(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 415 365**

(51) Int. CI.:

H04M 15/00 (2006.01)
H04W 4/24 (2009.01)
G06Q 20/12 (2012.01)
G06Q 20/32 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **11.08.2006 E 06779120 (2)**

(97) Fecha y número de publicación de la concesión europea: **03.04.2013 EP 1922681**

(54) Título: **Gestión de cuentas móviles**

(30) Prioridad:

12.08.2005 GB 0516616

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.07.2013

(73) Titular/es:

VODAFONE GROUP PLC (100.0%)
VODAFONE HOUSE THE CONNECTION
NEWBURY
BERKSHIRE RG14 2FN, GB

(72) Inventor/es:

MURDOCH, TIMOTHY, NORTON, SHERARD;
BOWLEY, CHRISTOPHER;
VAUGHAN, LESLEY-ANN;
CAREW, WARREN, DOUGLAS;
HUGHES, NICK y
LONIE, SUSIE

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Gestión de cuentas móviles

La presente invención versa acerca de la gestión de transacciones seguras en una red de la gestión de transacciones seguras en una red de comunicaciones inalámbricas. En particular, la invención versa acerca de la transferencia segura de mensajes que representan el intercambio de la titularidad de activos monetarios.

Una gran proporción de la población mundial no se ve atendida por instalaciones bancarias convencionales. Hay instalaciones limitadas para transferir dinero entre “empresas” (por ejemplo, de un negocio a otro) o entre individuos (de un sitio a otro). En consecuencia, a menudo, el efectivo debe cambiar de mano físicamente. Esta falta de instalaciones bancarias afecta mucho a pequeños empresarios en mercados emergentes.

Se entiende que la forma en que tales empresarios de poca envergadura acceden a financiación, denominada “microcrédito” o “microfinanzas”, resulta vital para estimular la actividad económica en los mercados emergentes.

La disponibilidad de servicios financieros (como microcréditos/microfinanzas) está limitada por la infraestructura implementada para distribuirlos, lo que hace a los sistemas existentes lentos, costosos y, cuando hay efectivo implicado, a menudo inseguros.

En muchas economías emergentes, la red celular proporciona la plataforma en la que pueden distribuirse servicios financieros, que supera en mucho el alcance de las líneas terrestres, de las sucursales bancarias y de los cajeros automáticos (ATM), que están restringidos en buena medida a las zonas urbanas. Por esta razón, se han implementado varios sistemas usando la funcionalidad de los mensajes cortos convencionales (SMS) de las redes celulares en un intento de abordar la necesidad de los clientes: dar acceso a servicios financieros usando las redes y los teléfonos móviles como canales de distribución.

Un sistema conocido, Fundamo Elevator, desplegado en Zambia como CelPay, estaba destinado a clientes de alto nivel adquisitivo y se basaba en el protocolo SIM. Se proporciona una tarjeta SIM CelPay a los clientes dados de alta. La tarjeta SIM está programada para generar un nuevo menú una vez que es insertada en un terminal móvil adecuado. Las cuentas de CelPay se nutren de fondos ya sea mediante una transferencia desde una cuenta bancaria convencional o depositando directamente efectivo o cheques en un banco socio de CelPay. Cuando el usuario de CelPay desea efectuar un pago, usa el menú de CelPay de su terminal para introducir un número de identificación personal (PIN) seguro. Tanto el pagador como el beneficiario reciben confirmación de la transacción (en forma de un mensaje SMS). Dado que cada transacción tiene un único número de referencia, con plenos detalles disponibles en línea (en la red mundial, la “Red”), el comerciante o proveedor (con la condición de que tenga acceso a la Red) tiene un registro completo de auditoría de quién pagó qué, y cuándo. El comerciante o proveedor también debe disponer de una cuenta especial habilitada para Celpay en la que se realizará cualquier transferencia. Después, según la instrucción del comerciante, los fondos pueden ser transferidos a la cuenta bancaria principal del comerciante.

Otro sistema, Globe G-Cash, en las Filipinas, usa la notificación SMS en relación con una “transferencia simple de dinero” convencional de persona a persona a través de agentes de sucursal. Se proporciona una cuenta G-Cash a cada usuario dado de alta. Los mensajes SMS que solicitan un pago en G-Cash a cuentas beneficiarias son enviados a un número de código corto (un servicio central) para su procesamiento (por ejemplo, para pagar un recibo o comprar crédito para llamadas).

Smart Money, también implementado en las Filipinas, usa “créditos inteligentes” como pagos electrónicos. La aplicación Smart Money hace uso de una tarjeta monedero electrónico que está vinculada con una cuenta de teléfono móvil. La tarjeta puede ser usada como una tarjeta de débito. Alternativamente, usando teléfonos móviles, los clientes con cuentas bancarias pueden, mediante SMS, cargar dinero en la tarjeta, transferir dinero entre tarjetas, realizar un seguimiento de transacciones, pagar recibos, etc.

Otro mecanismo bien conocido de transferencia de dinero en ausencia de instalaciones bancarias es la prestación de “enviar por cable” efectivo en forma de remesas internacionales, proporcionada por empresas como la Western Union.

Los sistemas existentes han encontrado cierto éxito. Sin embargo, dependen de que los clientes tengan acceso a una infraestructura convencional, como una cuenta bancaria, la Red y/o una sucursal adecuada. Esto excluye a muchos pequeños empresarios, para quienes el acceso a tan básica infraestructura es una carga considerable.

Para superar las dificultades precedentes, se proporciona un sistema de gestión de cuentas habilitado por teléfono móvil para mantener una pluralidad de cuentas virtuales en un sistema de comunicaciones celulares, transportando mensajes el sistema de comunicaciones celulares entre terminales móviles e incluyendo cada terminal móvil una tarjeta de datos con un identificador único, incluyendo el sistema de gestión de cuentas:

un medio de mensajería que está adaptado para recibir mensajes de transacciones entrantes procedentes de terminales móviles que usan el sistema de comunicaciones, incluyendo los mensajes entrantes el

identificador único del terminal móvil de origen, y para transmitir mensajes de transacciones salientes a los terminales móviles en respuesta;
un procesador de transacciones que está acoplado al medio de mensajería mediante un par de colas de mensajes y adaptado para interpretar los mensajes de transacciones entrantes y para producir correspondientes instrucciones de transacciones;
un medio de seguridad de mensajes, acoplado al procesador de transacciones, que autentica los mensajes de transacciones entrantes comparando el identificador único incluido con las entradas de una lista de cuentas virtuales válidas; y
una interfaz de almacenamiento de datos de transacciones, acoplada al procesador de transacciones, a través de la cual el procesador de transacciones se comunica con un almacén de datos, estando adaptada la interfaz para transportar instrucciones para modificar datos contenidos en una o más cuentas virtuales válidas almacenadas en el almacén de datos y para transportar mensajes de transacción completa desde el almacén de datos al procesador de transacciones cuando se completa la modificación;
en el que las colas de mensajes incluyen una cola de recepción y una cola de envío, estando adaptada la cola de recepción para poner en cola de espera los mensajes recibidos del procesador de transacciones y estando adaptada la cola de envío para enviar a la cola de espera los mensajes enviados al procesador de transacciones;
en el que el procesador de transacciones también está adaptado para interpretar mensajes de transacción completa y para dar salida a correspondientes mensajes interpretados de transacción completa hacia el medio de mensajería mediante la cola de recepción;
en el que cada mensaje interpretado de transacción completa incluye información de seguridad generada a partir de identificadores únicos de cuentas virtuales modificadas, estando adaptado el medio de mensajería para dirigir los mensajes salientes generados a partir de los mensajes interpretados de transacción completa hacia correspondientes terminales móviles; y
en el que cada mensaje saliente recibido está en un formato que requiere la introducción de una clave única desde la tarjeta de datos insertada en el terminal móvil, garantizándose con ello que el mensaje saliente solo pueda ser leído en presencia de una tarjeta de datos con una clave única que coincida con la información de seguridad del mensaje saliente.

Así, el sistema de gestión de cuentas es una plataforma de gestión de cuentas habilitado por teléfono móvil. Este sistema tiene la funcionalidad de permitir mover dinero tanto entre empresas como entre personas, a través de terminales móviles (en particular, mediante el uso de teléfonos móviles GSM, de disponibilidad generalizada). El sistema hace uso de un soporte lógico especialmente desarrollado que se ejecuta en una tarjeta SIM del teléfono móvil para mantener la conversación con el usuario final y usa el servicio de mensajes cortos (SMS) para la comunicación entre la tarjeta SIM y un servidor central. Esto tiene la ventaja de poder ejecutarse en teléfonos móviles de bajas prestaciones que no soporten necesariamente GPRS.

