(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 564 128**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.12.2012 E 12197621 (1)**

(97) Fecha y número de publicación de la concesión europea: **18.11.2015 EP 2608486**

(54) Título: **Un sistema implementado por ordenador para proporcionar a los usuarios acceso seguro a servidores de aplicaciones**

(30) Prioridad:

20.12.2011 IN MU35752011

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.03.2016

(73) Titular/es:

TATA CONSULTANCY SERVICES LTD. (100.0%)
Nirmal Building, 9th Floor Nariman Point
Mumbai 400 021, Maharashtra, IN

(72) Inventor/es:

BIDARE, PRASANNA

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Un sistema implementado por ordenador para proporcionar a los usuarios acceso seguro a servidores de aplicaciones

Campo de divulgación

La presente invención se refiere al campo de proporcionar a los usuarios acceso privado seguro a servidores de aplicaciones para transacciones.

Técnica anterior

P. Desblancs et al. divulgan en el artículo "Cordless Telephone System", Electrical Communication, Alcatel, Bruselas, BE, no. Quart. 4th, 1 de enero de 1998 (1998-01-01) en las páginas 286-291 ISSN: 0013-4252, un sistema que habilita que los usuarios hagan y reciban llamadas con sus teléfonos GSM por mediación de una red fija y mediante ello accedan al servicio de una segunda red como una red móvil. Por lo tanto, el sistema hace uso de un espectro de frecuencias seleccionado de una sub-banda de un espectro GSM de la operadora para facilitar las comunicaciones. Puesto que se deben usar las frecuencias GSM ya atribuidas a la operadora, no es posible atribuir una banda de frecuencias dedicada.

Antecedentes

Transacciones tales como la transferencia electrónica de fondos, la banca en línea, la e-adquisición de bienes y servicios y las transacciones que dan acceso a datos sensibles a través de cuentas privilegiadas son consideradas de naturaleza sensible. Tales transacciones se consideran sensibles porque constituyen la utilización de datos sensibles, tales como el número de cuenta, el número de identificación personal (PIN) en el caso de la transferencia electrónica de fondos y el nombre de usuario y la contraseña confidencial en caso de acceso electrónico de datos. Del mismo modo, los proveedores de servicios que proporcionan la implementación de la transacción mencionada anteriormente y gestionan la transacción a través de al menos sus servidores de aplicaciones se denominan proveedores de servicios sensibles.

Las instituciones bancarias y financieras (las BFI) son uno de los ejemplos de proveedores de servicios sensibles. Las BFI proporcionan a los usuarios varios servicios financieros, incluyendo la transferencia de dinero, la banca en línea, el comercio electrónico y similares. Por lo general, las transacciones realizadas por los usuarios con los servidores de aplicaciones asociados con las BFI implican el intercambio de información sensible de usuario relacionada incluyendo pero no limitada a número de cuenta bancaria, contraseña y número de identificación personal del usuario. En el escenario de hoy, es muy común que un usuario particular tenga varias cuentas de banca en línea y, con el fin de facilitar el recuerdo, los usuarios tienden a asociar todas sus cuentas de banca en línea con una única combinación de credenciales de autenticación que normalmente implican un nombre de usuario y una contraseña. Sin embargo, es de entender que las credenciales de autenticación pueden ser asociadas con otras diversas cuentas de usuario tales como cuentas de administrador del sistema, cuentas de gestión de base de datos y similares.

Puesto que un único conjunto de credenciales se asocian con varias cuentas en línea, hay una posibilidad de que las credenciales se utilicen muchas veces para obtener servicios de varios proveedores de servicios sensibles. Por otra parte, en el escenario de hoy, los usuarios tienden a hacer uso de múltiples aparatos de comunicación tales como teléfonos móviles, equipo físico específico para una aplicación, ordenadores portátiles y ordenadores de sobremesa para acceder a servidores de aplicaciones asociados con proveedores de servicios sensibles. En tales casos, debido a la multiplicidad asociada con las credenciales y debido al hecho de que las credenciales han sido utilizadas a través de múltiples aparatos, hay una posibilidad de que el secreto asociado con las credenciales pueda verse comprometido y, además, que las credenciales se puedan ver sometidas a piratas informáticos / suplantación de identidad / suplantación de procedencia y ataques de envenenamiento de DNS/navegador.

Hasta ahora las BFI han estado utilizando varios métodos para asegurar completamente sus redes privadas de extremo trasero. Las redes privadas de extremo trasero que se utilizan para interbancario, intrabancario, transacciones de punto de venta y transacciones basadas en banda magnética han sido operadas en hardware y software específicos que ofrecen gran seguridad a las transacciones mencionadas.

Sin embargo, no existe tal red privada de extremo delantero, segura, para clientes de BFI (usuarios) que por lo general utilicen redes públicas de línea de cable / inalámbricas para iniciar sesión en los servidores de BFI. A pesar de los mejores esfuerzos los sindicatos de BFI encuentran difícil hacer cumplir medidas de seguridad estrictas y correctas para los clientes que inician sesión en los servidores de BFI. Ya que los clientes hacen uso de múltiples dispositivos para conectarse a los servidores de BFI, es difícil ofrecer a los clientes conectividad privada segura.

Por lo tanto, se siente la necesidad de un sistema que proporciona una red privada segura de extremo delantero para los clientes de BFI (usuarios). El sistema debe coexistir con internet, pero sólo debe proporcionar un acceso

privado a aquellos clientes que necesitan iniciar sesión en los servidores de BFI. El sistema debe agregar a dichos usuarios justo en el punto de conmutación de red y proporcionarles un ancho de banda seguro privado para acceder al servidor de BFI solicitado, aunque después de una identificación personal. La red privada de extremo delantero debe también ser capaz de ofrecer resistencia a la suplantación de identidad, el envenenamiento de DNS, ataques de hombre medio, el envenenamiento de navegador y similares que afectan a la red de BFI existente en mayor medida.

