario incluyendo: una diversidad de información de auditoría de transacciones, tal como una identificación del dispositivo terminal (por ejemplo, un identificador único asociado con un dispositivo inalámbrico del usuario), un indicador de la fecha y la hora de la transacción, un número de trazado de auditoría del sistema y otra información; una diversidad de información inalámbrica, tal como una identificación del proveedor de servicios inalámbricos, un número de teléfono inalámbrico o una dirección u otra información; una diversidad de información de la tarjeta, tal como un número de tarjeta, una fecha de caducidad, una diversidad de datos de la Pista II, un bloque PIN cifrado según la DES, una diversidad de datos de la Pista I (por ejemplo, el nombre del usuario), un identificador del emisor (un nombre de banco, un número de enrutado, etc.); una diversidad de información de control de registro, tal como un indicador del estado y un indicador de datos de mantenimiento; una diversidad de información histórica, tal como una diversidad de estadísticas sobre los usos anteriores del usuario de una cuenta y una diversidad de información personal del usuario, tal como un nombre y otra información de contacto. La información relacionada con un número de cuentas proporcionada por una variedad de instituciones financieras pero perteneciente al mismo usuario puede enlazarse juntas o localizadas para un acceso más eficiente.

En la Figura 3 se muestra una arquitectura de software de un sistema modular 300 para el procesamiento de una diversidad de solicitudes de servicios de usuario de acuerdo con una realización de la invención. El sistema modular 300 puede usarse por un servidor de aplicaciones, tales como el Servidor de Aplicaciones 220 en la Figura 2, para procesar la diversidad de solicitudes de servicio del usuario colocadas a través del dispositivo de comunicaciones inalámbricas 110. El sistema modular 300 incluye un número de objetos de aplicaciones 310, tales como los Objetos de Aplicación 311 y 312. Los Objetos de Aplicación 311 y 312 se usan cada uno como una ruta de entrada estándar para la diversidad de solicitudes de servicios de usuario, tales como desde los Usuarios 301 y 302. Los Objetos de Aplicación 311 y 312 crean una transacción 320, tal como las Transacciones 321 y 322, que describen una diversidad de acciones a realizarse. El enrutador 330 evalúa las Transacciones 321 y 322 y dirige las Transacciones 321 y 322 a un proveedor adecuado 340, tal como uno de los Proveedores 341, 342 y 343. Los Proveedores 341, 342 y 343 proporcionan las operaciones para completar las Transacciones 321 y 322. En algunos casos, un proveedor, tal como el Proveedor 343, puede entregar una Solicitud de Servicio 350 para acceder a un recurso externo, tales como datos financieros mantenidos por una institución financiera, una base de datos de información del usuario o un sistema criptográfico. Los Proveedores 341, 342 y 343 pueden o bien dirigir la transacción a otro proveedor de servicios o pueden devolver una respuesta 360, tal como las Respuestas 361 y 362, a los Objetos de Aplicación 311 y 312.

Los Objetos de Aplicación 310 proporcionan cada uno una ruta de entrada estándar para una diversidad de Solicitudes de Servicio 350 del usuario e inician una diversidad de transacciones 320 dentro del sistema modular 300. Los Objetos de Aplicación 310 representan una diversidad de acciones individuales que se puede pedir que realice el sistema modular 300. Algunos ejemplos de Objetos de Aplicación 210 pueden incluir un objeto de consulta del saldo de la cuenta, un objeto de movimientos o una diversidad de objetos que corresponden a cualquiera de los otros servicios financieros y bancarios descritos con referencia a la Figura 1. En otra realización, cada objeto de aplicación 310 es un Enterprise JavaBean (EJB) que no mantiene estado y es accesible al usuario por medio de una Java Naming and Directory Interface (JNDI) (no mostrada). Cada Objeto de Aplicación 310 crea una transacción 320 que describe una acción a realizarse y contiene una diversidad de información del usuario necesaria para iniciar la acción. Por ejemplo, un objeto de consulta de saldo se usaría para crear una transacción de consulta de saldo y debería contener información del usuario básica tal como una identificación del usuario (por ejemplo un número de tarjeta ATM, etc.) y un PIN. Donde un usuario tenga múltiples cuentas, el objeto de consulta de saldo puede incluir también un identificador de cuenta. Cada objeto de aplicación 310 puede llamar también al Enrutador 330 para determinar un proveedor de destino 340 para procesar la transacción 320. En una realización, el Objeto de Aplicación 310 pasa la transacción 320 al Enrutador 330 en donde el Enrutador 330 evalúa la transacción 320 y la pasa a un proveedor seleccionado 340. Alternativamente, el Enrutador 330 puede evaluar la transacción 320, pero el Objeto de Aplicación 330 pasa realmente la transacción 320 al proveedor seleccionado 340 identificado por el Enrutador 330. Cada Objeto de Aplicación 310 puede también recibir una respuesta 360 desde el proveedor seleccionado 340 y pasar la respuesta 360 de vuelta a un usuario, tal como los usuarios 301 y 302. Cada Objeto de Aplicación 310 puede ser capaz también de llamar a un proveedor 340 para deshacer, reintentar o alterar la transacción 320 en respuesta a la respuesta 360, una nueva entrada desde el usuario u otras condiciones del sistema.

Una Transacción 320, tal como las Transacciones 321 y 322, puede incluir los datos requeridos por los proveedores 340 para completar la función del Objeto de Aplicación 310. La Transacción 320 puede incluir información básica

ES 2 330 409 T3

de la transacción, como un identificador único, una marca de tiempo, un marcador de estado, un originador y un destino (o una lista de proveedores 340 para completar la transacción). Cualquier cantidad de información adicional específica de la transacción puede añadirse a la transacción 320 como un elemento de datos. En una realización, el elemento de datos incluye uno o más pares clave/valor que proporcionan una descripción de los datos, tal como un número de cuenta o un PIN, y el dato en sí mismo, por ejemplo, Cuenta # 012345, bloque PIN cifrado según la DES 9876FCA456BDE802. El apartado de datos puede incluir una amplia variedad de datos y tipos de archivo y formatos, tal como una diversidad de números, una diversidad de indicadores, una diversidad de cadenas, una diversidad de archivos de datos, etc. Algunos objetos de datos de ejemplo podrían incluir un archivo gráfico o un cheque cancelado, un archivo de sonido o una muestra de reconocimiento de voz o una hoja de cálculo o una diversidad de transacciones recientes que afectan a un saldo de una cuenta. Los datos pueden incluir adicionalmente un testigo que incluye los datos devueltos en respuesta a una transacción previa. En una realización, cada transacción 320 se almacena como un documento XML para acceso, evaluación y modificación por el Enrutador 330 y los proveedores 340. En otra realización, cada transacción 320 contiene un registro completo de la historia de la transacción. Cada transacción 320 puede almacenarse automáticamente en una base de datos y puede archivarse para recuperación posterior.

El Enrutador 330 determina un Proveedor 340 para manejar la transacción 320. El Enrutador 330 usa una combinación de detalles de la transacción y/o información del sistema para determinar el Proveedor 340 de destino óptimo. Por ejemplo, el Enrutador 330 puede enrutar los datos de transacción de acuerdo con un número de cuenta, una cantidad de la transacción o un nombre de usuario. Pueden emplearse múltiples Enrutadores 330 por el sistema modular 300 para realizar tal enrutado. Una transacción simple 320 puede enrutarse varias veces durante el curso de su procesamiento y el Enrutador 330 puede usarse por los Proveedores 340 así como por los Objetos de Aplicación 310. En una realización, el Enrutador 330 incluye una tabla de enrutado en el formato de un documento de lenguaje de marcado extensible (XML) que lista una diversidad de condiciones y/o una diversidad de reglas bajo las que las transacciones 320 deberían enrutarse hacia un proveedor particular, tal como uno de los Proveedores 341, 342 ó 343.