Según un aspecto adicional de la invención, se proporciona un procedimiento habilitado por teléfono móvil para mantener una pluralidad de cuentas virtuales en un sistema de comunicaciones celulares, transportando el sistema de comunicaciones celulares mensajes entre terminales móviles e incluyendo cada terminal móvil una tarjeta de datos con un identificador único, comprendiendo el procedimiento:

recibir mensajes de transacciones entrantes procedentes de terminales móviles que usan el sistema de comunicaciones, incluyendo los mensajes entrantes el identificador único del terminal móvil de origen;
poner en cola de espera los mensajes entrantes;
interpretar los mensajes de transacciones entrantes;
autenticar los mensajes de transacciones entrantes comparando el identificador único incluido con las entradas de una lista de cuentas virtuales válidas;
cuando los mensajes de transacciones entrantes son auténticos, producir correspondientes instrucciones de transacciones para modificar datos contenidos en una o más cuentas virtuales válidas almacenadas en un almacén de datos;
recibir mensajes de transacción completa desde el almacén de datos cuando se completa la modificación;
poner en cola de espera los mensajes de transacción completa; y
transmitir los mensajes de transacciones salientes a los terminales móviles de origen, incluyendo cada mensaje interpretado de transacción completa información de seguridad generada a partir de identificadores únicos de cuentas virtuales modificadas;
en el que cada mensaje saliente recibido está en un formato que requiere la introducción de una clave única desde la tarjeta de datos insertada en el terminal móvil, garantizándose con ello que el mensaje saliente solo pueda ser leído en presencia de una tarjeta de datos con una clave única que coincida con la información de seguridad del mensaje saliente.

Creando una serie de cuentas virtuales dentro de una cuenta de depósito estándar operada en nombre de clientes individuales y de organizaciones, tal como instituciones de microfinanzas (MFI), la plataforma permite que usuarios individuales, proveedores de servicios y agentes para mover “fondos asignados” entre estas cuentas virtuales dan instrucciones al gestor de la cuenta para que lo haga; por ejemplo, a través de SMS.

Una vez que se ha dado a un individuo una cuenta virtual, puede asignarse dinero a esta (por ejemplo, por parte de un proveedor de servicios de microfinanzas). Puede moverse valor entre cuentas dentro del sistema de cuentas virtuales cuando se reciben instrucciones, digamos, a través de SMS. Por ejemplo, un individuo puede solicitar que se mueva valor entre su cuenta virtual y la correspondiente cuenta virtual de un comerciante al que compra bienes o servicios.

El valor representado por la cuenta virtual puede ser convertido en efectivo con cualquier agente dado de alta, tal como un revendedor de minutos de llamada o cualquier ubicación que tenga un “flujo de efectivo” adecuado (tiendas, gasolineras, etc.). Estos agentes están mucho más extendidos que las sucursales bancarias, y es más conveniente acceder a los mismos. El proceso es rápido y los costes de transacción deberían reducirse sustancialmente. En particular, este arreglo también obvia la necesidad del movimiento físico de “efectivo” (y de re(contarlo)) y, por ello, ofrece beneficios de seguridad para el usuario.

Usar tecnología móvil para realizar transacciones financieras más rápidas, más baratas y más seguras facilita la distribución de servicios financieros en mercados emergentes en los que otros mecanismos de transacciones financieras resultan poco atractivos. La invención también facilita la transferencia de dinero más generalizada entre trabajadores emigrantes y su familia.

Preferentemente, se proporciona la plataforma con una capa de seguridad. La capa de seguridad puede implementarse en cada etapa de una transacción. Esta capa está incorporada en el Gestor de cuentas para proteger contra un uso fraudulento.

La seguridad del intercambio de información entre usuarios individuales, proveedores de servicio y agentes (es decir, un terminal con un SIM apropiado instalado), por una parte, y del gestor de cuentas, por otra, puede mejorarse requiriendo el cifrado del mensaje (por ejemplo, un mensaje SMS) usando una clave que es compartida entre ambas partes. Para efectuar este cifrado de clave compartida, el SIM usado en el terminal puede estar dotado de una aplicación con un Juego de Herramientas SIM (STK) para cifrar y descifrar tales mensajes.

Alternativamente, o además, puede proporcionarse seguridad usando otras comprobaciones de ID y seguridad independientes del SIM o el terminal. Ejemplos de tales comprobaciones alternativas incluyen: números de identificación personal (PIN), combinaciones de nombre de usuario/contraseña; parámetros biométricos (por ejemplo, barridos del iris, huellas dactilares, reconocimiento de patrones de voz, etc.). Estas comprobaciones pueden usar funcionalidades existentes en el terminal (es decir, el teclado y el micrófono) para obtener datos para el procesamiento en un servidor seguro: así, pueden usarse una respuesta interactiva de voz (IVR) o un reconocimiento de voz para obtener del usuario información segura. Una ventaja de esto es que un terminal y un único SIM pueden ser compartidos por toda una comunidad de usuarios, de forma similar a un dispositivo de punto de venta: las cuentas de usuario pueden distinguirse requiriendo la introducción de información adicional de ID y seguridad.

Preferentemente, también se proporciona un medio de documentación que permite que se realice un seguimiento del movimiento de valor entre las cuentas virtuales. El medio de documentación también puede realizar un seguimiento de la conversión en efectivo. Por ello, el medio de documentación proporciona una pista de auditoría que puede ser requerida por las autoridades reguladoras.

Para una mejor comprensión de la presente invención, se describirá ahora una realización a título de ejemplo, con referencia a los dibujos adjuntos, en los que:

la Figura 1 muestra esquemáticamente una red en la que la invención puede ser usada;
la Figura 2 es un dibujo esquemático de un sistema microfinanciero que incorpora un sistema de gestión de cuentas virtuales según la presente invención;
la Figura 3 muestra el flujo de información en el sistema de la Figura 2;
la Figura 4 ilustra algunas de las transacciones microfinancieras facilitadas por la presente invención; y
la Figura 5 ilustra la operación de una prestación de envío de mensajes para superar las restricciones de cortafuegos.

La Figura 1 muestra esquemáticamente una red en la que la invención puede ser usada. La figura muestra una red celular. Sin embargo, debería apreciarse que la invención es aplicable a cualquier tipo de red, aunque es particularmente aplicable a una red en la que al menos algunos de los dispositivos se comuniquen usando telecomunicaciones móviles/transmisión inalámbrica de datos. El terminal móvil 1 está dado de alta en la red 3 de telecomunicaciones móviles GSM/GPRS o UMTS (3G). El terminal móvil 1 puede ser un terminal telefónico móvil, una agenda electrónica (PDA) o un ordenador portátil equipado con una tarjeta de datos. El terminal móvil 1 se comunica de forma inalámbrica con la red 3 de telecomunicaciones móviles a través de una red de acceso de radio (RAN) de la red 3 de telecomunicaciones móviles, que comprende, en el caso de una red UMTS, una estación base 5 (nodo B) y un controlador 7 de red de radio (RNC). Las comunicaciones entre el terminal móvil 1 y la red 3 de telecomunicaciones móviles se encaminan desde la red de acceso de radio mediante nodos 9 de soporte de GPRS (SGSN), que pueden estar conectados mediante un enlace fijo (cable) a la red 3 de telecomunicaciones móviles.

De manera convencional, una multiplicidad de otros terminales móviles está dada de alta en la red 3 de telecomunicaciones móviles. Estos terminales móviles incluyen los terminales móviles 11 y 13. Los terminales 11 y 13 se comunican con la red 3 de telecomunicaciones móviles de una manera similar al terminal 1, es decir, mediante uno nodo B 5 apropiado, el RNC 7 y el SGSN 9.

La red 3 de telecomunicaciones móviles incluye un nodo 17 de soporte pasarela GPRS (GGSN) que permite las comunicaciones basadas en IP con otras redes, tal como Internet 19 mediante un enlace apropiado 21. Varios terminales están conectados con Internet (mediante enlaces fijos o inalámbricos) y se muestran a título de ejemplo un terminal PC 23 y un terminal PDA 25.

Cada uno de los terminales móviles 1, 11 y 13 está dotado de un respectivo módulo 15 de identidad de abonado (SIM). Durante el proceso de fabricación de cada SIM, se almacena en el mismo información de autenticación bajo control de la red 3 de telecomunicaciones móviles. La propia red 3 de telecomunicaciones móviles almacena detalles de cada uno de los SIM usados bajo su control. En operación de la red 3 de telecomunicaciones móviles, un terminal 1, 11, 13 se autentica (por ejemplo, cuando el usuario activa el terminal en la red de cara a realizar o recibir llamadas) porque la red envía un desafío al terminal 1, 11, 13 que incorpora un SIM 15, en respuesta a lo cual el SIM 15 calcula una respuesta (dependiente de la información predeterminada contenida en el SIM: típicamente un algoritmo de autenticación y una clave única Ki) y la transmite, devolviéndola a la red 3 de telecomunicaciones móviles. La red 3 de telecomunicaciones móviles incluye un procesador 17 de autenticación que genera el desafío y que recibe la respuesta del terminal 1, 11, 13.

Usando información almacenada de antemano relativa al contenido del SIM relevante 15, el procesador de autenticación calcula el valor esperado de la respuesta procedente del terminal móvil 1, 11, 13. Si la respuesta recibida coincide con la respuesta calculada esperada, se considera que el SIM 15 y el terminal móvil asociado están autenticados.