Algunos de los sistemas de la técnica anterior que ofrecen acceso de sesión único e identidad personal única incluyen ”Intercambio Abierto de Identidad", que se concentra en la socialización de las identidades de los usuarios, las soluciones Eco albergadas por RSA/Symantec para sus socios empresariales en plataformas SSL, y otros ciertos programas como la tarjeta de identificación global y el esquema de identificación biométrica ADHAR (Iniciativa del Gobierno de la India). Sin embargo, ninguno de estos sistemas proporciona un enlace de comunicación seguro privado para los usuarios en Internet para acceder a los servidores de BFI.

Algunos de los tipos de ataques de suplantación de procedencia / ataques de piratas informáticos se explican a continuación:

• Ataque de intermediario: El ataque de intermediario es una forma de espionaje. Aquí el atacante hace que las víctimas (dos partes implicadas en la comunicación) crean que están hablando directamente entre sí a través de una conexión privada, aunque toda la conversación habría sido espiada por el atacante.

• Ataque de intruso en navegador: El ataque de intruso en el navegador implica la creación de un troyano que infecta un navegador web. De una manera invisible para el usuario y la aplicación de hospedador, este software malicioso modifica las páginas web, los contenidos de transacción y/o inserta contenidos de transacción adicionales. Este tipo de ataque puede tener éxito con independencia de que mecanismos de seguridad tales como PKI (infraestructura de clave pública) y/o soluciones de autenticación de dos o tres factores estén en su lugar.

• Ataques de suplantación de identidad: Los correos electrónicos de suplantación de identidad suelen incluir un enlace a un sitio web que pide información personal o financiera con la intención de robar información personal/financiera como contraseñas bancarias, los PIN de tarjetas de crédito y similares.

• Ataque de redireccionamiento: El ataque de de redireccionamiento se logra cambiando parte de la información relacionada con la dirección web que el ISP almacena para aumentar la velocidad de navegación web. Un virus altera el comportamiento de los navegadores de Internet al redirigir al usuario a un sitio ficticio cuando intentan iniciar sesión en sitios web.

• Ataques de caballo de Troya: Los ataques de caballo de Troya infectan un ordenador a través de sitios web o a través de correos electrónicos. Un troyano es un programa que puede grabar las pulsaciones de teclado y enviar información de vuelta a su base.

• Secuestro de sistema de nombres de dominio (DNS): El secuestro de DNS se realiza mediante la explotación del software de servidor DNS o cambiando el archivo de hospedador residente en un ordenador determinado. El pirata informático redirige el tráfico de datos destinado a ese ordenador en particular, a otro sitio web falso.

• Los ataques de denegación de servicio (DoS) hacen los sitios web no disponibles temporalmente o indefinidamente lo que resulta en la falta de disponibilidad de los sitios web correspondientes.

En un entorno de comunicación de línea terrestre convencional, los usuarios (denominados en lo sucesivo "usuarios") utilizan sus aparatos de comunicación para acceder a los servidores de aplicaciones asociados con los proveedores de servicios sensibles. El ancho de banda requerido por los usuarios para acceder a los servidores de aplicaciones es proporcionado por una línea de comunicación tradicional ADSL (por sus siglas en inglés “Asymmetric Digital Subscriber Line” - línea de abonado digital asimétrica) que se utiliza de forma simultánea por varios proveedores de servicios de Internet para proporcionar conectividad a internet a sus respectivos usuarios. La seguridad a disposición de dichas líneas ADSL compartidas está restringida a aplicaciones criptográficas estándar. Dado el uso generalizado de las líneas ADSL compartidas, es posible que incluso usuarios no éticos y piratas informáticos están familiarizados con los estándares de encriptación utilizados a través de las líneas de comunicación compartidas. Dado que los usuarios hacen uso de líneas ADSL compartidas que comúnmente son utilizadas por multitud de usuarios para acceder a Internet, hay una posibilidad de que las transacciones realizadas por los usuarios sobre las líneas ADSL compartidas puedan ser pirateadas.

Por otra parte, ya que incluso los servidores de aplicaciones se hacen accesibles a través de la línea ADSL compartida, existe la posibilidad de que cualquier transacción financiera iniciada por el usuario, y aprobada, gestionada por el servidor de aplicaciones correspondiente pudiera ser pirateada. Además, dado que las líneas de comunicación compartidas no ofrecen la posibilidad de rastrear a los usuarios, es casi imposible determinar el origen del usuario que solicita un acceso a los servidores de aplicaciones. Además, no hay ninguna posibilidad clara en el

cortafuegos de los proveedores de servicios para que cualquier usuario salga en base al sitio que quieren visitar o que la BFI restrinja al usuario que viene de un cortafuegos no reconocido.

Existe una situación similar para todas las conexiones de datos que se ofrecen en la red inalámbrica. Aquí, sin embargo los usuarios utilizan sus dispositivos móviles para hacer llamada de datos o inicio de sesión, este tipo de llamadas se desvían en el centro conmutador de mensajes inalámbrico y salen a un dominio WWW externo a través del cortafuegos de la operadora y por lo tanto diluye el resto de la seguridad que goza la infraestructura móvil actual. Significa, en los dos enlaces de comunicación, que no hay privacidad ofrecida en base a las necesidades del negocio. Aún así, existe un proceso criptográfico independiente a eludir, que ha probado ser insuficiente y por lo tanto existe una gran cantidad de fuga de dinero en efectivo y credibilidad de negocios.

Los sistemas que facilitan inicios de sesión empresariales, inicios de sesión de gestión de fideicomiso, gestión de la nube y similares también se enfrentan a problemas similares a los de las BFI y se requiere una solución que se pueda extender con eficacia a todos los sistemas antes mencionados. Por otra parte, se siente la necesidad de un sistema que:

• proporciona a los usuarios ancho de banda de canal de comunicación privado seguro y resistente a piratas informáticos para la comunicación con servidores de aplicaciones asociados con proveedores de servicios sensibles;

• proporciona una solución de una sola ventana privada para la comunicación entre todos los proveedores de servicios sensibles disponibles y sus respectivos usuarios;

• garantiza que el nivel de seguridad a disposición de todos los proveedores de servicios sensibles y sus respectivos usuarios es de naturaleza uniforme, pero dinámica en términos de seguridad;

• garantiza que al menos el usuario es autenticado antes del comienzo de una transacción;

• garantiza que los usuarios, así como servidores de aplicaciones asociados con los proveedores de servicios sensibles, se autentican antes del comienzo de las transacciones;

• garantiza que cada trama involucrada en una transacción de usuario está asegurada y el servidor involucrado en la transacción de usuario se autentica cada vez que se inicia una transacción;

• hace uso de las técnicas de comunicación híbridas para garantizar que las transacciones realizadas a través del sistema están en un canal de comunicación privado y por lo tanto resistente a piratas informáticos; y

• ofrece modo "fuera de banda" y privado de la comunicación entre servidores de aplicaciones asociados con proveedores de servicios sensibles y sus respectivos usuarios.