Los Proveedores 341, 342 y 343 utilizan una diversidad de módulos que incluyen un conjunto lógico para completar al menos una parte de la diversidad de funciones realizadas por uno o más Objetos de Aplicación 310. Tales Proveedores 340 usan los datos almacenados dentro de la transacción 320 para realizar cada una de tales funciones. Los Proveedores 340 pueden devolver una respuesta al Objeto de Aplicación 310 que creó la transacción 320 o pueden pasar la transacción 320 a otro Proveedor 340, consultando o sin consultar al Enrutador 330. El Proveedor 340 realiza su(s) función(es) localmente usando los datos de la transacción 320 y una diversidad de recursos locales y una diversidad de información del sistema y devuelve una respuesta 361 al Objeto de Aplicaciones 210. Algunos Proveedores 340, tales como el Proveedor 342, pueden realizar también la(s) función(es) localmente usando los datos de la transacción 320 y una diversidad de recursos locales y una diversidad de información del sistema, sin embargo, tal (es) función(es) puede(n) ser sólo una parte de la(s) función(es) total(es) requerida(s) por el Objeto de Aplicación 310. La transacción 320 puede modificarse para incluir datos generados por el Proveedor 342 y puede entonces enrutarse a otro Proveedor 340, tal como el Proveedor 343. Algunos Proveedores 340, tales como el Proveedor 343, pueden enrutar todos o una parte de los datos contenidos en la transacción 320 a un Servicio 350 y pueden recibir entonces una diversidad de datos de respuesta desde el Servicio 350 para formular una Respuesta 362 al Objeto de Aplicaciones 210. En una realización, un número de tales Proveedores 340 puede trabajar simultáneamente sobre la misma transacción 320. En otra realización, los Proveedores 340 pueden perseguir el mismo objetivo a través de una diversidad de canales diferentes. Por ejemplo, múltiples Proveedores 340 pueden realizar Servicios múltiples 350 para tener una respuesta más rápida donde varían una diversidad de tiempos de respuestas (por ejemplo, un servicio puede ser más rápido que otros servicios para cualquier solicitud dada dependiendo de un factor de disponibilidad del servidor y de otros factores).

Un Servicio 350, tal como un servicio de envío de datos o un servicio de protocolo de comunicaciones, puede usarse para intercambiar datos con un recurso externo, tal como un sistema de red financiera, un sistema criptográfico o un repositorio de datos. Cada Servicio 350 puede personalizarse para una diversidad de protocolos de comunicación y una diversidad de requisitos de datos de un recurso externo específico. El Servicio 350 puede tanto enviar como recibir datos y los datos recibidos pueden entregarse entonces al Proveedor de servicios 340 que inició el Servicio 350 o pueden añadirse a la transacción 320 y/o pueden devolverse al Objeto de Aplicación 310 en una Respuesta 360.

Las Respuestas 361 y 362 pueden cada una contener una respuesta o una resolución a la transacción 320 creada por el Objeto de Aplicaciones 310. Las Respuestas 361 y 362 pueden incluir cada una información solicitada por el Objeto de Aplicaciones 310 o pueden incluir una explicación de por qué la solicitud expuesta en el Objeto de Aplicaciones 310 no puede ser cumplimentada. En una realización, una Respuesta 360 puede incluir un valor para indicar si se completó o no con éxito la transacción 320; un mensaje que explica por qué la transacción 320 no fue completada con éxito; si es necesario, un testigo, tal como una referencia a la transacción 320 actual, que puede usarse como parte de una transacción posterior, y una diversidad de elementos de datos adicionales (como se ha descrito anteriormente con respecto a la transacción 320). La información devuelta en las Respuestas 360 puede devolverse en su totalidad o en parte al usuario que inició el uso de los Objetos de Aplicación 310 y/o puede ser la base de una transacción adicional 320 iniciada a través del mismo o de otro Objeto de Aplicación 310.

La Figura 4 muestra un diagrama de flujo ilustrando las etapas en el proceso de registro para usar un sistema inalámbrico de transacción financiera, tal como el sistema descrito anteriormente con referencia a las Figuras 1-3. El registro permite a un usuario identificar el dispositivo de comunicaciones inalámbrico 110 (u otros dispositivos) a través del que se accederá al sistema de transacción y para proporcionar los datos de la Pista II desde una o más

ES 2 330 409 T3

de las tarjetas magnéticas del usuario (por ejemplo, tarjetas ATM, tarjetas de débito, tarjetas de crédito, etc.) para las que se permitirá una diversidad de transacciones. En la etapa 410, se inicia un servicio de registro con el sistema de transacción desde un dispositivo terminal equipado con un lector de tarjetas magnéticas. Por ejemplo, un usuario puede ir a un ATM y seleccionar un servicio de registro de un menú de servicios; el usuario puede usar un terminal POS u otro terminal de registro dedicado en una tienda al por menor, tal como una terminal de registro situada en una instalación de un vendedor de servicios/teléfonos inalámbricos; el usuario puede acceder a una página web desde un ordenador personal equipado con un periférico lector de tarjetas magnético y seleccionar una opción de registro; o el usuario puede ir a un banco que emitió una tarjeta particular y usar el terminal de establecimiento del PIN o a otro terminal del banco con un lector de tarjeta magnética para iniciar el servicio de registro. En la etapa 420, se identifica un proveedor de servicios inalámbricos para el usuario. Por ejemplo, el usuario selecciona entre un número de una diversidad de proveedores de servicios inalámbricos disponibles que permiten que se realicen una diversidad de transacciones financieras inalámbricas a través del sistema de transacción. En la etapa 430, un dispositivo de comunicaciones inalámbrico, u otro dispositivo, se identifica para su uso por el usuario en el acceso al sistema de transacción. Por ejemplo, el usuario puede introducir un número de teléfono inalámbrico para el dispositivo de comunicaciones inalámbricas, una dirección de red proporcionada por el proveedor de servicios inalámbricos del usuario, o un número de identificación del dispositivo o un código (por ejemplo, un identificador único proporcionado por un fabricante del dispositivo de comunicaciones inalámbrico). El sistema de transacción puede usar esta información introducida para identificar automáticamente (por ejemplo, el ID del comunicante) una fuente de cualquier solicitud de servicio entrante y acceder a la información del usuario sin requerir ninguna otra entrada del usuario. En la etapa 440, se registran los datos de la tarjeta magnética del usuario y se almacenan en una fuente de datos accesibles para el sistema de transacción. Por ejemplo, el usuario puede pasar su tarjeta magnética a través del lector de tarjetas magnéticas sobre el dispositivo terminal que usa el usuario para el registro y la información de la tarjeta magnética (por ejemplo, los datos de la Pista II, etc.) se envían al sistema de transacción para registrarse en la base de información del usuario, que puede localizarse interna o externamente al sistema de transacción. Las etapas 450 y 460 pueden ser opcionales para uno o más usuarios, dependiendo de las preocupaciones de seguridad del usuario y de las capacidades de cifrado del dispositivo de comunicaciones inalámbricas del usuario. En la etapa 450, el usuario registra su PIN suministrado por la institución financiera que emite la tarjeta. El PIN cifrado del usuario puede registrarse dentro de la base de datos de información del usuario y usarse por el sistema de transacción cuando se accede a datos usando los protocolos de red ATM. El registro del PIN evita que el usuario tenga que enviar nunca el PIN sobre la red a través del dispositivo de comunicaciones inalámbricas, particularmente un dispositivo de comunicaciones inalámbricas sin capacidades de cifrado. En la etapa 460, el usuario selecciona la clave de servicio inalámbrica. La clave de servicio inalámbrica puede usarse por el sistema de transacción para verificar la identidad del usuario. La clave de servicio inalámbrica puede usarse para acceder a una diversidad de servicios proporcionados por el sistema de transacción que no requieren las medidas de seguridad completas del PIN del usuario o servicios tales que pueden usarse por usuarios que han registrado previamente sus PIN con el sistema. La clave del servicio inalámbrica puede usarse también en conjunto con una identificación del dispositivo y el PIN del usuario para proporcionar un nivel de seguridad más alto.