Debería entenderse que puede llevarse a cabo tal proceso de autenticación para cualquier terminal dotado de un SIM 15 bajo control de la red 3 de telecomunicaciones móviles. En la realización, el terminal se comunica de forma inalámbrica con la red 3 de telecomunicaciones móviles a través de la red de acceso de radio de la red, aunque esto no es esencial. Por ejemplo, el terminal puede comunicarse con la red a través de la red de telefonía fija (PSTN), a través de un “punto de acceso” UMA y/o a través de Internet. El PC 23 y la PDA 25 también pueden estar dotados de un SIM 15 bajo control de la red.

El SIM 15 usando por el terminal 1, 11, 13, 23, 25 puede ser un SIM del tipo definido en las especificaciones de los estándares GSM o UMTS, o puede ser una simulación de un SIM, es decir, soporte lógico o soporte físico que lleve a cabo una función correspondiente a la del SIM. El SIM puede ser conforme a la disposición descrita en el documento WO-A-2004 036513.

Debería hacerse notar que el proceso de autenticación que se describe no autentica necesariamente la identidad humana del usuario. Por ejemplo, las redes de telecomunicaciones móviles tienen abonados de prepago a los que se dota de SIM a cabo del prepago, permitiéndoles usar servicios de red. Sin embargo, la identidad de tales abonados de prepago puede no ser conocida por la red. No obstante, tal usuario no puede hacer uso de la red hasta que la red haya autenticado el SIM del usuario, es decir, haya confirmado que tal usuario es un usuario particular que tiene una cuenta particular de prepago con una red.

La red mostrada en la Figura 1 comprende también la red 3 de telecomunicaciones móviles como Internet 19 (que comprende ella misma una multiplicidad de otras redes).

El procedimiento para la transmisión de “mensajes cortos” es diferente. La expresión “mensajes cortos” o “mensajes SMS”, usada en relación con las realizaciones, significa mensajes cortos, definidos en las especificaciones de los estándares GSM o 3G. Tales mensajes están comúnmente en forma de mensajes de textos de longitud máxima limitada, pero pueden tener otras formas, tal como en forma de datos binarios, o pueden contener datos de configuración para cambiar los parámetros funcionales de un móvil. La invención no está limitada a la transmisión de mensajes de este tipo de “mensajes cortos”.

Los mensajes cortos pueden ser enviados hacia o desde móviles tales como los móviles 1, 11, 13 y otros pertenecientes a la red 3. Sin embargo, además, pueden enviarse mensajes cortos hacia o desde “entidades de mensajes cortos” (SME), tales como las mostradas en 20, 20A, 20B. Estas SME pueden estar en forma de terminales de diversos tipos, tales como terminales fijos, para el envío de mensajes cortos de diversos tipos a móviles y para la recepción de mensajes cortos procedentes de móviles. Por ejemplo, las SME pueden estar en forma de terminales asociados con ordenadores bancarios u ordenadores de otros tipos que generen información (por ejemplo, información comercial) para su transmisión a móviles y para la recepción, en respuesta, de mensajes cortos procedentes de móviles, pero pueden ser de muchos otros tipos, tales como servidores de aplicaciones de diversos tipos.

La red 3 tiene un centro 26 de servicio de mensajes cortos (SMSC) asociado con ella. Las SME 20, 20A, 20B están conectadas al SMSC 26 mediante redes fijas 30 de un tipo adecuado. Cuando un móvil desea enviar un mensaje

corto, lo hará a través del SMSC 26 de su red 3. Así, por ejemplo, si el móvil 1 desea enviar un mensaje corto al móvil 11, el mensaje corto es direccionado automáticamente por el móvil 11 al SMSC 26, que luego entrega el mensaje corto al móvil 11 (tras registrar los detalles necesarios para permitir que se realice un cargo al móvil 1). Por lo tanto, cada mensaje corto lleva la dirección del SMSC local (esta dirección es generada automáticamente por el remitente), junto con la dirección del destinatario deseado del mensaje corto. Cuando el SMSC local recibe el mensaje corto, lee la dirección (el MSISDN o número ISDN de la estación móvil o el número de teléfono del destinatario deseado) y despacha el mensaje corto en consecuencia.

Los mensaje SMS pueden ser asegurados y autenticados según la disposición descrita en la publicación de solicitud de patente, en tramitación como la presente, nº GB-A-2415574.

En una realización básica, la invención permite una transferencia sencilla de valor entre clientes, habiéndose dotado a cada cliente de una cuenta virtual respectiva en la plataforma. Según la invención, las transacciones de cuentas se realizan por entero en una red de telecomunicaciones (por ejemplo, una red GSM). Un intercambio de mensajes de transacciones SMS provoca la transferencia de fondos entre una cuenta de cliente y otra cuenta de cliente, estando gestionada cada cuenta por el sistema gestor de cuentas, permitiendo con ello que se envíe dinero a casa o al país sin los riesgos de seguridad normalmente implicados en tales actividades. Además, los clientes únicamente requieren una tarjeta SIM para poder operar tales cuentas virtuales, estando insertada la tarjeta SIM en un terminal adecuado (generalmente, un terminal móvil) para conectarse con la red de telecomunicaciones.

La Figura 2 ilustra las interacciones entre “actores” en un sistema microfinancieras. Puede instalarse un sistema de gestión de cuentas virtuales según la presente invención en el centro de datos, de modo que los clientes y los operadores puedan acceder a las prestaciones ya sea a través de terminales móviles o mediante un enlace de red (ya sea una línea alquilada o Internet).

La cuenta virtual de cada cliente tiene una bandeja de entrada asociada de la SIM dentro de la cual se almacenan preferentemente las transacciones recientes, representando por ello el saldo actual de la cuenta virtual.

Se hace provisión para la administración del entorno de red conmutada, para el soporte de clientes y para el mantenimiento de los datos almacenados en el centro de datos. Cuando es necesario, se establece una red privada virtual (VPN) usando un concentrador VPN (por ejemplo, el Cisco 3000). El concentrador VPN permite la creación de un túnel VPN para el desarrollo y la administración de los datos almacenados remotamente en el centro de datos. en particular, la provisión de una VPN facilita el acceso por parte de socios/clientes organizativos individuales (por ejemplo, instituciones microfinancieras (MFI), concesiones de tiempo de comunicación que actúan como agentes) a sus cuentas centrales usando una conexión de Internet.

Como alternativa a la dirección de mensajes de transacciones SMS a un SMSC acoplado a la red cableada, los mensajes de transacciones SMS también pueden dirigirse a un centro de SMSC, que encamina los mensajes SMS como paquetes a través de Internet (como, por ejemplo, correo electrónico con el protocolo SNMP, protocolo simple de correo).

Además de la provisión de una interfaz de terminal basada en SMS, o como alternativa de la misma, el sistema de gestión de cuentas virtuales puede ser objeto de acceso, opcionalmente, por medio de uno o más canales dentro de una gama de canales complementarios, que incluyen la red mundial, GPRS, datos no estructurados de servicio suplementario (USSD) y voz.

Además de la transferencia de valor entre cuentas virtuales, los mensajes de transacciones SMS se usan para reintegros e imposiciones de efectivo en un proceso facilitado por la provisión de una cuenta de agente. Los agentes autorizados del sistema de gestión de cuentas, como los revendedores de crédito telefónico (o los dueños de tiendas), están dotados de elementos adicionales de menú para permitirles verificar el reintegro y/o la imposición de efectivo físico con el agente.

Alternativamente, o además, el cliente puede comprar mercancía directamente sin el uso de efectivo físico transfiriendo fondos a una cuenta del comerciante. De nuevo, la cuenta del comerciante es una cuenta del sistema de gestión de cuentas virtuales proporcionada a los comerciantes para permitir la venta de bienes y servicios a cambio de una transferencia de fondos desde una cuenta de cliente al comerciante.

Puede ilustrarse una transacción típica con referencia a los elementos de la Figura 3. Un usuario de teléfono móvil inicia la transacción navegando por los menús mostrados en la pantalla de su teléfono móvil 302 hasta una aplicación de transacción de fondos en la tarjeta SIM (instalada en el teléfono 302). Asimismo, otros usuarios también realizan transacciones en el sistema usando sus teléfonos móviles 304, 306. El usuario escoge entonces la transacción apropiada de un menú de la aplicación de transacciones de fondos e introduce la información solicitada, tal como una cuenta destinataria, el importe, el PIN, etc. La información se empaqueta en un mensaje cifrado y luego es enviada por SMS a un procesador 340 de transacciones. Para llegar al procesador 340 de transacciones, el mensaje cifrado debe pasar, en primer lugar, a través del centro 310 del servicio de mensajes cortos —SMSC— del operador y un módulo 330 de servicio de SMS. La conexión desde los teléfonos móviles al SMSC se realiza mediante la red móvil.

Las líneas gruesas de la Fig. 3 representan colas de mensajes (MQ). Las MQ pueden actuar entre ordenadores y permiten que las dos entidades de cada extremo funcionen de manera independiente. Una entidad envía un mensaje, sin aguardar una respuesta, y la otra lo recibe y lo procesa en un momento posterior. Por ejemplo, el módulo 330 de servicio de SMS puede seguir recibiendo mensajes SMS y retransmitirlos a una cola mientras el procesador 340 de transacciones esté desconectado temporalmente para su mantenimiento.