Objetos

Algunos de los objetos no limitativos de la presente divulgación, que al menos una realización del presente documento satisface, son los siguientes:

Un objeto de la presente divulgación es proporcionar a los usuarios un canal de comunicación privado seguro y resistente a piratas informáticos para conectarse a servidores de aplicaciones asociados con proveedores de servicios sensibles.

Un objeto más de la presente divulgación es proporcionar una solución de una sola ventana privada para la comunicación entre todos los proveedores disponibles de servicios sensibles y sus respectivos usuarios.

Aún otro objeto de la presente divulgación es proporcionar un sistema que garantiza que el nivel de seguridad a disposición de todos los proveedores de servicios sensibles y sus respectivos usuarios es de naturaleza uniforme.

Todavía un objeto adicional de la presente divulgación es proporcionar un sistema que garantiza que al menos el usuario es autenticado antes del inicio de una transacción.

Otro objeto de la presente divulgación es proporcionar un sistema que garantiza que los usuarios, así como servidores de aplicaciones asociados con proveedores de servicios sensibles están claramente autenticados y cada trama de la transacción está asegurada.

Un objetivo más de la presente divulgación es proporcionar un sistema que hace uso de múltiples técnicas de comunicación privada para garantizar que las transacciones realizadas a través del sistema son resistentes a piratas informáticos.

Otro objeto de la presente divulgación es hacer disponible un sistema que ofrece modo “fuera de banda” y privado de comunicación entre servidores de aplicaciones asociados con proveedores de servicios sensibles y sus respectivos usuarios.

Aún otro objeto de la presente divulgación es proporcionar conectividad fuera de banda y servicios tanto en el extremo de usuario como en el extremo de servidor de aplicaciones.

Todavía un objeto adicional de la presente divulgación es proporcionar un sistema que hace uso de un mecanismo global “de desafío de dos factores” para identificar / autenticar apropiadamente al usuario. Otro objeto de la presente divulgación es proporcionar un sistema que ofrece una fácil retro-adaptación en términos de despliegue.

Otro objeto aún de la presente divulgación es proporcionar un sistema que deja huella cero a pesar de que al sistema se acceda desde entornos web no asegurados incluyendo cibercafés, zonas Wi-Fi y similares.

Todavía un objeto adicional de la presente divulgación es proporcionar un sistema que proporcione al usuario un acceso a servidores de aplicaciones asociados con proveedores de servicios sensibles sólo después de que el usuario que se ha autenticado con el sistema.

Otro objeto de la presente divulgación es proporcionar un sistema que hace uso de técnicas de "rastreo de geo-localización" para identificar la ubicación del usuario que intenta acceder al sistema.

Aún otro objeto de la presente divulgación es hacer disponible un sistema que proporciona al usuario credenciales comunes correspondientes a varios proveedores de servicios sensibles.

Todavía un objeto adicional de la presente divulgación es proporcionar un sistema que es altamente escalable, robusto y rentable para disfrutar de los beneficios de ofertas de Internet ubicuas.

Otros objetos y ventajas de la presente divulgación serán más evidentes a partir de la siguiente descripción cuando se lea en conjunción con las figuras que se acompañan, que no están destinadas a limitar el alcance de la presente divulgación.

Sumario

La presente divulgación prevé un sistema implementado por ordenador para proporcionar a los usuarios acceso seguro a servidores de aplicaciones. El sistema, de conformidad con la presente divulgación, incluye:

• un motor de comunicación que se comunica con un conjunto de aparatos de comunicación, configurado el motor de comunicación para recibir al menos una petición de un aparato de comunicación de petición, en el que la petición corresponde a una petición para acceder a al menos un servidor de aplicaciones;

• medios híbridos de telecomunicaciones que cooperan con el motor de comunicación, adaptados los medios híbridos de telecomunicaciones para establecer un enlace de comunicación privado, fuera de banda (tanto en el extremo de usuario como en el extremo de servidor de aplicaciones), con el aparato de comunicación de petición y asignar ancho de banda de comunicación privado, fuera de banda, al aparato de comunicación de petición, en el que el tipo de enlace de comunicación privado, fuera de banda, se determina basándose en el tipo del canal de comunicación previamente asociado con el aparato de comunicación de petición.

De acuerdo con la presente divulgación, el sistema incluye un motor de autenticación que se comunica con el aparato de comunicación de petición a través del enlace de comunicación privado, fuera de banda, comprendiendo el motor de autenticación:

■ medios de generación de desafío adaptados para utilizar el ancho de banda de comunicación privado, fuera de banda, para transmitir desafíos de factores múltiples incluyendo desafío de primer factor, desafío de segundo factor y desafío de tercer factor, al aparato de comunicación de petición;

■ medios de verificación adaptados para verificar la identidad del usuario asociado con el aparato de comunicación de petición basándose en la respuesta del usuario a por lo menos uno de los desafíos de factores múltiples, adaptados, además, los medios de verificación para verificar la autenticidad del servidor de aplicaciones cuyo acceso fue pedido por el usuario, basándose en al menos certificados digitales asociados con el servidor de aplicaciones; y

■ medios de unión adaptados para utilizar el ancho de banda de comunicación privado, fuera de banda, para establecer un enlace de comunicación privado, fuera de la banda, entre el aparato de comunicación de petición y el servidor de aplicaciones sólo en el caso de que el usuario y el servidor de aplicaciones se verifican con éxito por los medios de verificación.