La Figura 5 muestra un diagrama de flujo ilustrando las etapas en el proceso del uso de una diversidad de servicios de transacciones bancarias y financieras a través de un dispositivo de comunicaciones inalámbricas y un sistema de transacción, tal como el sistema descrito anteriormente con relación a las Figuras 1-3. Este proceso permite al usuario utilizar uno o más servicios financieros y bancarios disponibles a través del sistema de transacción, tal como cualquiera de los servicios financieros y bancarios descritos con referencia a la Figura 1. En la etapa 510, se inicia una comunicación con el sistema de transacción. Por ejemplo, el usuario puede marcar un número de teléfono particular o un código de acceso desde su dispositivo de comunicaciones inalámbrico. Alternativamente, el usuario puede iniciar un botón, atajo, opción del menú u objeto similar para iniciar una transacción a través de una página en la Web o un dispositivo de comunicaciones inalámbrico basado en la Web. En la etapa 520, se selecciona un servicio de una diversidad de opciones de servicio disponibles. Por ejemplo, puede proporcionarse al usuario una lista o un menú de una diversidad de servicios disponibles (por ejemplo, un servicio de consulta de saldo, un servicio de movimientos, un servicio de transferencia, etc.). Y el usuario puede indicar cuál de la diversidad de los servicios está interesado en usar. Alternativamente, el usuario puede introducir un código de comando indicando el servicio deseado. En la etapa 530, se proporciona al sistema de transacción un número de cuenta para una o más cuentas a las que el usuario puede desear acceder. El sistema de transacción puede estar habilitado para identificar al usuario (por ejemplo, mediante la ID del comunicante) y puede proporcionar automáticamente un número de cuenta para el usuario. Si el usuario tiene múltiples cuentas habilitadas para transacciones inalámbricas, puede ser capaz de seleccionar una de tales cuentas desde una lista de cuentas habilitadas proporcionadas por el sistema de transacción. En la etapa 540, puede proporcionarse un PIN o clave para verificar la identidad del usuario del dispositivo de comunicaciones inalámbricas y autorizar las transacciones del usuario. Por ejemplo, puede preguntarse al usuario por su PIN asociado con el número de cuenta seleccionado. Alternativamente, puede preguntarse al usuario por una clave para permitir el uso de los datos del PIN almacenados accesibles para el sistema de transacción. En la etapa 550, el usuario puede proporcionar cualquier entrada adicional necesaria para facilitar la ejecución del servicio seleccionado. Por ejemplo, el usuario puede seleccionar un número de transacciones o una diversidad de fechas de transacciones a mostrarse en unos movimientos a generarse por el servicio de movimientos, o el usuario puede hacer una selección de un aviso particular que añadir o borrar de una lista anterior de preferencias de avisos para el usuario. En algunos casos, una selección de servicio y una previsión del número de cuenta u otra identificación del usuario será todo lo que el usuario necesita introducir para ejecutar el servicio seleccionado. En una realización, las etapas 520-550 pueden combinarse en una simple etapa en donde el usuario introduce un código de servicio seguido por un número de cuenta; un PIN, y cualquier otra información necesaria para ejecutar el servicio seleccionado. De modo similar, una diversidad de alias, una diversidad de servicios definidos especialmente o una diversidad de botones dedicados puede permitir a un usuario iniciar un servicio de uso

ES 2 330 409 T3

común sin que se requiera que el usuario seleccione directamente o teclee la información necesaria en las etapas 520-550. En la etapa 560, se proporcionan al usuario los resultados de los servicios requeridos. Por ejemplo, se visualiza sobre la pantalla del dispositivo de comunicaciones inalámbricas del usuario un saldo de la cuenta o una lista de las transacciones. En algunos casos, un indicador de un éxito o un fallo de una transacción puede ser el resultado devuelto al usuario. Una o más de las etapas anteriores pueden repetirse una o más veces para transacciones de servicios múltiples o para una transacción de servicio simple que incluye múltiples intercambios entre el usuario y el sistema de transacción.

La Figura 6 muestra las etapas realizadas en un proceso para proporcionar transacciones inalámbricas bancarias y financieras usando un sistema de transacción, tal como el sistema de transacción descrito anteriormente con referencia a las Figuras 1-3. En la etapa 610, el sistema de transacciones recibe una solicitud de servicio de un usuario. La solicitud de servicio puede recibirse en una comunicación simple o puede utilizar múltiples comunicaciones para acumular toda la información del usuario requerida para ejecutar el servicio solicitado. En la etapa 620, el sistema de transacción crea una transacción para supervisar la información relativa al servicio solicitado y para iniciar el procesamiento del servicio solicitado. En la etapa 630, el sistema de transacción valida la identificación del usuario. Por ejemplo, la validación de la identificación del usuario puede incluir la identificación del dispositivo de comunicaciones inalámbricas o una fuente del servicio solicitado (por ejemplo, usando una ID del comunicante y comparando el número identificado con una base de datos de números de usuarios registrados), la recepción o la recuperación de uno o más números de cuentas y su comparación con los números de cuenta registrados, la recepción o la recuperación de uno o más PIN y su comparación con los PIN registrados y/o la recepción de una clave y su comparación con la clave de usuario esperada (asociada con el dispositivo de comunicaciones inalámbricas del usuario, el número de cuenta del usuario u otra identificación del usuario remitida). En la etapa 640, el sistema de transacción identifica cualquier requisito de intercambio de datos con fuentes externas, tal como instituciones financieras que usan los protocolos de la red ATM. Si no se requieren fuentes externas, el sistema de transacción puede proseguir con la etapa 660 y procesar internamente el servicio solicitado. Si se requiere un servicio externo, pero se requiere un protocolo de comunicaciones distinto del que se usa por la red ATM, el sistema de transacción puede proseguir con la etapa 650 e iniciar la comunicación con el dispositivo externo. Si el servicio externo usa los protocolos de comunicación de la red ATM, entonces el sistema de transacción puede proseguir con las etapas 680 y 690 para generar un bloque PIN cifrado según la DES y acceder a los datos de la Pista II registrados para el usuario. Cuando se genera el bloque PIN cifrado según la DES y se ha accedido a los datos de la Pista II del usuario, el sistema de transacción puede proseguir con la etapa 650. En la etapa 650, el sistema de transacción inicia cualquier comunicación requerida con los recursos externos para cumplimentar el servicio solicitado. En la etapa 660, el sistema de transacción completa cualquier proceso adicional para el servicio solicitado. En la etapa 670, se devuelven los resultados del servicio solicitado mediante el sistema de transacción al usuario que ha realizado la solicitud del servicio, por medio del dispositivo de comunicaciones inalámbricas a través del que se realizó la solicitud del servicio. Estas etapas pueden procesarse en una diversidad de órdenes alternativos y una o más de las etapas pueden repetirse una o más veces para manejar solicitudes de servicio múltiples o solicitudes de servicio más complejas.