El procesador 340 de transacciones responde a eventos como la llegada de un mensaje entrante o una notificación de entrega, la notificación de la aceptación del SMSC de un mensaje saliente, la expiración de un temporizador o una solicitud externa. Determina la respuesta correcta al evento y la lleva a cabo.

Según ilustra la Figura 3, el procesador 340 de transacciones puede conectarse simultáneamente con más de un SMSC 310, 320. Esto permite diferencias en la funcionalidad de diferentes SMSC. La arquitectura también permite múltiples servicios SMS 330, potencialmente dispersos en una pluralidad de ordenadores anfitriones 300, estando conectado cada servicio SMS 330 con uno más SMSC. También permite múltiples procesadores 340 de transacciones de cara a un cambio de escala.

El procesador 340 de transacciones es responsable de la aceptación de solicitudes entrantes de diferentes tipos y de encargarse de ellas hasta su finalización. Cada solicitud entrante inicia una nueva transacción. Antes de completarse, la nueva transacción puede implicar una o más etapas en un periodo de tiempo (en algunos casos, de hasta 45 minutos). Considérese, por ejemplo, a un cliente que inicie una transacción de Envío de Dinero. Cuando el procesador 340 de transacciones recibe el mensaje de solicitud, el procesador verifica el mensaje, consulta la base de datos 350 principal y, si tiene éxito, envía una respuesta al teléfono móvil 302 del cliente, confirmando que la transacción ha tenido lugar. Unos segundos o minutos después, el procesador 340 de transacciones recibe confirmación de la entrega de la respuesta, confirma la transacción a la base de datos 350 de transacciones y envía una notificación al destinatario.

A menudo, se agrupan múltiples eventos en una sola transacción. Por ejemplo, cuando se activa por vez primera un SIM capaz de realizar transacciones de fondos, se envía un mensaje SMS desde el SIM al procesador 340 de transacciones. El procesador 340 de transacciones descifra y decodifica el mensaje entrante para descubrir que es una solicitud de activación y que incluye el PIN correcto para ese número de teléfono.

Pasa la solicitud a la base de datos 360 de contabilidad y, si autoriza la activación, devuelve un menú inicial en varios mensajes SMS, a través del SMSC 310 y del módulo 330 de servicio de SMS. Esto se entrega como un SMS binario a la propia aplicación del SIM. Cuando llegan acuses de recibo de la entrega con éxito para todos los mensajes SMS, el procesador 340 de transacciones envía un mensaje ulterior SMS de texto al teléfono 302 que contiene el SIM ahora activado diciendo al usuario que la activación tuvo éxito. Todos estos eventos —el mensaje inicial, la notificación procedente del SMSC 310 de la aceptación de los mensajes del menú inicial y cada una de las notificaciones de entrega— son agrupados por el procesador 340 de transacciones como una única transacción de nivel de aplicación.

En una implementación preferente, el procesador 340 de transacciones hace amplio uso de la Biblioteca Empresarial de Microsoft [RTM], siendo las transacciones transacciones de nivel MS-DTC y comunicándose los eventos entrantes por medio de mensajes MSMQ. En este caso, se dispone el procesador 340 de transacciones para garantizar que todo —desde la lectura de un mensaje de una cola, el resultante procesamiento de la base de datos y cualquier mensaje enviado— está cubierto por una única transacción MS-DTC respectiva. Por lo tanto, en el supuesto caso de que ocurriese cualquier error durante el procesamiento, todo el trabajo se deshace mediante una única marcha atrás y puede ser reiniciado: en consecuencia, esta implementación es capaz de hacer frente a bloqueos de la base de datos.

El procesador 340 de transacciones está adaptado, preferentemente, para anidar transacciones, usando una transacción exterior para obtener el evento siguiente y una transacción interior para procesarlo. Preferentemente, si la transacción interior falla, se permite que la exterior prosiga, basándose en que hacer que falle meramente hace que el evento vuelva a ser leído y que ocurra el mismo error. Solo si la transacción interior da como resultado un error persistente tras varios reintentos falla la exterior. Hay un mecanismo para limitar el número de tales reintentos.

El componente 380 de seguridad de los mensajes es responsable del cifrado y el descifrado de los mensajes enviados entre la aplicación del SIM (no mostrado, residente en el teléfono móvil 302 del usuario) y el procesador 340 de transacciones. Como parte de la decodificación, se verifican los PIN (y las contraseñas) y los nuevos PIN se cifran de tal forma que los PIN no cifrados y las claves no quedan expuestos fuera del componente 380 de seguridad de los mensajes. Cada SIM usa una clave diferente para cifrar y descifrar mensajes. La verificación de que se usó la clave apropiada se toma como prueba de que un mensaje se originó en un teléfono móvil 302 particular.

Preferentemente, los mensajes son entregados a la aplicación del SIM del teléfono móvil del usuario como programas de mensajes (binarios). Esto proporciona un canal bidireccional de comunicaciones totalmente seguro, robusto contra amenazas a la seguridad, como la “suplantación” de servidores de gestión de cuentas. Sin embargo, en algunos casos, se impide que las aplicaciones de la tarjeta SIM reciban tales mensajes SMS mientras se

muestran menús en la pantalla del teléfono móvil 302. En tales casos, el sistema puede ser configurado de tal modo que los mensajes enviados desde el servidor se envíen a los SIM como mensajes de texto legible.

En una realización, el componente 380 de seguridad de los mensajes es un componente COM+ que se ejecuta como una aplicación servidora COM+ dedicada. Además de descifrar y decodificar mensajes recibidos de la aplicación SIM y de cifrar mensajes que han de enviarse a la aplicación SIM, el componente 380 proporciona procedimientos para obtener información de la fecha y la generación asociada con un PIN cifrado; obtener información de la fecha y la generación asociada con un elemento cifrado; cifrar claves maestras; generar una clave específica al SIM según un algoritmo predefinido de clave maestra; cifrar contraseñas; y verificar contraseñas con contraseñas cifradas.

El componente 380 usa la seguridad del papel COM+ para limitar procedimientos particulares de interfaz a usuarios particulares. Por ejemplo, solo el operador del servicio puede descifrar y cifrar mensajes para la aplicación de transacciones SIM, pero el usuario 370 de la cuenta web puede crear números PIN.

El esquema particular de cifrado adoptado se selecciona según las prestaciones de los SIM usados. Sin embargo, resulta preferible que todos los SIM compartan una única clave pública (con la condición de que los SIM soporten el cifrado con clave pública). Cuando esto no resulta posible, puede generarse, en su lugar una clave específica al SIM a partir de una única clave simétrica compartida y de información de ID única al SIM. En este caso, la fiabilidad de la seguridad depende del secreto de la clave simétrica compartida.

Como ejemplo de la flexibilidad inherente de la solución de la gestión de cuentas, el sistema de la invención ha sido configurado para soportar la operación de una institución microfinanciera, MFI. La Figura 4 ilustra las etapas de la operación de esta realización de la invención. La MFI mantiene una cuenta virtual central en el centro de datos. además, se proporcionan cuentas virtuales para diferentes papeles dentro de un esquema microfinanciero: directores de sucursal, que distribuyen pequeños préstamos dentro de las comunidades; clientes, titulares de cuentas virtuales que reciben préstamos de la MFI; y tesoreros de grupo, cuyo trabajo es verificar que los préstamos se están devolviendo correctamente.

Cuando la MFI autoriza la liberación de fondos para su distribución como préstamos por parte de un director de sucursal, se envía un mensaje adecuado de transacción SMS. El mensaje de transacción SMS efectúa la transferencia de fondos a la cuenta del director de sucursal. A su vez, el director de sucursal distribuye préstamos dentro de un grupo de cuentas de clientes. Las cuentas de clientes reciben el abono de la suma autorizada, usando de nuevo un mensaje de transacción SMS.

Los clientes de una MFI particular aceptan devolver su préstamo transfiriendo fondos con una frecuencia predeterminada a la cuenta del tesorero de grupo. Esta actividad también es efectuada mediante el intercambio de mensajes SMS seguros. Finalmente, una vez que está satisfecho de que se han realizado las debidas devoluciones, el tesorero de grupo transfiere la suma apropiada, devolviéndola a la cuenta central de la MFI.

El sistema de la invención proporciona una comunicación bidireccional segura con el SIM a través de mensajes de transacciones SIM. Se proporciona una clave única para cada SIM. Por lo tanto, el sistema proporciona una transparencia completa en términos de qué SIM inicia qué transacción, facilitando la auditoría y otras funciones reguladoras.

La interfaz que opera en cada terminal habilitado incluye un “intérprete”. El intérprete es una aplicación similar a un navegador. En las realizaciones que preceden, cada mensaje de transacción SMS que solicita una transacción de gestión de cuentas se construye mediante el uso de un menú de diálogo presentado por el intérprete en el que se pide al cliente que indique: la cuenta destinataria, el valor que ha de transferirse (o reintegrarse), la fecha de la transferencia, y que introduzca datos de seguridad para la autenticación. El intérprete es plenamente personalizable por vía aérea. Los menús, incluso el idioma presentado, pueden cambiar de forma remota. Cada acción de los elementos del menú es efectuada por un respectivo miniprograma (por ejemplo, Javascript ejecutándose en el navegador o como una miniaplicación). Además, la interfaz es sensible a eventos controlados por el servidor.