De acuerdo con la presente divulgación, los medios híbridos de telecomunicaciones incluyen además medios de conmutación adaptados para conmutar automáticamente el aparato de comunicación de petición al enlace de comunicación privado, fuera de banda.

De acuerdo con la presente divulgación, el motor de autenticación incluye un repositorio adaptado para almacenar al menos uno de una pluralidad de números aleatorios, una pluralidad de identificadores de imagen, una pluralidad de capturas, credenciales biométricas únicas correspondientes a los usuarios, una pluralidad de caracteres alfanuméricos y una pluralidad de ecuaciones.

De acuerdo con la presente divulgación, los medios de generación de desafíos incluyen terceros medios que cooperan con el repositorio y adaptados para generar opcionalmente un desafío de tercer factor en forma de ecuación de una sola vez, de duración limitada.

De acuerdo con la presente divulgación, el ancho de banda de comunicación privado, fuera de banda, se asigna a través de un enlace de comunicación privado, fuera de banda, seleccionado del grupo que consiste en un enlace de comunicación privado cableado, un enlace de comunicación privado inalámbrico y una conexión privada de red, basada en inalámbrico.

De acuerdo con la presente divulgación, el sistema incluye además medios de terminación adaptados para terminar de forma automática el enlace de comunicación privado, fuera de banda, al completar la comunicación entre el aparato de comunicación de petición y el servidor de aplicaciones cuyo acceso fue pedido por el usuario.

La presente divulgación prevé un método implementado por ordenador para proporcionar a los usuarios acceso seguro a servidores de aplicaciones. El método implementado por ordenador, de acuerdo con la presente divulgación, incluye las siguientes etapas:

• recibir al menos una petición de un aparato de comunicación de petición asociado con un usuario, en el que la petición corresponde a una petición para acceder a al menos un servidor de aplicaciones;

• rastrear la ubicación del aparato de comunicación de petición y rastrear el tipo de canal de comunicación utilizado por el aparato de comunicación de petición para transmitir la petición;

• asignar ancho de banda de comunicación privado, fuera de banda, para el aparato de comunicación de petición y establecer un enlace de comunicación privado, fuera de banda, con el aparato de comunicación de petición;

• utilizar el ancho de banda de comunicación privado, fuera de banda, para transmitir desafíos de factores múltiples incluyendo desafío de primer factor, desafío de segundo factor y desafío de tercer factor, al aparato de comunicación de petición;

• verificar el usuario asociado con el aparato de comunicación de petición basándose en la respuesta del usuario a por lo menos uno de los desafíos de factores múltiples, y verificar la autenticidad del servidor de aplicaciones cuyo acceso fue pedido por el usuario, basándose en al menos certificados digitales asociados con el servidor de aplicaciones; y

• usar el ancho de banda de comunicación privado, fuera de banda, para establecer un enlace de comunicación privado, fuera de banda, entre el aparato de comunicación de petición y el servidor de aplicaciones sólo en el caso de que el usuario y el servidor de aplicaciones se verifican con éxito.

De acuerdo con la presente divulgación, en el que la etapa de establecer un enlace de comunicación privado, fuera de banda, con el aparato de comunicación de petición incluye además la etapa de conmutar automáticamente el aparato de comunicación de petición al enlace de comunicación privado, fuera de banda.

De acuerdo con la presente divulgación, la etapa de utilizar el ancho de banda de comunicación privado, fuera de banda, para establecer un enlace de comunicación privado, fuera de banda, con el aparato de comunicación de petición incluye además la etapa iniciar un apretón de manos SSL (Secured Socket Layer) con el aparato de comunicación de petición.

De acuerdo con la presente divulgación, la etapa de utilizar el ancho de banda de comunicación privado, fuera de banda, para establecer un enlace de comunicación privado, fuera de banda, con el aparato de comunicación de petición incluye además la etapa de terminar automáticamente el enlace de comunicación privado, fuera de banda, al completar la comunicación entre el aparato de comunicación de petición y el servidor de aplicaciones.

Breve descripción de los dibujos que se acompañan

El método y el sistema implementado por ordenador para proporcionar a los usuarios acceso seguro a servidores de

aplicaciones se describirán ahora con referencia a los dibujos no limitativos que se acompañan, en los cuales:

la figura 1A y la figura 1B son representaciones esquemáticas de los sistemas de la técnica anterior utilizados para proporcionar acceso a servidores de aplicaciones asociados con proveedores de servicios sensibles;

la figura 2 es una representación esquemática del sistema para proporcionar a los usuarios acceso seguro a servidores de aplicaciones, de acuerdo con la presente divulgación;

la figura 2A es un diagrama de bloques que representa la conectividad entre el motor de autenticación y el servidor de aplicaciones, de acuerdo con la presente divulgación;

la figura 2B proporciona una representación gráfica de la manera en que el sistema de la presente divulgación proporciona a los usuarios acceso seguro a servidores de aplicaciones;

la figura 2C ilustra la implementación de la aplicación de extremo trasero correspondiente al sistema de la presente divulgación;

la figura 3 ilustra el flujo de datos en todo el sistema previsto por la presente divulgación;

las figuras 4A y 4B corresponden a un diagrama de flujo que ilustra las etapas implicadas en el método para facilitar el pago seguro por internet y las transacciones, de acuerdo con la presente divulgación;

la figura 5 corresponde a un diagrama de flujo que ilustra la comunicación entre los usuarios finales y servidores de aplicaciones, de acuerdo con la presente divulgación.

Descripción detallada de los dibujos que se acompañan

La presente descripción se describirá ahora con referencia a los dibujos que se acompañan, que no limitan el alcance y ámbito de la divulgación. La descripción proporcionada es puramente a modo de ejemplo e ilustración.

Las realizaciones del presente documento y las diversas características y detalles ventajosos de las mismas se explican con referencia a las realizaciones no limitantes en la siguiente descripción. Descripciones de componentes bien conocidos y técnicas de procesamiento se omiten para no oscurecer innecesariamente las realizaciones en el presente documento. Los ejemplos usados en este documento están destinados simplemente a facilitar la comprensión de maneras en que las realizaciones en el presente documento pueden ponerse en práctica y permitir aún más a los expertos en la técnica poner en práctica las realizaciones en el presente documento. Por consiguiente, los ejemplos no deben interpretarse como limitantes del alcance de las realizaciones en el presente documento.