En la Figura 7 se muestran una diversidad de terminales de servicio que utilizan una variedad de procedimientos de interfase. Un teléfono móvil 710 habilitado para SMS, un teléfono móvil 720 habilitado para WAP, una PDA con un módem inalámbrico 730 y un ordenador portátil con un módem 740 se muestran conectados a un Sistema de Transacción 750 a través de una o más conexiones de red 760. El Sistema de Transacción 750 se conecta también a través de conexiones de red 760 a al menos un Proveedor de Servicios 751 y a una fuente de datos 752. El Sistema de Transacción 750 puede ser un sistema de transacción sustancialmente como se muestra y se describe con referencia a las Figuras 1-6. El Proveedor de Servicios 751 puede ser un proveedor de datos financieros, tal como un banco, compañía de tarjetas de crédito, compañía de facturación o proveedor de comunicaciones u otro proveedor de servicios, tal como un proveedor de contenidos. La fuente de datos 752 puede ser un registro de datos del usuario, tal como una base de datos que contiene números de cuenta, datos de la Pista II, claves y otra información, para facilitar las transacciones financieras inalámbricas a través de la red de transferencias de fondos electrónica, tal como una red ATM. Las conexiones de red 760 pueden incluir una o más redes de comunicación, tal como una red de comunicaciones inalámbricas y la Internet.

El teléfono móvil 710 habilitado para SMS incluye una pantalla 711 (por ejemplo una pantalla de texto LCD) para visualizar un mensaje de texto y una diversidad de botones 712 para proporcionar las entradas del usuario, incluyendo las entradas numéricas y/o alfanuméricas. En una realización, el teléfono 710 incluye el botón 713 para iniciar la transacción de servicio a través del sistema de transacción 750. El botón 713 puede ser un botón dedicado para el lanzamiento de aplicaciones financieras o puede ser una tecla de función programable programada para iniciar una transacción de servicio. Cuando el usuario del teléfono 710 desea iniciar una transacción, pulsa el botón 713. La pulsación del botón 713 inicia una comunicación con un número de teléfono particular, URL o a través de otro protocolo de comunicación para iniciar un enlace a un servidor de interfase en el Sistema de Transacción 750. En una realización, el teléfono 710 incluye una memoria de acceso aleatorio programable (por ejemplo, SIM, etc.) incluyendo al menos una parte de la lógica de aplicación y/o datos (por ejemplo, estructura del menú, protocolo de seguridad, etc.) residente en el teléfono. En un teléfono de cliente fino, la pulsación del botón 713 puede enviar un mensaje inicial a un servidor de interfase en el Sistema de Transacción 750 que entonces devolverá una serie de texto de peticiones o instrucciones para la navegación por una o más aplicaciones. En el ejemplo de funcionamiento del teléfono 710, puede pedirse primero al usuario que introduzca un número de cuenta, una ID del usuario u otro identificador. Puede pedirse entonces al usuario un PIN, clave u otra verificación de seguridad. Una vez se han verificado la identidad y la seguridad por el Sistema de Transacción 750, puede pedirse al usuario que introduzca "1" para la consulta de saldo,

ES 2 330 409 T3

“2” para los movimientos de cuenta, “3” para una transferencia de saldo o “4” para más opciones. El usuario puede navegar entonces por uno o más menús activados por números usando el teclado numérico incluido en los botones 712 para utilizar una o más aplicaciones.

5 El teléfono móvil 720 habilitado para WAP incluye una pantalla 721 (por ejemplo una pantalla gráfica LCD) para visualizar una interfase de usuario gráfica y una diversidad de botones 722 para proporcionar las entradas del usuario. El teléfono 720 puede incluir una aplicación de navegador WAP para la presentación de los datos de interfase proporcionados por el sistema de interfase del Sistema de Transacción 750. En una realización, el teléfono 720 puede incluir una o más pequeñas aplicaciones almacenadas en la memoria del teléfono 720 para habilitar una o más aplicaciones proporcionadas por el Sistema de Transacción 750. En una realización, el teléfono 720 incluye un menú principal de las funciones del teléfono 723, en las que el usuario puede seleccionar las funciones “CAJERO” o alguna otra designación para iniciar las transacciones de servicio con el Sistema de Transacción 750. La selección de la elección CAJERO (ATM) del menú de opciones puede dirigir al teléfono 720 a establecer la comunicación a través de una URL inalámbrica de la Web correspondiente a uno o más sistemas de interfases incluidos en el Sistema de Transacción 750. 10 El usuario puede navegar entonces por una serie de interfases alfanuméricas, gráficas o una combinación para pedir las entradas del usuario y proporcionar información del Sistema de Transacción 750. La navegación por los menús y opciones proporcionadas sobre la pantalla 721 puede llevarse a cabo a través de peticiones numéricas, como se ha descrito para el teléfono 710 anteriormente o se pueden usar botones de navegación alternativos (por ejemplo, teclas de dirección), un puntero basado en el sistema de navegación (por ejemplo, pantalla táctil y puntero, teclado para dedos, etc.) u otro sistema de navegación. En una realización, la interfase se presenta a partir de uno o más documentos WML y/o aplicaciones Java incluidas en el Sistema de Transacción 750. 15

La PDA con un módem inalámbrico 730 puede incluir una pantalla gráfica 731 que incorpora un dispositivo de entrada, tal como una pantalla táctil (con o sin un puntero). Pueden usarse también otros dispositivos de entrada, tales como teclas de navegación, un teclado, un ratón, hardware y software de reconocimiento de voz u otro periférico o dispositivo de entrada integrado. En el ejemplo mostrado, la PDA 730 incluye un icono una interfase de usuario gráfica basada en ventanas. Las aplicaciones disponibles a través del Sistema de Transacción 750 pueden accederse usando un navegador, con o sin pequeñas aplicaciones u otra lógica y/o datos almacenados dentro de la PDA 730. La iniciación de las transacciones del servicio a través del Sistema de Transacción 750 puede incluir el lanzamiento del navegador y su direccionamiento a una URL correspondiente al sistema de interfase adecuado en el Sistema de Transacción 750. El lanzamiento del navegador, el establecimiento de la conexión de red y el contacto con la URL puede estar o no integrado en una o más etapas. En la realización mostrada, se proporciona un icono 732 (por ejemplo, un acceso directo) para lanzar rápidamente el navegador, establecer una conexión y contactar con la URL en una única etapa. Pueden usarse también marcadores, favoritos u otros procedimientos. En una realización, la interfase se presenta desde uno o más documentos WML o HTML y/o aplicaciones Java incluidas en el Sistema de Transacción 750. 20 25 30 35

El ordenador portátil con un módem 740 puede incluir una pantalla 741, un dispositivo de entrada 742 (por ejemplo un teclado), y otros componentes integrales y periféricos como es conocido en la técnica. El ordenador portátil 740 puede acceder al Sistema de Transacción 750 e iniciar los servicios de transacción a través de uno o más sitios Web y uno o más URL correspondientes disponibles sobre la Red Global Mundial (World Wide Web). En una realización, las aplicaciones del Sistema de Transacción 750 están habilitadas a través de una o más páginas Web y se visualizan usando un navegador Web, tal como Netscape Navigator o Internet Explorer. Se puede acceder a las páginas Web a través de cualquier método de navegación de Red Global Mundial como es conocido en la técnica. En una realización, puede habilitarse un icono que actúa como un atajo sobre el escritorio del usuario o integrado dentro de otra aplicación, tal como una aplicación de gestión financiera (por ejemplo, Quicken o Microsoft Money). En una realización, puede integrarse un icono correspondiente a un enlace de hipertexto a la URL de un sitio Web en uno o más de otros sitios Web, tal como la página de inicio de un usuario, un sitio Web de portal financiero, un sitio Web de servicios financieros, etc. Las aplicaciones en el Sistema de Transacción 750 habilitadas a través de una o más páginas Web sobre la Red Global Mundial pueden ser accesibles a través de tanto conexiones inalámbricas (por ejemplo un módem inalámbrico), como se ha descrito anteriormente, como a través de conexiones basadas en cables (por ejemplo, módems, adaptadores de red, etc.). Las aplicaciones en el Sistema Transacción 750 pueden utilizar también una o más aplicaciones residentes en la memoria del ordenador portátil 740, tal como pequeñas aplicaciones o aplicaciones completas. Estas aplicaciones pueden ser descargables o distribuidas en otra forma a los usuarios para uso en sus dispositivos de servicios finales. 40 45 50

55 Las combinaciones de dispositivos finales de servicio y de protocolos de interfase descritos anteriormente con referencia la Figura 7 son solamente ejemplos y no se intenta que sean exhaustivos de todas las combinaciones disponibles de dispositivos inalámbricos e interfases compatibles y métodos de navegación, las combinaciones adicionales y las ventajas y desventajas de esas combinaciones serán fácilmente evidentes para aquellos expertos en la técnica.