El sistema contempla los diferentes requisitos de los usuarios del sistema. Dependiendo del papel del usuario (por ejemplo, usuario, agente, tesorero, director de sucursal), el sistema puede ser personalizado con menús y opciones apropiados. Tales actualizaciones son efectuadas convenientemente mediante actualizaciones por vía aérea.

Una vez generado y enviado, el mensaje de texto es recibido en un primer centro de servicio de mensajes cortos (SMSC), el SMSC se acopla al entorno de la red conmutada por medio de una pasarela SMSC. A continuación, el servicio SMS transfiere el mensaje de transacción SMS a través del entorno de la red conmutada a un procesador de transacciones que interpreta el mensaje de transacción SMS y, una vez que el SMS ha sido autenticado, altera en consecuencia los datos que representan cada cuenta afectada por el mensaje de transacción SMS, almacenándose los datos en un centro de datos.

Usando el intérprete (con esta característica opcional habilitada), se presenta al usuario una bandeja de entrada de la cuenta, separada de la bandeja de entrada convencional de SMS, mediante la cual puede mantener un historial

de transacciones. La bandeja de entrada de la cuenta solo es accesible a través de la funcionalidad de autenticación del SIM insertado en el terminal, de modo que la autenticación del SIM garantiza la integridad del historial de transacciones.

Para confirmar la terminación de una transacción dada, se genera entonces un correspondiente mensaje de transacción completa para cada cuenta afectada por la transacción y, acto seguido, el mensaje de transacción completa se encapsula en un mensaje cifrado que solo puede ser abierto correctamente por un terminal móvil que tenga una tarjeta SIM con la clave correcta de descifrado. De hecho, el mensaje de transacción completa está firmado electrónicamente con una clave específica al SIM. Los mensajes cifrados tienen el formato de mensajes SMS y se distribuyen por medio del servicio SMS al solicitante de la transacción y al titular de la cuenta afectada. Estos mensajes SMS se entregan en las bandejas de entrada de cuenta de las respectivas cuentas, de modo que solo el usuario verificado del SIM pueda ver el estado de las transacciones.

En el caso en que más de un usuario tiene acceso al terminal y se comparte un único SIM, puede hacer falta información de ID y de seguridad adicional. El acceso proporcionado está entonces limitado a una correspondiente bandeja de entrada de la cuenta, inaccesible a otros usuarios, pero almacenada en el SIM pese a todo.

Preferentemente, los centros de servicio de mensajes cortos (SMSC) en los que opera el gestor de cuentas son personalizables, en particular en términos de la duración del retardo en el envío de cualquier SMS. El servicio es expandible (soportando múltiples SMSC) y susceptible de cambio de escala (almacenando diferentes números de teléfono en el mismo SMSC, permitiendo con ello más de una institución microfinanciera).

Preferentemente, el servicio también se implementa de forma que sea agnóstico con respecto a la infraestructura de red que transporta los mensajes de transacciones. Una presentación significativa para la implementación es la capacidad de albergar los servidores de forma remota.

En algunas implementaciones, las restricciones de cortafuegos limitan el número de ubicaciones de red en las que puede obtenerse un acceso simultáneo a más de un SMSC. Esta limitación puede abordarse implementando una aplicación de servicio, un remitente de mensajes (véase la Fig. 5), para remitir los mensajes MQ desde una cola de mensajes de un ordenador a la cola de mensajes de otro ordenador usando protocolos que estén adaptados para atravesar tales cortafuegos. Dado que la comunicación entre el procesador 340 de transacciones y los SMSC 310, 320 comienza con mensajes MQ, este servicio permite que el sistema esté situado en otro lugar. Considérese la situación cuando una primera red de datos solo permite las conexiones salientes. Para que el procesador de transacciones pueda estar albergado fuera de la primera red de datos (pero que siga teniendo acceso al SMSC de esa primera red de datos), el remitente de mensajes debe ser capaz de enviar y recibir mensajes MQ a través del cortafuegos que impide las conexiones entrantes.

El remitente de mensajes consiste en dos partes: un servicio web y un cliente implementado como, por ejemplo, un servicio de Windows NT. El cliente se ejecuta en el ordenador dentro del cortafuegos (ordenador A) e inicia todas las llamadas al servicio web que se ejecuta en el ordenador B. Dado que las llamadas al servicio web utilizan HTTP, esto se permite. La Figura 5 muestra cómo se interconectan las partes.

Convenientemente, el sistema es capaz de imponer normas de encaminamiento basadas en los costes, garantizando que los mensajes de transacciones SMS se encaminen según criterios predeterminados, tales como coste económico mínimo, distancia mínima y servicio más rápido. En realizaciones preferentes, el sistema impone normas que se actualizan de forma dinámica, garantizando con ello que el operador pueda proporcionar el servicio al menor coste. A menudo, se usará un proveedor local de servicios móviles para los mensajes SMS entrantes. Fundamentalmente, esto permite la provisión de servicios SMS que están libres de coste para el usuario. Esto también mantiene bajos los costes del tráfico SMS.

Está claro que cuando el precio del tráfico SMS es menos importante, hay poca restricción sobre la ubicación geográfica: la plataforma podría ser implementada para ejecutarse desde cualquier lugar del mundo. Puede proporcionarse un acceso de itinerancia a tales servicios cuando los costes no sean prohibitivos.

Para aplicaciones internacionales, la base de datos y la lógica del gestor de cuentas virtuales están dotados, preferentemente, de aplicaciones de ampliación para que se encarguen de las conversiones de divisas y de diferencias de idioma y reguladoras (por ejemplo, medidas antifraude).

La arquitectura del sistema significa que las transacciones de uno a muchos son de implementación relativamente simple: así, por ejemplo, puede usarse una sola transacción de agente para recargar tres cuentas virtuales separadas.

Se prefiere que el procesador de transacciones esté dotado de una prestación multiplexora de SMS que determine cuál de varios SMSC posibles debería ser usado para entregar cualquier mensaje SMS dado.

Además de la prestación de encargarse de la solicitud de transacciones procedente de los SIM de usuario y del acceso a la red, el gestor de transacciones también tiene, convenientemente, una prestación de encargarse de

solicitudes de tiempo de comunicación procedentes de los clientes de prepago (ya sea para el propio usuario o en nombre de otro usuario y/o teléfono). Tales solicitudes podrían originarse en el menú de la aplicación de transacciones o del acceso a una página electrónica adecuada.

En una mejora adicional de la invención, el sistema puede solicitar o deducir la ubicación física del usuario. con esta información de ubicación (por ejemplo, la ID de la célula), el sistema puede garantizar que la información proporcionada al usuario sea relevante para el contexto físico de ese usuario. Esto permite que los terminales se usen como un instrumento intracomunitario que anuncie recursos disponibles localmente, etc.

REIVINDICACIONES

1. Un sistema de gestión de cuentas habilitado por teléfono móvil para mantener una pluralidad de cuentas virtuales en un sistema de comunicaciones celulares, incluyendo el sistema de comunicaciones celulares para transportar mensajes entre terminales móviles (302, 304, 306) e incluyendo cada terminal móvil una tarjeta de datos con un identificador único, incluyendo el sistema de gestión de cuentas:

un medio (330) de mensajería que está adaptado para recibir mensajes de transacciones entrantes procedentes de terminales móviles que usan el sistema de comunicaciones, incluyendo los mensajes entrantes el identificador único del terminal móvil de origen, y para transmitir mensajes de transacciones salientes a los terminales móviles en respuesta;
un procesador (340) de transacciones que está acoplado al medio de mensajería mediante un par de colas (332, 334) de mensajes y adaptado para interpretar los mensajes de transacciones entrantes y para producir correspondientes instrucciones de transacciones;
un medio (380) de seguridad de mensajes, acoplado al procesador (340) de transacciones, que autentica los mensajes de transacciones entrantes comparando el identificador único incluido con las entradas de una lista de cuentas virtuales válidas; y
una interfaz de almacenamiento de datos de transacciones, acoplada al procesador (340) de transacciones, a través de la cual el procesador de transacciones se comunica con un almacén (350) de datos, estando adaptada la interfaz para transportar instrucciones para modificar datos contenidos en una o más cuentas virtuales válidas almacenadas en el almacén de datos y para transportar mensajes de transacción completa desde el almacén de datos al procesador (340) de transacciones cuando se completa la modificación;
en el que las colas (332, 334) de mensajes incluyen una cola de recepción y una cola de envío, estando adaptada la cola de recepción para poner en cola de espera los mensajes recibidos del procesador (340) de transacciones y estando adaptada la cola de envío para enviar a la cola de espera los mensajes enviados al procesador (340) de transacciones;
en el que el procesador (340) de transacciones también está adaptado para interpretar mensajes de transacción completa y para dar salida a correspondientes mensajes interpretados de transacción completa hacia el medio (330) de mensajería mediante la cola de recepción;
en el que cada mensaje interpretado de transacción completa incluye información de seguridad generada a partir de identificadores únicos de cuentas virtuales modificadas, estando adaptado el medio de mensajería para dirigir los mensajes salientes generados a partir de los mensajes interpretados de transacción completa hacia correspondientes terminales móviles; y
en el que cada mensaje saliente recibido está en un formato que requiere la introducción de una clave única desde la tarjeta de datos insertada en el terminal móvil, garantizándose con ello que el mensaje saliente solo pueda ser leído en presencia de una tarjeta de datos con una clave única que coincida con la información de seguridad del mensaje saliente.