La descripción de aquí en adelante, de las realizaciones específicas, revelará completamente la naturaleza general de las realizaciones en el presente documento que otros pueden, mediante la aplicación de los conocimientos actuales, modificar fácilmente y/o adaptar para diversas aplicaciones sin salir tales realizaciones específicas del concepto genérico y, por lo tanto, tales adaptaciones y modificaciones deberían y se pretende que estén comprendidas dentro del significado y gama de equivalentes de las realizaciones descritas. Ha de entenderse que la fraseología o terminología empleada en el presente documento es para el propósito de descripción y no de limitación. Por lo tanto, aunque las realizaciones en el presente documento se han descrito en términos de realizaciones preferidas, los expertos en la técnica reconocerán que las realizaciones en el presente documento se pueden poner en práctica con modificaciones dentro del espíritu y alcance de las realizaciones como se describe en el presente documento.

El sistema y el método previsto en la presente descripción no se limitan a proporcionar a los usuarios acceso seguro a servidores de aplicaciones. El sistema y el método también aseguran que las transacciones realizadas por los usuarios a través de los servidores de aplicaciones permanecen protegidas y resistentes a piratas informáticos. El término “transacción” en esta memoria descriptiva indica transacciones sensibles, incluyendo pero no limitadas a la transferencia electrónica de fondos, e-contratación de bienes y servicios, operaciones bancarias en línea, transacciones que dan acceso a elementos de datos privilegiados y sensibles y similares. La utilidad del sistema y el método previstos en la presente divulgación no se limita al manejo de las transacciones correspondientes a las instituciones bancarias y financieras y se puede extender al manejo de cualquier tipo de transacción, incluido el acceso electrónico de datos y similares.

Por lo general, las transacciones antes mencionadas se implementan por vía electrónica. Dado que la mayoría de las transacciones antes mencionadas son de naturaleza sensible, los usuarios que llevan a cabo estas transacciones deben autenticarse antes de realizar las transacciones. Típicamente, un usuario en particular tiene que realizar múltiples transacciones correspondientes a múltiples proveedores de servicios sensibles y, para acordarse mejor, los usuarios tienden a asociar el mismo conjunto de credenciales (normalmente, un nombre de usuario común y contraseña común) para acceder a una pluralidad de servidores de aplicaciones tales como

servidor de transferencia de archivos, servidores bancarios y similares. Por otra parte, los usuarios usan múltiples aparatos / equipos de comunicación, tales como ordenadores portátiles, teléfonos móviles y similares, para comunicarse con servidores de aplicaciones asociados con proveedores de servicios sensibles. En tales casos, debido a la multiplicidad asociada con las credenciales de autenticación y debido al hecho de que las credenciales han sido utilizadas a través de múltiples aparatos, hay una posibilidad de que el secreto asociado con las credenciales de autenticación pudiera verse comprometido y, además, las credenciales de autenticación podrían ser sometidas a ataques de piratas informáticos / suplantación de identidad / suplantación de procedencia y subsiguientemente ser mal utilizadas.

La figura 1A ilustra el sistema de la técnica anterior para la realización de transacciones electrónicas. En el sistema de la técnica anterior, los usuarios hacen uso de aparatos de comunicación para acceder a los servidores de aplicaciones. Como se muestra en la figura 1A, "Usuario A" y un "Usuario B" utilizan sus aparatos de comunicación inalámbricos / de línea de cable incluyendo pero no limitados a teléfono móvil, ordenador portátil, ordenador de sobremesa y el iPad para iniciar sesión en Internet para conectarse a la institución financiera deseada "Banco A" o "Banco B". Como se ve en la figura 1A, el "Usuario A" se conecta a "ISP A" y el "Usuario B" se conecta a "MISP B" (del inglés "Mobile Internet Service Provider" - proveedor de servicios de internet móvil), utilizando una gama de tecnologías, incluyendo red inalámbrica móvil basada en 3G o línea ADSL (línea de abonado digital asimétrica) física. Posteriormente, el usuario "A" y el usuario "B" inician sesión en el sitio web público de la red de banca predeterminado asociado con respectivos bancos utilizando sus credenciales de inicio de sesión pre-registradas. La seguridad de las credenciales y los datos de transacción financieros está garantizada por la utilización de interfaces de aplicaciones de criptografía en el sistema de la técnica anterior. Este modo convencional de llevar a cabo una transacción financiera no es seguro, ya que no es posible ofrecer los detalles de la conexión privada entre el banco y los usuarios, por lo tanto una conexión ilegítima no puede denegarse por la aplicación de la red de banca. Por otra parte, la línea de comunicación ADSL tradicional o las redes inalámbricas móviles tradicionales son utilizadas simultáneamente por varios proveedores de servicios de Internet para proporcionar conectividad a internet a sus respectivos usuarios. La seguridad a disposición de dichas líneas ADSL / redes inalámbricas móviles compartidas se limita a aplicaciones criptográficas estándar. Dado el uso generalizado de las líneas ADSL y redes inalámbricas móviles compartidas, es posible que los usuarios no éticos y los piratas informáticos estén familiarizados con los estándares de encriptación utilizados en todas las líneas de comunicación compartidas estándar. Por lo tanto, existe la posibilidad de que las transacciones realizadas por los usuarios sobre las líneas ADSL / redes inalámbricas móviles compartidas puedan ser pirateadas. Por otra parte, ya que incluso los servidores de aplicaciones, en este caso los servidores de aplicaciones asociados con "Banco A" y "Banco B", se hacen accesibles a través de línea ADSL / red inalámbrica móvil compartida, existe la posibilidad de que cualquier transacción financiera iniciada por el usuario, y aprobada, gestionada por el servidor de aplicaciones correspondiente también pueda ser pirateada. Además, puesto que se accede a servidores de aplicaciones a través de líneas ADSL compartidas o enlace de comunicación basado en GPRS compartido, hay una posibilidad de que los piratas informáticos también puedan piratear los servidores de aplicaciones.