60 Esa invención se ha descrito en conexión con las realizaciones preferidas. Estas realizaciones se intenta que sean solamente ilustrativas. Se apreciará fácilmente por aquellos expertos en la técnica que se pueden realizar modificaciones a estas realizaciones preferidas sin separarse del alcance de la invención como se ha definido en el presente documento. 65

REIVINDICACIONES

1. Un sistema de transacción financiera para proporcionar servicios bancarios y financieros que comprende:

5 (a) una red de datos financieros que utiliza un protocolo de seguridad de datos predeterminado para recibir y transmitir los datos financieros del usuario;

10 (b) un sistema de gestión de la transacción (130, 120) en comunicación con dicha red de datos financieros para ejecutar transacciones seguras de servicios financieros a través de dicha red de datos financieros de acuerdo con el protocolo de seguridad de datos predeterminado en respuesta a las solicitudes de servicio de los usuarios; y

15 (c) un dispositivo de comunicaciones (110, 710) para transmitir y recibir las solicitudes de servicio de los usuarios, siendo procesadas las solicitudes de servicio de los usuarios por dicho sistema de gestión de la transacción (120, 130) usando los datos financieros recuperados desde dicha red de datos financieros;

en el que dicho sistema de gestión de la transacción recibe la solicitud de servicio del usuario en una primera norma de cifrado y remite al menos una parte de los datos de la solicitud de servicio del usuario a dicha red de datos financieros en una segunda norma de cifrado; y

20 en el que el protocolo de seguridad de datos de dicha red de datos financieros incluye datos de validación embebidos en una ficha de seguridad específica del usuario que es una tarjeta;

caracterizado por que:

25 dicho sistema de gestión de la transacción incluye una fuente de datos de dichos datos de validación enlazados al menos a una identificación del usuario, por lo que dicho sistema de gestión de la transacción puede remitir los datos de validación a dicha red de datos financieros en respuesta a la solicitud de servicio del usuario que no contiene los datos de validación.

30 2. El sistema de la reivindicación 1, en el que el sistema de transacción financiera es un sistema inalámbrico de transacción financiera y el dispositivo de comunicaciones es un dispositivo de comunicaciones inalámbricas para transmitir y recibir de modo inalámbrico las solicitudes de servicio del usuario.

35 3. El sistema de la reivindicación 1, en el que el protocolo de seguridad de datos de dicha red de datos financieras incluye un PIN cifrado según la DES y dicho sistema de transacción incluye un sistema criptográfico para convertir un PIN a cifrado DES.

40 4. El sistema de la reivindicación 3, en el que el sistema criptográfico se adapta para recibir el PIN cifrado en un cifrado distinto del cifrado DES y para devolver el PIN en cifrado DES.

5. El sistema de la reivindicación 1, en el que dicha segunda norma de cifrado distinta de DES es el cifrado SSL o WTSL.

45 6. El sistema de la reivindicación 1, en el que los datos de validación son los datos de la Pista II y la ficha específica del usuario es una tarjeta que incluye una banda de datos magnética.

50 7. El sistema de la reivindicación 1, comprendiendo además un terminal de registro en comunicación con dicho sistema de gestión de la transacción y que incluye un lector de tarjetas, por el que un usuario puede remitir dichos datos de validación a dicho sistema de gestión de la transacción para el almacenamiento en la fuente de datos.

8. El sistema de la reivindicación 1, en el que dicho sistema de gestión de la transacción incluye una pasarela de comunicaciones (210), un servidor de aplicaciones (220) y un servidor de interfase (230).

55 9. El sistema de la reivindicación 1, en el que dicho sistema de gestión de la transacción incluye una pasarela de la red de datos financieros para dirigir los datos financieros entre una diversidad de proveedores de servicios financieros y/o otras pasarelas de redes de datos financieros incluidos en dicha red de datos financieros.

60 10. El sistema de la reivindicación 1, en el que dicho sistema de gestión de la transacción es un dispositivo SMS, un dispositivo WAP o un dispositivo habilitado para la Web.

11. Una fuente de datos para el uso en la remisión de transacciones financieras a una red de datos financieros (760) que comprende:

65 (a) un identificador del usuario para un usuario; y

ES 2 330 409 T3

(b) datos de validación de la cuenta para al menos una cuenta de usuario asociada con dicho identificador del usuario, correspondiendo dichos datos de validación de la cuenta a datos de una ficha de seguridad que es una tarjeta que requiere que se tenga acceso a un lector de tarjetas;

5 **caracterizado** por que:

la fuente de datos se dispone para permitir el acceso desde un sistema de gestión de la transacción para formular una solicitud de servicios financieros para el usuario a través de la red de datos financieros (760) en respuesta a una solicitud de servicio del usuario que no contiene los datos de validación de la cuenta, disponiéndose la fuente de datos para proporcionar dichos datos de validación de la cuenta a dicho sistema de gestión de la transacción de forma que en respuesta a dicha solicitud de servicio del usuario el sistema de gestión de la transacción puede remitir los datos de validación a la red de datos financieros en dicha solicitud de servicios financieros.

12. La fuente de datos de la reivindicación 11, en la que los datos de validación son los datos de la Pista II y la ficha de seguridad es una tarjeta que incluye una banda de datos magnética que contiene los datos de la Pista II.

13. La fuente de datos de la reivindicación 11, comprendiendo además una diversidad de identificadores de cuenta del usuario, asociados cada uno de dicha diversidad de identificadores de cuenta con dichos datos de validación de cuenta para el acceso a cada cuenta.

14. La fuente de datos de la reivindicación 11, comprendiendo además datos de validación del usuario para la validación del usuario antes de remitir la solicitud de servicios financieros que incluye dichos datos de validación de cuenta a la red de datos financieros.

15. La fuente de datos de la reivindicación 14, en la que dichos datos de validación del usuario incluyen una clave y/o un identificador del dispositivo terminal.

16. La fuente de datos de la reivindicación 11, comprendiendo además un PIN cifrado asociado con dichos datos de validación de la cuenta para la remisión a la red de datos financieros en una solicitud de servicio financiero.

17. Un método de proporcionar transacciones financieras, basado en los datos de una red de datos financieros que usa un protocolo de seguridad predeterminado que involucra unos datos de validación de cuenta de una ficha de seguridad específica del usuario en la forma de una tarjeta, comprendiendo el método las etapas de:

(a) recibir una solicitud de servicio (610) de un usuario que usa un dispositivo terminal unido a la red (710, 720, 740), incluyendo la solicitud de servicio, medios para identificar una cuenta de usuario y que no incluye ni un PIN cifrado para cumplir con el protocolo de seguridad predeterminado de la red de datos financieros ni dichos datos de validación de la cuenta de la tarjeta del usuario para su uso en el protocolo de seguridad predeterminado;

(b) proporcionar un PIN cifrado para cumplir el protocolo de seguridad predeterminado de la red de datos financieros mediante la remisión de un PIN no cifrado para cumplir con el protocolo de seguridad predeterminado a un sistema criptográfico que devuelve el PIN cifrado para cumplir con el protocolo de seguridad predeterminado;

(c) proporcionar una información de validación de la cuenta que corresponde a los datos de validación de la cuenta de la tarjeta del usuario, mediante el acceso a una fuente de datos de un sistema de gestión de la transacción, conteniendo la fuente de datos los datos de validación de la cuenta de la tarjeta del usuario para una cuenta especificada por la solicitud de servicio del usuario;

(d) iniciar una transacción de servicio financiero a través de la red de datos financieros (760, 750) que incluye el PIN cifrado para cumplir el protocolo de seguridad predeterminado y el dato de validación de la cuenta de la tarjeta del usuario; y

(e) devolver al usuario un resultado del servicio solicitado basándose en el resultado de la transacción de servicios financieros.