2. Un sistema según se reivindica en la reivindicación 1 en el que el medio de procesamiento de transacciones incluye, además, un componente de documentación para proporcionar una funcionalidad de documentación, de modo que pueda hacerse un seguimiento del movimiento de valor entre las cuentas virtuales.

3. Un sistema según se reivindica en las reivindicaciones 1 o 2 en el que el medio de procesamiento de transacciones proporciona una pluralidad de cuentas virtuales, representando cada cuenta uno de varios roles distintos dentro de un esquema microfinanciero.

4. Un sistema según se reivindica en una cualquiera de las reivindicaciones 1 a 3 en el que el medio de procesamiento de transacciones tiene funcionalidad adicional y en el se protege adicionalmente el acceso remoto a la funcionalidad adicional al requerir el establecimiento de una red privada virtual.

5. Un sistema según se reivindica en una cualquiera de las reivindicaciones 1 a 4 en el que el medio de mensajería está adaptado para recibir mensajes de transacciones entrantes directamente de un componente SMSC del sistema de comunicaciones.

6. Un sistema según se reivindica en una cualquiera de las reivindicaciones 1 a 4 en el que el medio de mensajería está adaptado para recibir mensajes de transacciones entrantes procedentes de una entidad de mensajes cortos, que está adaptada para interceptar mensajes de transacciones entrantes desde el sistema de comunicaciones celulares y para distribuir los mensajes de transacciones entrantes en una interfaz de Internet.

7. Un sistema según se reivindica en cualquiera de las reivindicaciones 5 o 6 en el que la ruta tomada por cada mensaje de transacción entrante es determinado en función del coste según un conjunto predeterminado de criterios de coste.

8. Un sistema según se reivindica en la reivindicación 7 en el que los criterios se actualizan dinámicamente en respuesta a cambios en coste.

9. Un sistema microfinanciero que comprende:

el sistema de gestión de cuentas de una cualquiera de las reivindicaciones 1 a 8; y
un terminal móvil (302) dispuesto para habilitar el sistema de gestión de cuentas.

10. Un procedimiento habilitado por teléfono móvil para mantener una pluralidad de cuentas virtuales en un sistema de comunicaciones celulares, transportando el sistema de comunicaciones celulares mensajes entre terminales móviles e incluyendo cada terminal móvil una tarjeta de datos con un identificador único, comprendiendo el procedimiento:

recibir mensajes de transacciones entrantes procedentes de terminales móviles que usan el sistema de comunicaciones, incluyendo los mensajes entrantes el identificador único del terminal móvil de origen;
poner en cola de espera los mensajes entrantes;
interpretar los mensajes de transacciones entrantes;
autenticar los mensajes de transacciones entrantes comparando el identificador único incluido con las entradas de una lista de cuentas virtuales válidas;
cuando los mensajes de transacciones entrantes son auténticos, producir correspondientes instrucciones de transacciones para modificar datos contenidos en una o más cuentas virtuales válidas almacenadas en un almacén de datos;
recibir mensajes de transacción completa desde el almacén de datos cuando se completa la modificación;
poner en cola de espera los mensajes de transacción completa; y
transmitir los mensajes de transacciones salientes, puestos en cola espera, a los terminales móviles de origen, incluyendo cada mensaje interpretado de transacción completa información de seguridad generada a partir de identificadores únicos de cuentas virtuales modificadas;
en el que cada mensaje saliente recibido está en un formato que requiere la introducción de una clave única desde la tarjeta de datos insertada en el terminal móvil, garantizándose con ello que el mensaje saliente solo pueda ser leído en presencia de una tarjeta de datos con una clave única que coincida con la información de seguridad del mensaje saliente.

11. Un procedimiento para llevar a cabo una transacción en un sistema microfinanciero, comprendiendo el procedimiento:

el procedimiento de la reivindicación 10; y
un procedimiento para operar un terminal móvil (302) dispuesto para habilitar el procedimiento de la reivindicación 10, incluyendo el procedimiento para operar el terminal móvil (302):

proporcionar una aplicación intérprete personalizable;
usar la aplicación intérprete para componer menús para su visualización en el teléfono móvil (302);
aceptar información de transacciones introducida a través de los menús;
generar mensajes de transacciones entrantes según la información de transacciones introducida;
transmitir al sistema los mensajes de transacciones entrantes;
recibir del sistema mensajes de transacciones salientes; y
visualizar en el terminal móvil (302) confirmación de la terminación de la transacción.

12. El procedimiento de la reivindicación 11 en el que, en el procedimiento para operar un terminal móvil (302), la etapa de composición de un menú para su visualización incluye la etapa de recibir un mensaje de menú y adaptar el menú en respuesta al contenido del mensaje de menú, personalizándose con ello el menú para los diferentes requisitos de los usuarios del sistema.

13. El procedimiento de la reivindicación 12 en el que, en el procedimiento para operar un terminal móvil (302), el mensaje de menú se recibe como una actualización por vía aérea.

14. El procedimiento de las reivindicaciones 12 o 13 en el que el procedimiento para operar un terminal móvil (302) comprende, además, determinar la ubicación física del terminal y generar información en función de la ubicación, incluyendo el mensaje de menú información en función de la ubicación apropiada a la ubicación física del terminal.

15. El procedimiento de una cualquiera de las reivindicaciones 11 a 14 en el que, en el que el procedimiento para operar un terminal móvil (302), la etapa de aceptación de información de transacciones introducida incluye:

presentar al usuario un menú de diálogo;
pedir que el usuario introduzca información de transacciones; y
almacenar la información de transacciones introducida en un formato adecuado para su procesamiento en un mensaje de transacción.

16. El procedimiento de la reivindicación 15 en el que, en el que el procedimiento para operar un terminal móvil (302), la información de transacciones introducida incluye información que identifica uno o más de los parámetros siguientes: la cuenta seleccionada; el valor que ha de transferirse; la fecha de la transferencia; el valor que ha de reintegrarse; la fecha del reintegro; y los datos de seguridad para la autenticación.

17. El procedimiento de las reivindicaciones 11 a 16 en el que, en el que el procedimiento para operar un terminal móvil (302), la etapa de aceptación de información de transacciones introducida incluye una etapa preliminar de autenticación del intento de acceder a una bandeja de entrada de una cuenta dada por medio de la funcionalidad de autenticación de la tarjeta de datos insertada en el terminal móvil, con lo que se garantiza la integridad del historial de transacciones por medio de la autenticación del SIM.

18. El procedimiento de la reivindicación 17 en el que, en el que el procedimiento para operar un terminal móvil (302), la etapa de autenticación incluye: pedir que el usuario hable al micrófono del que está dotado el terminal; grabar una entrada de voz; y comparar la entrada de voz con una muestra verificada de la voz del usuario; y confirmar que la voz es la del usuario, autenticando con ello al usuario con el reconocimiento de voz.