La figura 1B ilustra el sistema de la técnica anterior para la realización de transacciones electrónicas a través de aparatos de comunicación de los usuarios incluyendo teléfonos móviles y ordenadores personales. Como se muestra en la figura 1B, los usuarios A0 a An y los usuarios B0 a Bn utilizan sus aparatos de comunicación inalámbrica, incluyendo pero no limitado a teléfono móvil, y el iPad para iniciar sesión en Internet para conectarse a la institución financiera deseada "Banco A" y "Banco B", respectivamente. Como se ve en la figura 1B, el "Usuario A" se conecta a la "MISP A" y "Usuario B" se conecta a "MISP B" usando una variedad de tecnologías incluyendo red inalámbrica móvil basada en 3G. Posteriormente, el usuario "A" y el usuario "B" inician sesión en el sitio web de la red de banca pública predeterminada asociada con respectivos bancos utilizando sus credenciales de inicio de sesión pre-registradas. La seguridad de las credenciales y los datos de transacción financieros está garantizada por la utilización de interfaces de aplicaciones de criptografía en el sistema de la técnica anterior. Este modo convencional de llevar a cabo una transacción financiera no es seguro, ya que no es posible ofrecer los detalles de la conexión privada entre el banco y los usuarios, por lo tanto una conexión ilegítima no puede denegarse por la aplicación de la red de banca. Por otra parte, las redes inalámbricas móviles / líneas ADSL físicas tradicionales se utilizan simultáneamente por varios proveedores de servicios de Internet para proporcionar conectividad a internet a sus respectivos usuarios. La seguridad a disposición de dichas redes inalámbricas móviles / líneas ADSL físicas compartidas está restringida a aplicaciones criptográficas estándar. Dado el uso generalizado de las redes inalámbricas móviles, es posible que los usuarios no éticos y los piratas informáticos estén familiarizados con los estándares de encriptación utilizados en todas las líneas de comunicación compartidas estándar. Por lo tanto, existe la posibilidad de que las transacciones realizadas por los usuarios en las redes inalámbricas móviles / líneas ADSL físicas compartidas puedan ser pirateadas. Por otra parte, ya que incluso los servidores de aplicaciones, en este caso los servidores de aplicaciones asociados con "Banco A" y "Banco B", son accesibles a través de la red inalámbrica móvil / líneas ADSL físicas compartidas, hay una posibilidad de que cualquier transacción financiera iniciada por el usuario, y aprobada, gestionada por el servidor de aplicaciones correspondiente también pueda ser pirateada. Además, puesto que se accede a servidores de aplicaciones a través de enlace de comunicación basado en GPRS/3G / líneas ADSL físicas compartidas, hay una posibilidad de que los piratas informáticos también puedan piratear los servidores de aplicaciones.

Por otra parte, el modo convencional de realizar transacciones electrónicas requiere que los usuarios se registren de

forma individual para cada proveedor de servicio y por lo tanto mantener múltiples identidades o varios conjuntos de credenciales de autenticación que más a menudo conducen a la duplicación de las credenciales de autenticación para facilitar el recuerdo y las hace vulnerables a ataques de adivinación, en los que el pirata informático es capaz de adivinar las credenciales de autenticación de un usuario en particular.

Por lo tanto, para superar los inconvenientes asociados con el modo convencional de llevar a cabo transacciones electrónicas y para superar las deficiencias asociadas con los sistemas de la técnica anterior, la presente divulgación prevé un sistema y un método para proporcionar a los usuarios acceso seguro a servidores de aplicaciones. La presente divulgación prevé un sistema que actúa como una pasarela segura de confianza entre los usuarios y los servidores de aplicaciones asociadas con proveedores de servicios sensibles como la banca y las instituciones financieras y similares. En el caso de sistemas convencionales los usuarios contactan o inician sesión directamente en los servidores de aplicaciones asociados con proveedores de servicios sensibles. Pero en el caso del sistema previsto por la presente divulgación, se hace que los usuarios contacten con el sistema de la divulgación y, tras la verificación de sus respectivas identidades, se les permite acceder a los servidores de aplicaciones asociados con proveedores de servicios sensibles.

Si se considera el ejemplo de las transacciones financieras electrónicas sensibles, la mayoría de los usuarios que inician transacciones financieras electrónicas utilizan varias cuentas que tienen iguales conjunto de credenciales (nombre de usuario y contraseña comunes) y aparato para interactuar con los servidores de aplicaciones asociados a las BFI (Banca e Instituciones Financieras; denominadas proveedores de servicios sensibles de aquí en adelante). El fenómeno de la utilización de múltiples aparatos de comunicación, junto con el uso de nombre de usuario común y contraseña común para múltiples transacciones y aún así diversas compromete el secreto asociado con las credenciales y hace que las transacciones sean vulnerables a ataques de piratas informáticos, ataques de suplantación de identidad, ataques de suplantación de procedencia y similares. La vulnerabilidad asociada a las transacciones se multiplica debido al hecho de que los proveedores de servicios sensibles no pueden asegurar a los usuarios la disponibilidad de canal de comunicación seguro y los usuarios se ven obligados a hacer uso de ancho de banda de red que es compartido por y accesible a multitud de usuarios de Internet.