18. El método de la reivindicación 17, en el que el PIN devuelto se cifra según la DES.

19. El método de la reivindicación 17, en el que los datos de validación de la cuenta incluyen los datos de la Pista II y la ficha de seguridad del usuario es una tarjeta con una banda magnética de datos.

20. El método de la reivindicación 17, comprendiendo además la etapa de recibir los datos de validación de la cuenta del usuario de la tarjeta del usuario a través de un dispositivo terminal de registro que incluye un lector de tarjetas y guardar los datos de validación de la cuenta en una fuente de datos para el uso en la etapa (c), siendo dicho dispositivo terminal en red del usuario un dispositivo de comunicaciones no equipado con dicho lector de tarjetas.

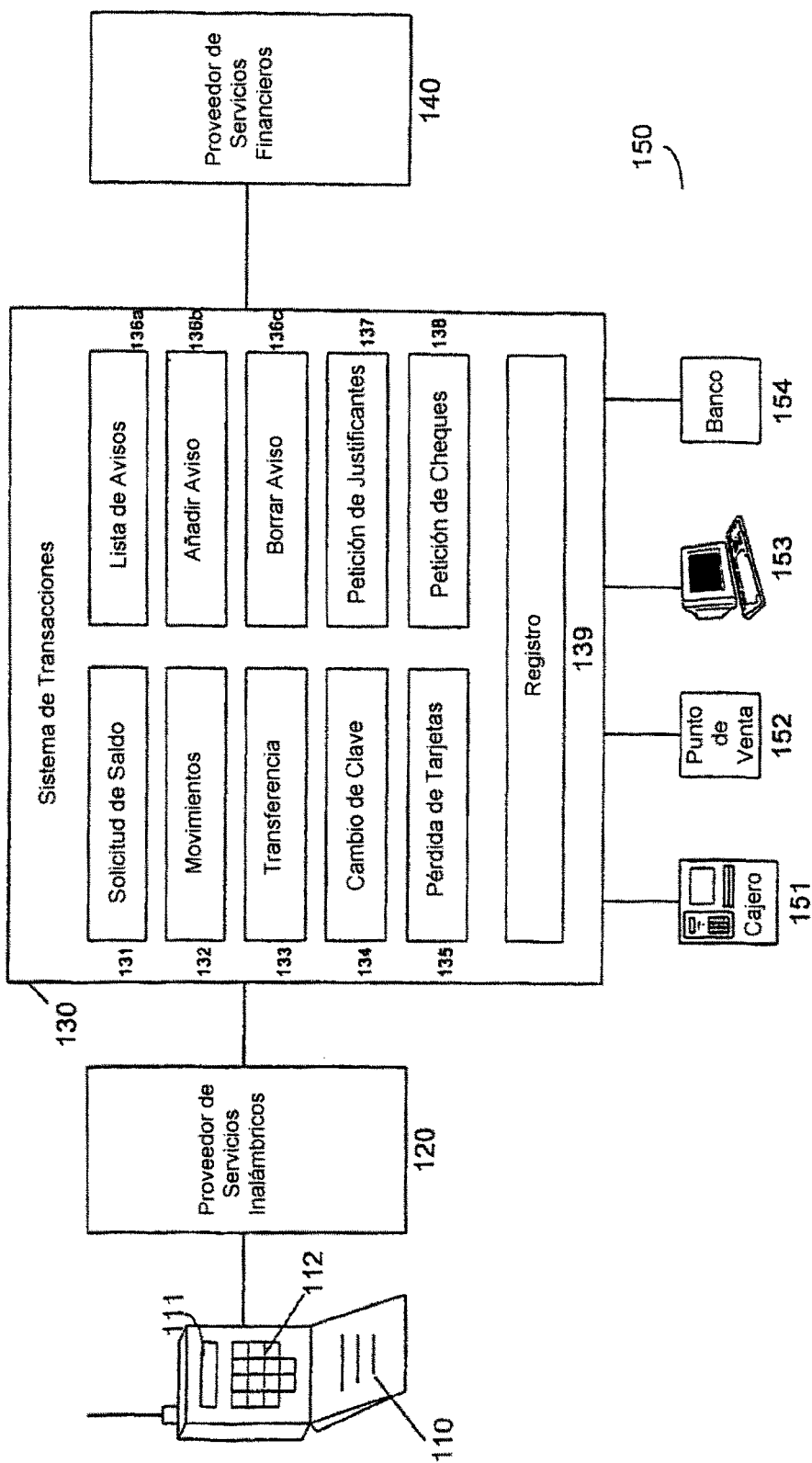


Figura 1

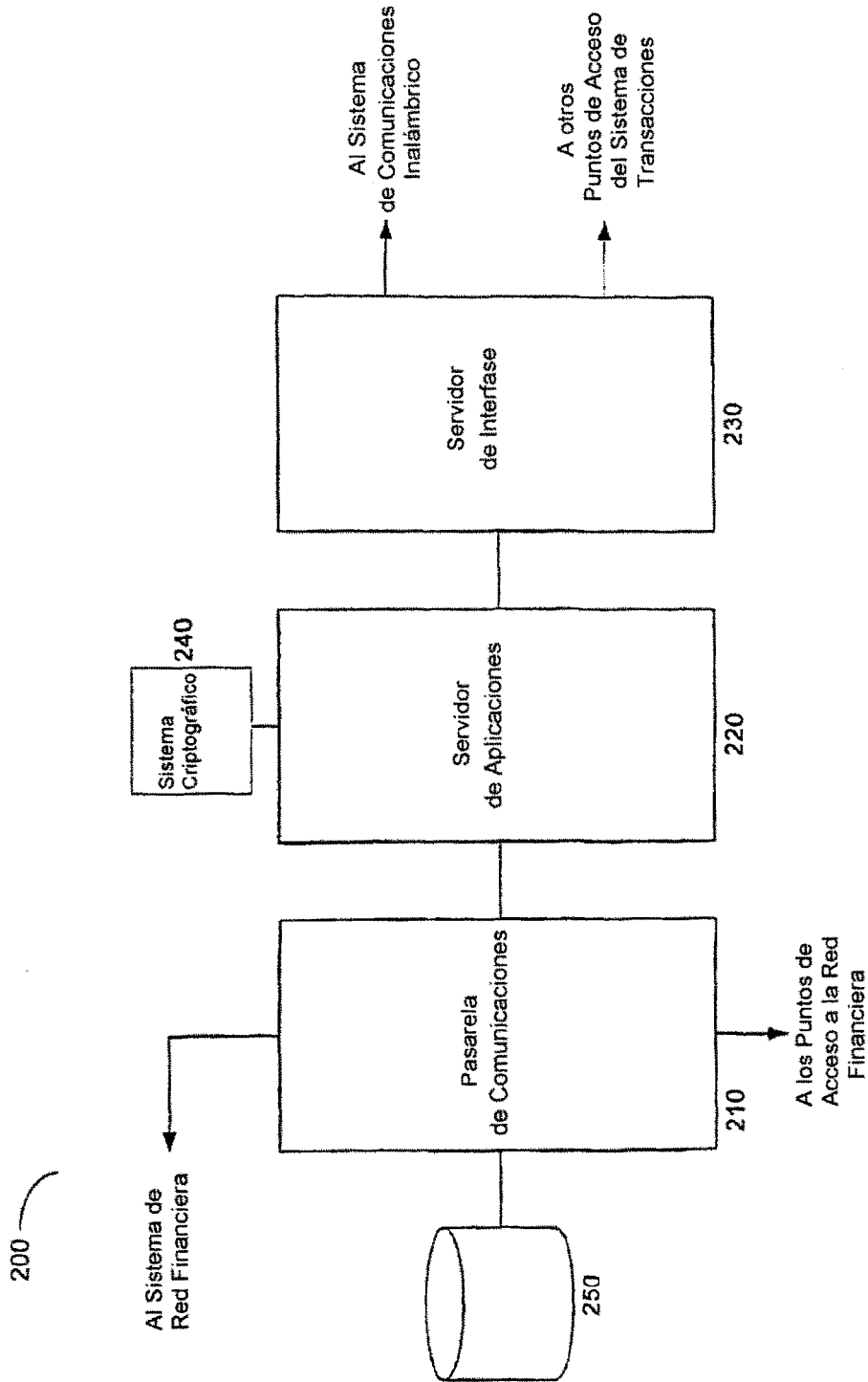


Figura 2

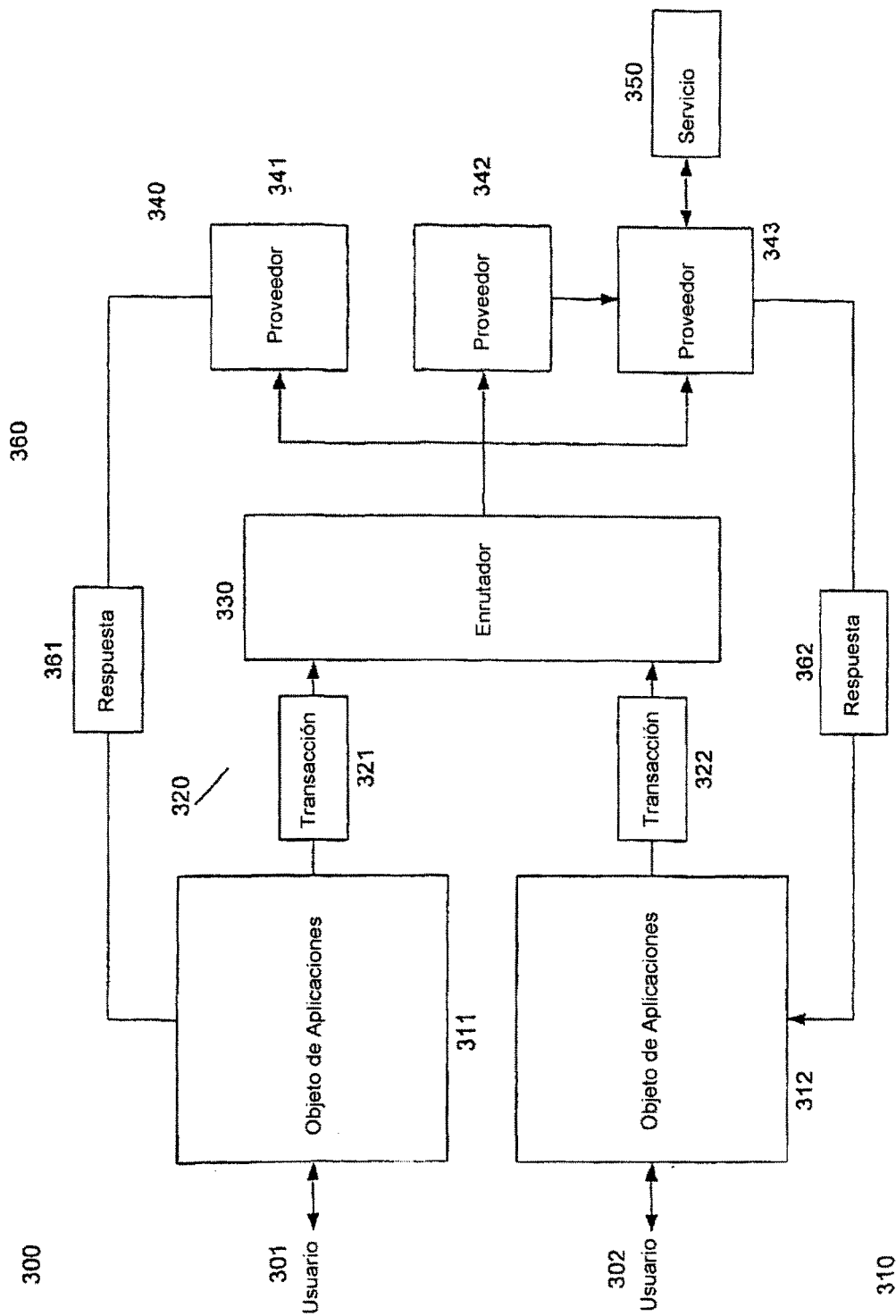


Figura 3

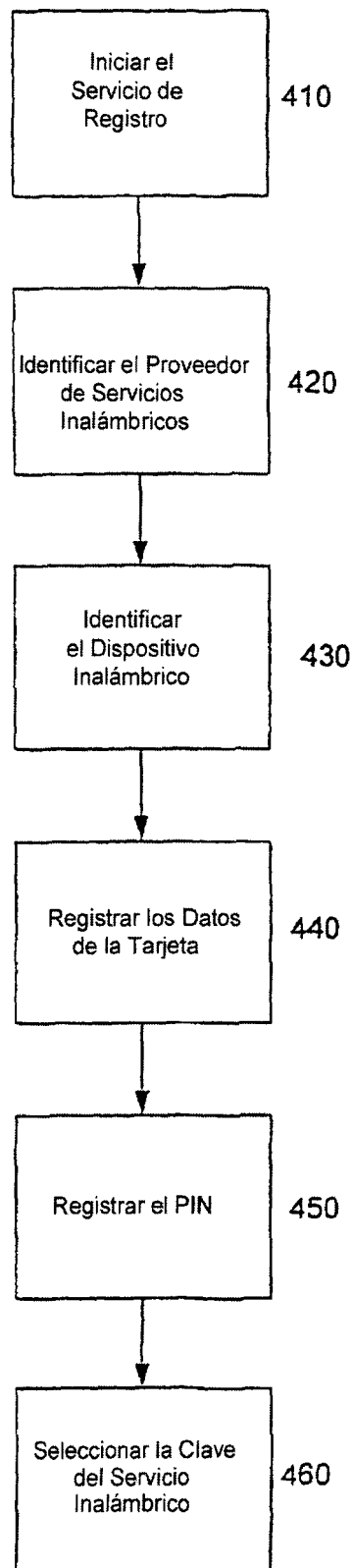


Figura 4

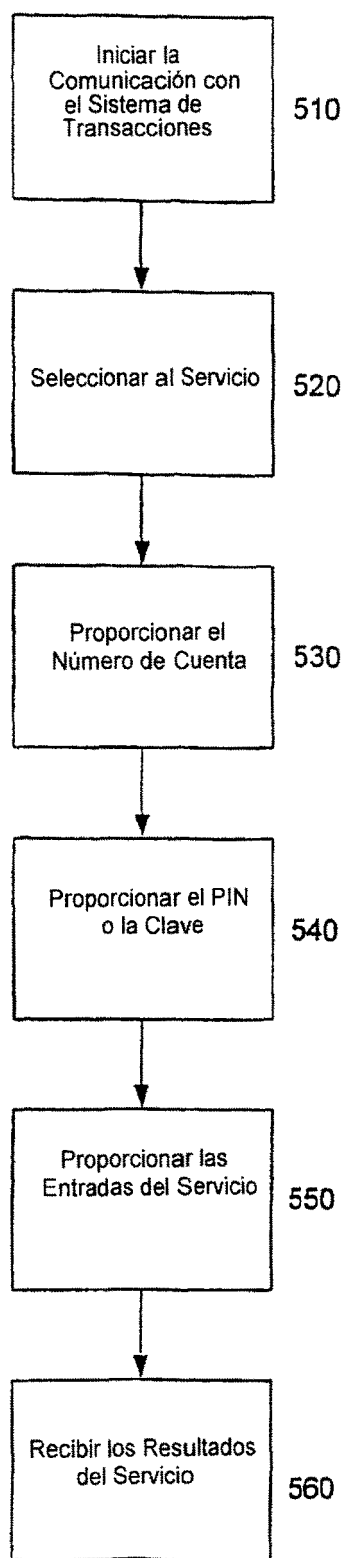


Figura 5

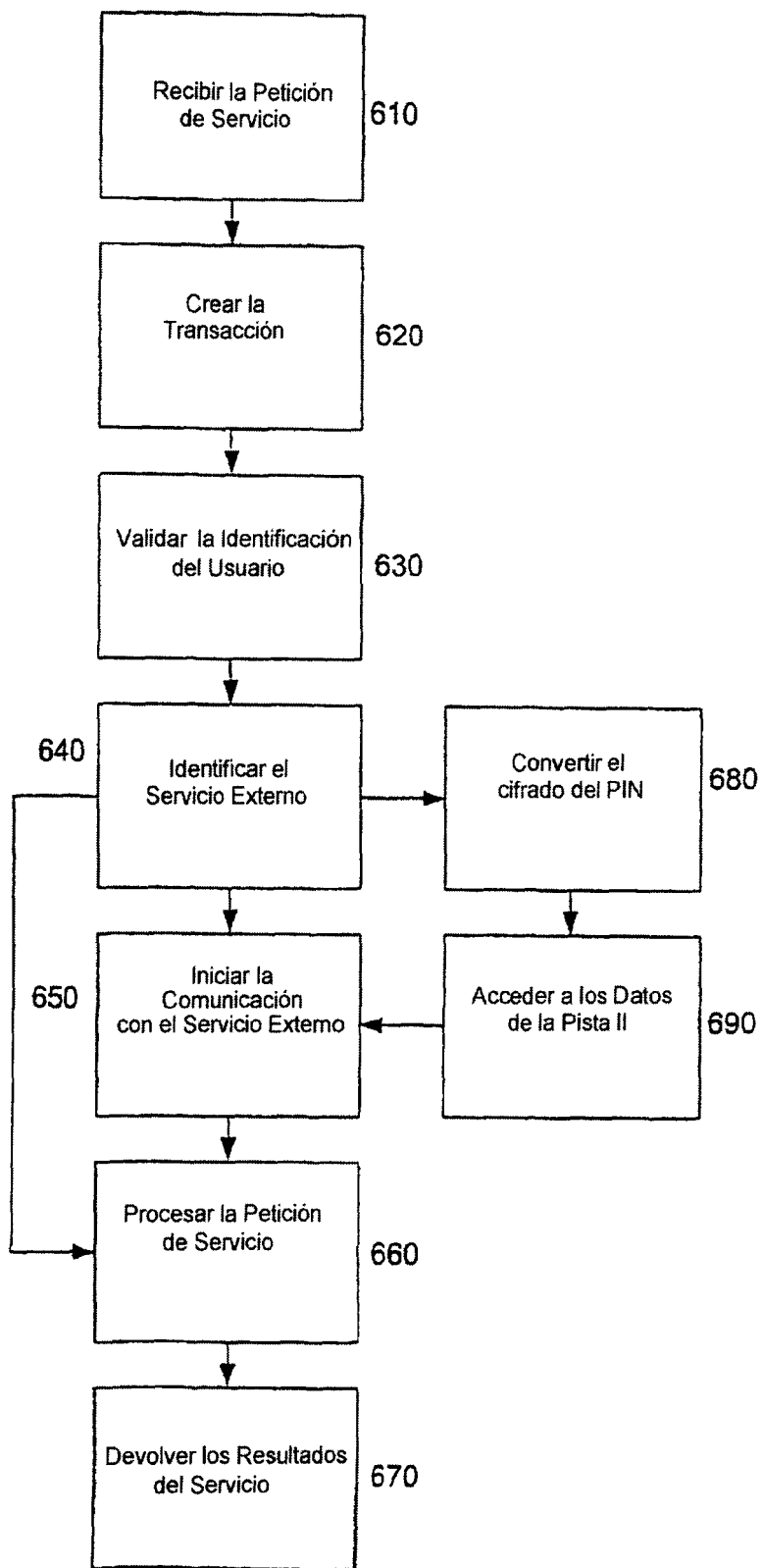


Figura 6

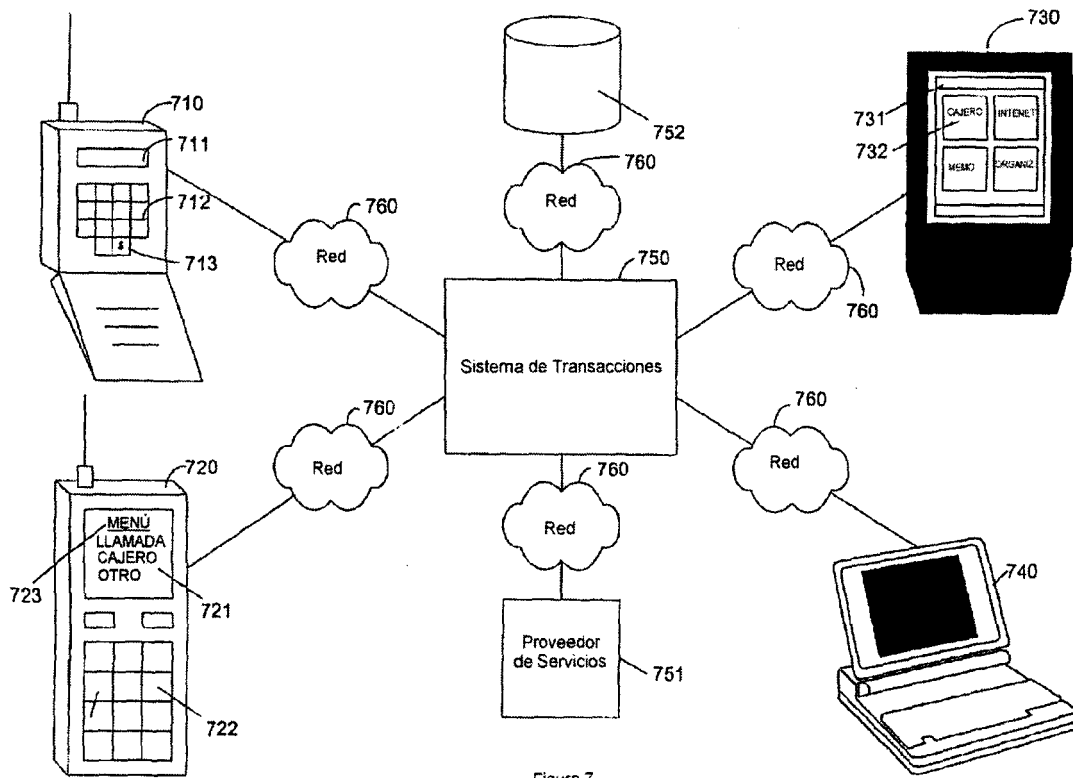


Figura 7