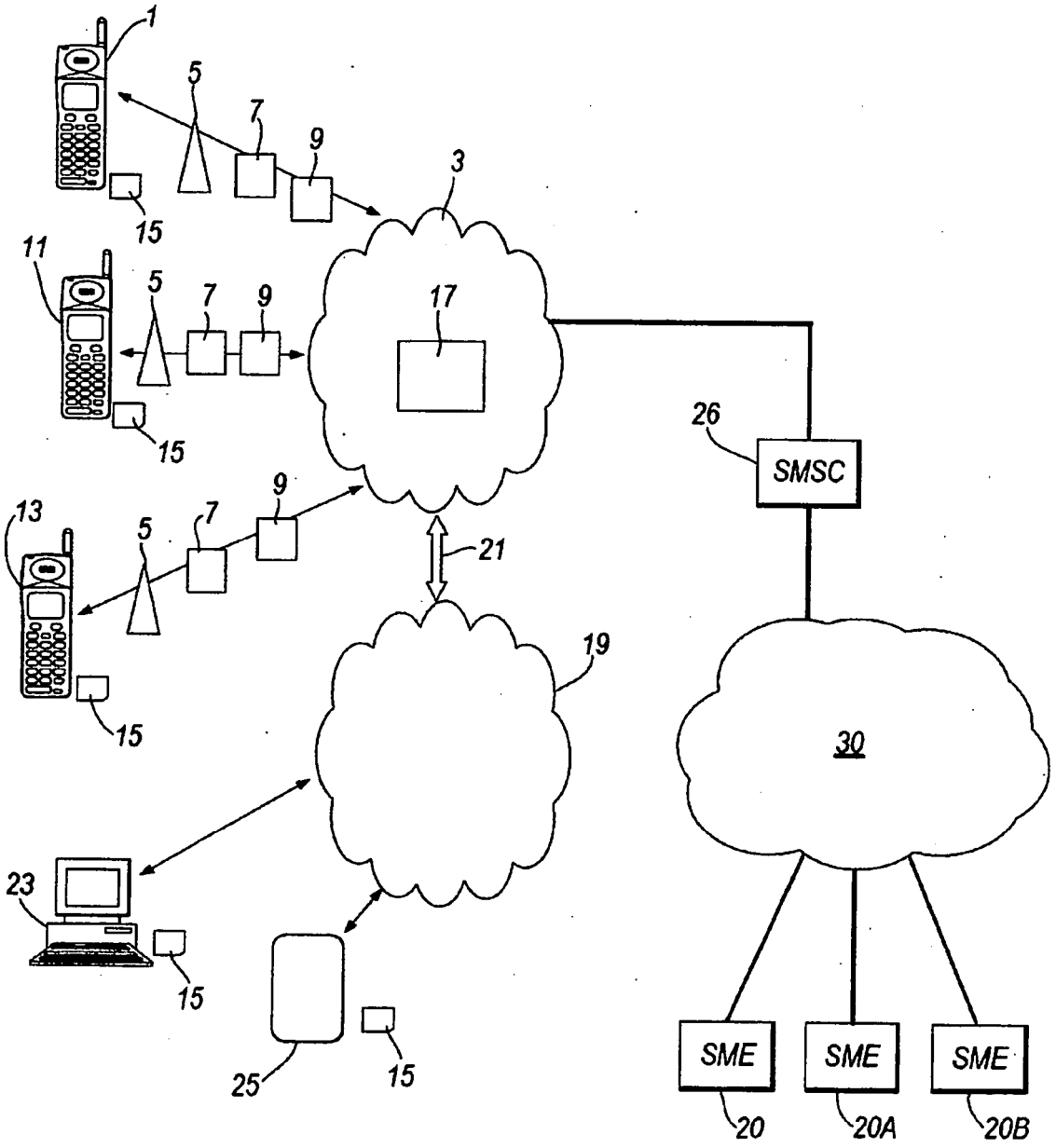
1
5
7
9
3
15
11
5
7
9
17
15
26
SMSC
13
5
7
9
21
19
15
30
23
15
25
15
SME
SME
SME
20
20A
20B

Figura 1

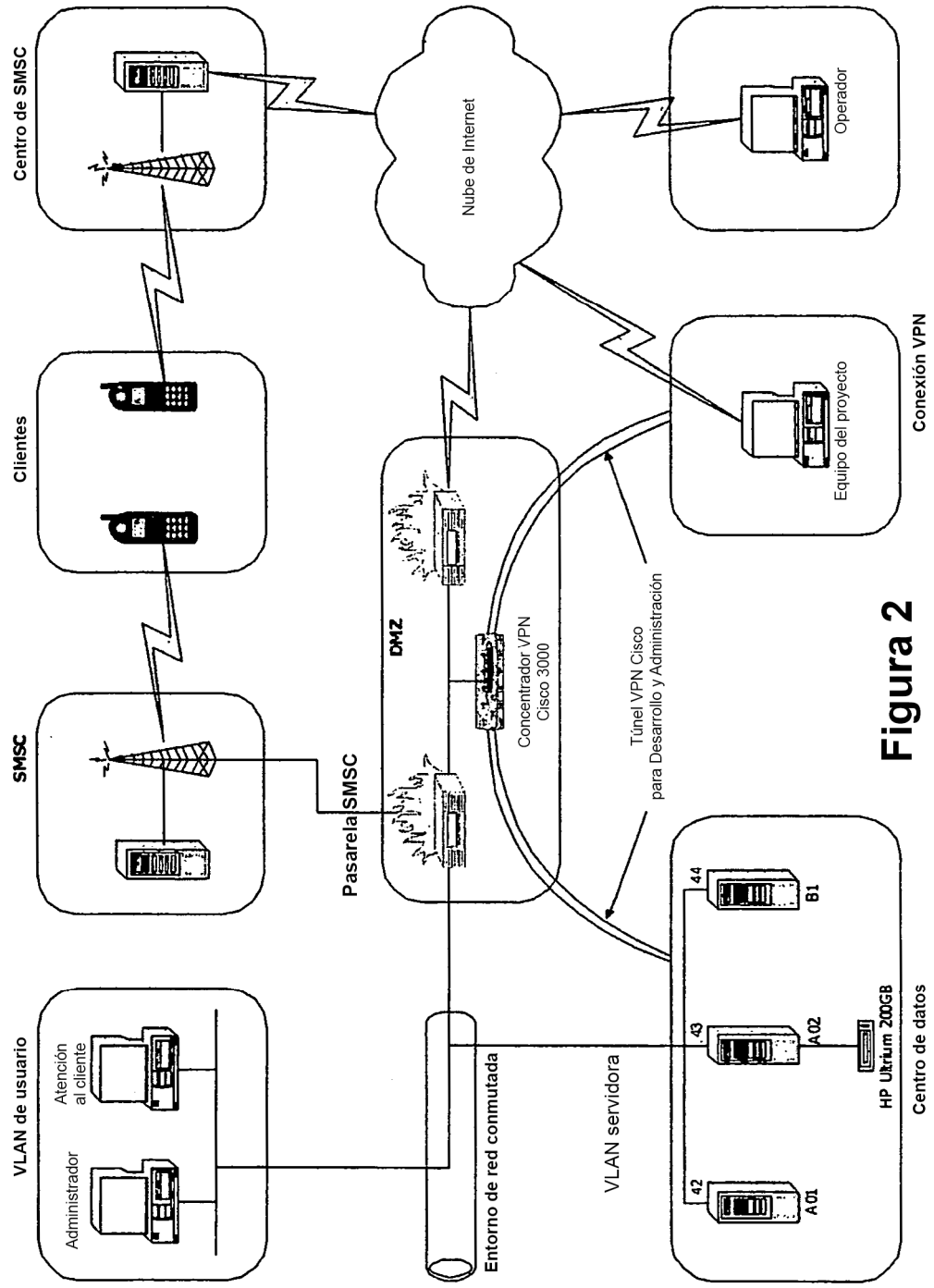
Centro de SMSC
Nube de Internet
Operador
Clientes
Equipo del proyecto
Conexión VPN
SMSC
DMZ
Concentrador VPN
Cisco 3000
Túnel VPN Cisco
para Desarrollo y Administración
Pasarela SMSC
VLAN de usuario
Atención
al cliente
Administrador
Entorno de red conmutada
VLAN servidora
44
B1
43
A02
HP Ultrium 200GB
42
A01
Centro de datos

Figura 2

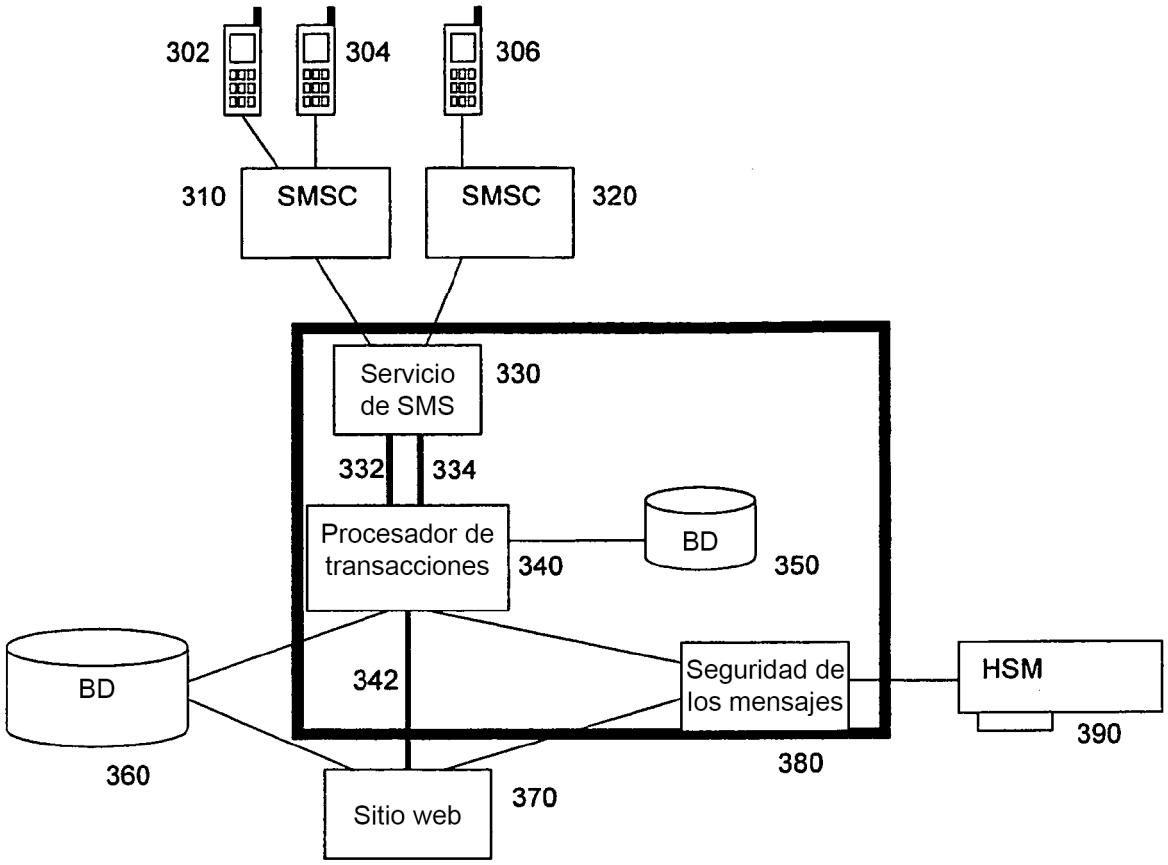
302
304
306
310
SMSC
SMSC
320
Servicio de SMS
330
332
334
Procesador de transacciones
340
BD
350
BD
360
342
Seguridad de los mensajes
380
HSM
390
Sitio web
370