Por lo tanto, para proporcionar a los usuarios un canal de comunicación privado seguro para realizar transacciones sensibles y para asegurar que las transacciones sensibles permanecen seguras independientemente del tipo de dispositivo usado para la comunicación y también para absolver a los proveedores de servicios sensibles de la responsabilidad de proporcionar canal de comunicación seguro a los usuarios para llevar a cabo las transacciones y garantizar la seguridad de las transacciones realizadas por los usuarios, la presente divulgación ofrece un sistema y un método que actúan como una pasarela de confianza entre los servidores de aplicaciones asociados con los proveedores de servicios sensibles y los usuarios. El sistema previsto en la presente divulgación también hace que sea obligatorio para los usuarios establecer comunicación con el sistema que actúa como un servidor intermediario. El sistema, que actúa como un servidor intermediario, verifica las credenciales de los usuarios y tras la verificación exitosa de credenciales del usuario redirige al usuario al servidor de aplicaciones pedido, a través de un canal de comunicación seguro privado establecido entre el aparato de comunicación del usuario y el servidor de aplicaciones. Tal redirección se lleva a cabo a través de una red privada de comunicación que ofrece ancho de banda privado, fuera de banda, para tales comunicaciones y es inaccesible a cualquier persona que no sea el usuario que ha accedido, y que ha sido autenticado por el sistema de la presente divulgación. Al usuario se le hace utilizar posteriormente el enlace de comunicación privado, fuera de banda, para llevar a cabo sus transacciones. Al ofrecer un ancho de banda de comunicación privado a los usuarios, el sistema de la presente divulgación se asegura de que las transacciones realizadas por los usuarios están totalmente aseguradas. Además, mediante la autenticación de los usuarios cuando inician la sesión, el sistema de la presente divulgación absuelve a los proveedores de servicios sensibles de la responsabilidad de la autenticación de sus respectivos usuarios. Aún más, el sistema de la presente divulgación ofrece desafíos únicos de tres factores a los usuarios para tener una identificación clara de su identidad web.

Por otra parte, el sistema absuelve a los usuarios de la responsabilidad de recordar varios conjuntos de credenciales de autenticación y en su lugar ofrece un único proceso de inicio de sesión basado en autenticación de múltiples factores que podría a su vez ser utilizado para acceder a los servicios ofrecidos por todos los proveedores de servicios registrados en el sistema de la presente divulgación. Además, los usuarios se conectan a servidores de aplicaciones deseadas a través de ancho de banda privado, asignado exclusivamente, basada en sesión. Por lo tanto, la presente divulgación proporciona una red segura y privada para la comunicación entre usuarios y proveedores de servicios sensibles.

El sistema de la presente divulgación implementa los siguientes aspectos para realizar transacciones electrónicas seguras y resistentes a piratas informáticos:

• un conjunto de credenciales de autenticación para acceder a múltiples servidores de aplicaciones: cada usuario dispone de un único conjunto de credenciales de autenticación para acceder a los servicios ofrecidos por diversos proveedores de servicios sensibles, lo que elimina por lo tanto el problema de la multiplicidad de credenciales de autenticación;

• autenticación de factores múltiples: los usuarios pueden optar por uno o más niveles de autenticación / proceso de respuesta de desafío usando imágenes, números y huellas biológicas como parte de su conjunto único de credenciales de autenticación. Los usuarios también pueden seleccionar previamente una o más imágenes no verbales para confirmar la autenticidad del servidor de origen. Las imágenes no verbales preseleccionadas ayudan en la desactivación de envenenamiento de DNS (Sistema de Nombres de Dominio) y cuestiones conexas;

• los servidores de aplicaciones que intervienen en el proceso de comunicación no están alojados en la red de DNS (Sistema de Nombres de Dominio) y, por tanto, son resistentes al envenenamiento de DNS y otros problemas de seguridad relacionados;

• rastreo de geo-localización y conductual: el sistema de la presente divulgación, tras la confirmación de las credenciales de autenticación del usuario, rastrea el último nodo (acera) utilizado por el usuario en caso de conexión a Internet y rastrea el MSC (centro de conmutación de servicios móviles) utilizado por el usuario en caso de conexiones móviles inalámbricas. El rastreo de geo-localización y conductual permite que el sistema determine la identidad del usuario y rechace cualquier conexión ilegítima;

• gestión de cookies: el sistema de la presente divulgación realiza una gestión de cookies de anticipación al infligir cambios dinámicos en el navegador web del aparato de comunicación de petición asociado con el usuario y luego destruye los cambios tras la desconexión, por lo que la huella cero está disponible para los piratas informáticos, especialmente en entornos hostiles como los cibercafés y aeropuertos;

• canal de comunicación privado dedicado, fuera de banda: un canal de comunicación privado dedicado, fuera de banda, está a disposición del usuario cuando inicia sesión en el sistema;

• autenticación criptográficamente correcta y pasarela de autorización: el sistema de la presente divulgación inicia un apretón de manos SSL (Secure Socket Layers) con el aparato de comunicación de petición asociado con el usuario, realiza la autenticación de múltiples factores para el usuario, escribe una cookie de Internet en los navegadores asociados con el aparato de comunicación de petición, y verifica el certificado digital del servidor de aplicaciones antes de redirigir al usuario hacia el servidor de aplicaciones a través de un canal de comunicación seguro, privado, fuera de banda;

• mapeo seguro entre diversos canales de comunicación: el sistema de la presente divulgación proporciona mecanismos de comunicación a canal de comunicación de interfaz seleccionado por el usuario con la red óptica pasiva asociada con los servidores de aplicaciones;

• con un canal privado y seguro de comunicación establecido entre el aparato de comunicación del usuario y el servidor de aplicaciones correspondiente, información propia y confidencial puede ser intercambiada en páginas criptográficamente seguras, de API (Aplicación Programmer Interface) independiente del navegador ; y

• modelo de ingresos de pago por uso: los proveedores de servicios sensibles se facturan usando el modelo de ingresos “pago por uso” que calcula el coste basándose en el ancho de banda utilizado por un proveedor de servicios específico.

Haciendo referencia a la figura 2, se muestra un diagrama de bloques correspondiente al sistema 100 para facilitar las transacciones electrónicas seguras. El sistema 100, de acuerdo con la presente divulgación incluye un motor de comunicación indicado por el número de referencia 12. El motor de comunicación 12 facilita la interacción entre el sistema 100 y los usuarios que deseen acceder al sistema 100 con el fin de acceder ulteriormente a los servidores de aplicaciones asociados con proveedores de servicios sensibles tales como las BFI. El motor de comunicación 12 incluye un conmutador (no mostrado en las figuras), que permite a varios usuarios iniciar sesión en el sistema 100 simultáneamente. El conmutador podría ser un conmutador de nivel de metro “L2“. El motor de comunicación 12 incluye medios de recepción indicados por el número de referencia 12A, que están adaptados para recibir al menos una petición de un usuario, en el que la petición corresponde a una petición para acceder a al menos un servidor de aplicaciones receptor. El motor de comunicación 12 asegura que cada servidor de aplicaciones conectado al sistema 100 tiene una conexión de red óptica pasiva (PON) dedicada. La conexión PON proporcionada por el motor de comunicación 12 incluye enlaces de fibra óptica dedicados entre cada uno de los servidores de aplicaciones y el sistema 100.