Figura 3

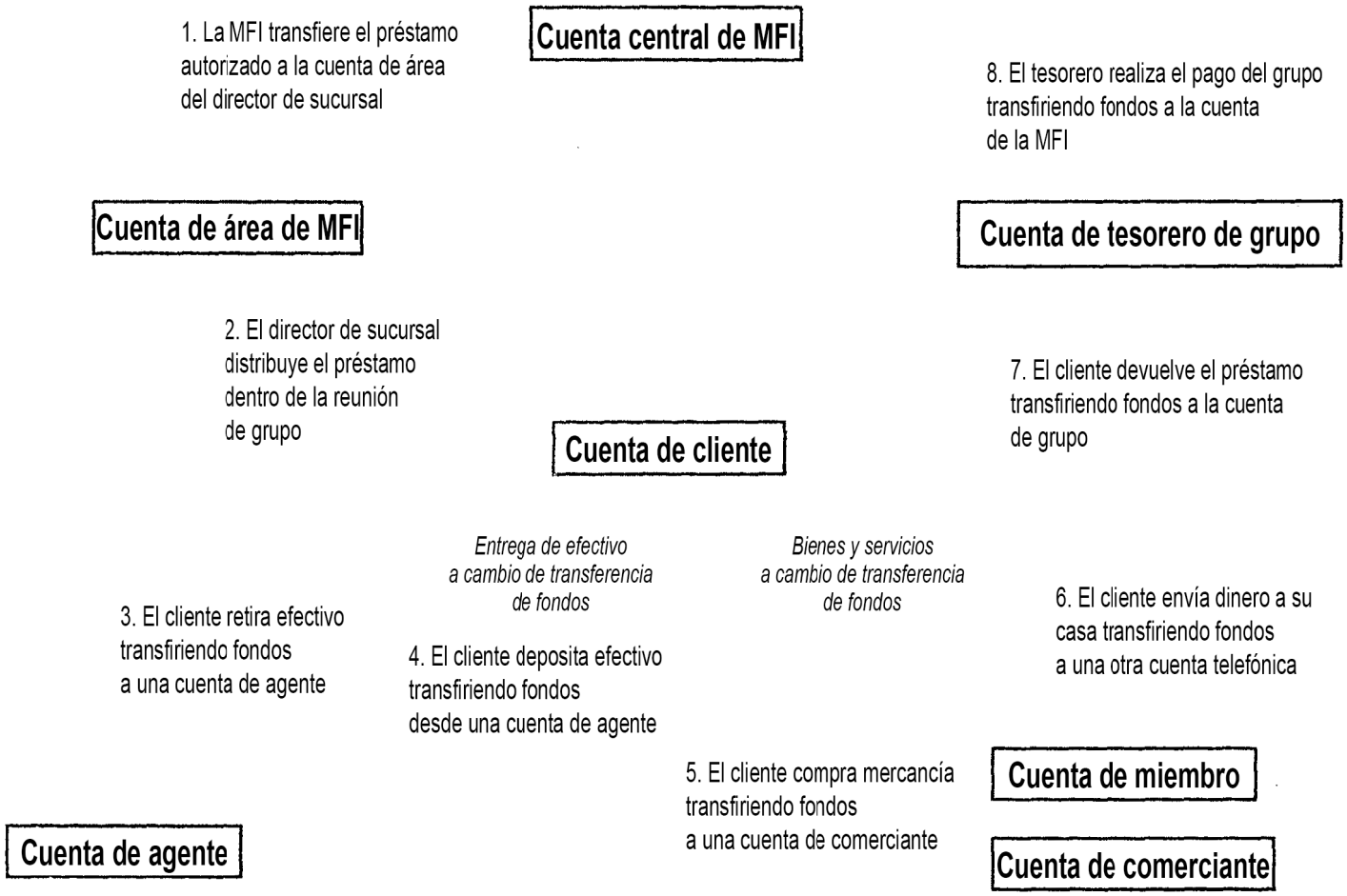
1. La MFI transfiere el préstamo autorizado a la cuenta de área del director de sucursal
Cuenta central de MFI
8. El tesorero realiza el pago del grupo transfiriendo fondos a la cuenta de la MFI
Cuenta de área de MFI
Cuenta de tesorero de grupo
2. El director de sucursal distribuye el préstamo dentro de la reunión de grupo
7. El cliente devuelve el préstamo transfiriendo fondos a la cuenta de grupo
Cuenta de cliente
Entrega de efectivo a cambio de transferencia de fondos
Bienes y servicios a cambio de transferencia de fondos
3. El cliente retira efectivo transfiriendo fondos a una cuenta de agente
4. El cliente deposita efectivo transfiriendo fondos desde una cuenta de agente
6. El cliente envía dinero a su casa transfiriendo fondos a una otra cuenta telefónica
5. El cliente compra mercancía transfiriendo fondos a una cuenta de comerciante
Cuenta de miembro
Cuenta de agente
Cuenta de comerciante

Figura 4

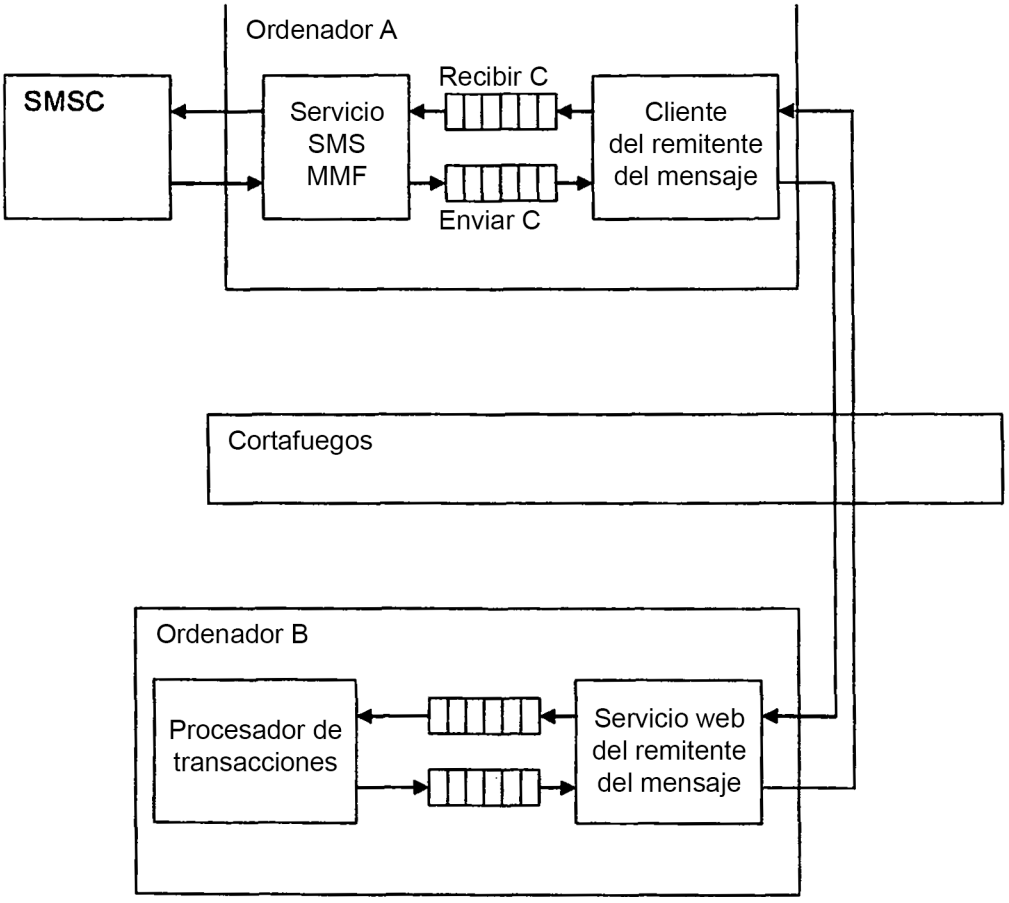
Ordenador A
SMSC
Servicio SMS MMF
Recibir C
Enviar C
Cliente del remitente del mensaje
Cortafuegos
Ordenador B
Procesador de transacciones
Servicio web del remitente del mensaje

Figura 5