El motor de comunicación 12 conecta un usuario al sistema 100 utilizando la línea cable / inalámbrica / 3G convencionales. De acuerdo con la presente divulgación, el motor de comunicación 12 incluye además medios de rastreo indicados por el número de referencia 12B. Tan pronto como un usuario inicia sesión en el sistema 100 a través de la red convencional de línea de cable / inalámbrica / 3G, los medios de rastreo 12B rastrean la ubicación de la última acera o la última milla equivalente (nodo), es decir, la ubicación del aparato de comunicación utilizado por el usuario para iniciar sesión en el sistema 100. En caso de que la última acera (nodo / aparato de comunicación) asociada con el usuario sea un ordenador de sobremesa / ordenador portátil y el ordenador de sobremesa / ordenador portátil incluya una conexión de red de línea de cable, entonces los medios de rastreo 12B

rastrean la localización de tal ordenador de sobremesa / ordenador portátil. Con posterioridad al rastreo de la ubicación de la última acera (nodo) del usuario, la responsabilidad de proporcionar conectividad de red de línea de cable se traspasa desde la red de telecomunicaciones convencional proporcionada por el proveedor de servicios de Internet (ISP) estándar a la red de telecomunicaciones privada ofrecida por los medios de telecomunicaciones híbridos 16. En consecuencia, si los medios de rastreo 12B determinan que la última acera (nodo) asociada con el usuario es un teléfono móvil habilitado 3G, entonces los medios de rastreo 12B rastrean la ubicación del dispositivo móvil (en la conectividad) utilizado por el usuario para iniciar sesión en el sistema 100 y posteriormente la responsabilidad de proporcionar conectividad de red inalámbrica se traspasa de la red de telecomunicaciones basada en 3G convencional a la red de telecomunicaciones privada ofrecida por los medios de telecomunicaciones híbridos 16.

Los medios de telecomunicaciones híbridos 16, de acuerdo con la presente divulgación, realizan la tarea de asignar ancho de banda de línea de cable / inalámbrico privado, seguro, fuera de banda, para, en primer lugar, la comunicación entre el aparato de comunicación del usuario y el motor de autenticación 18 y, en segundo lugar, para la comunicación entre el aparato de comunicación del usuario y el servidor de aplicaciones cuyo acceso fue pedido por el usuario.

Cuando la responsabilidad de proporcionar la conectividad de red se traspasa desde la red de telecomunicaciones convencional proporcionada por el proveedor de servicios de Internet (ISP) estándar a la red de telecomunicaciones privada ofrecida por los medios de telecomunicaciones híbridos 16, los medios de telecomunicaciones híbridos 16 asignan ancho de banda seguro privado, basado en sesión, al menos temporalmente, a ese usuario particular. Si se determina que el usuario ha iniciado sesión usando un dispositivo inalámbrico, entonces se asigna ancho de banda inalámbrico, basado en sesión, seguro, privado, fuera de banda, y si no ancho de banda de línea de cable, basado en sesión, fuera de banda.

Los medios de telecomunicaciones híbridos 16 gestionan su propio ancho de banda bruto de línea de cable / inalámbrico y permiten que el aparato de comunicación del usuario se conecte al sistema 100 o al servidor de aplicaciones al que el usuario requiere acceso. La asignación de ancho de banda privado de línea de cable/inalámbrico, fuera de banda, basado en sesión, comprueba que la comunicación entre el usuario y el servidor de aplicaciones es privado, seguro y por lo tanto invisible a otros usuarios de la World Wide Web. La asignación dedicada de ancho de banda dependiente de sesión, privado y fuera de banda también facilita la gestión segura de túneles para cada sesión. Los medios de telecomunicaciones híbridos 16 incluyen medios de conmutación indicados con el número de referencia 16A para iniciar el "traspaso" de la transacción desde la red de comunicación convencional a la red / enlace de comunicación privado, fuera de la banda. Los medios de conmutación 16A redirigen al usuario que está iniciando sesión en el sistema 100 desde la red de telecomunicaciones proporcionada por operadoras de telefonía móvil o la red de telecomunicaciones proporcionada por los proveedores de servicios de Internet convencionales al enlace de comunicación privado, fuera de banda, ofrecido por los medios de telecomunicaciones híbridos 16.

De acuerdo con la presente divulgación, tan pronto como el usuario es redirigido al enlace de comunicación privado, fuera de banda, ofrecido por los medios de telecomunicaciones híbridos 16, el motor de autenticación 18, a través del enlace de telecomunicaciones privado, fuera de banda, inicia un apretón de manos seguro de patrón aleatorio / específico de sesión / específico de trama con el aparato de comunicación de petición asociado con el usuario y realiza la autenticación de múltiples factores para el usuario. El motor de autenticación 14 ofrece por lo menos un desafío de primer factor, preferiblemente un desafío de segundo factor y opcionalmente un desafío de tercer factor al usuario a través del enlace de telecomunicaciones privada, fuera de la banda.

De acuerdo con la presente divulgación, el motor de autenticación 18 incluye medios de generación de desafíos 18A adaptados para proporcionar a los usuarios al menos el desafío de primer factor, preferiblemente el desafío de segundo factor y el desafío de tercer factor opcional.

En un proceso típico de autenticación de múltiples factores, varios desafíos, incluyendo las OTP (contraseñas de una sola vez), imágenes y desafíos de identificación biométricos, deben ser tramitados entre el usuario y el servidor de aplicaciones destinado. Dichas credenciales sólo pueden salvaguardarse si y si tal comunicación tiene lugar a través de un enlace de comunicación privado seguro resistente al pirateo informático. Los medios de generación de desafíos incluyen primeros medios (no mostrados en las figuras) adaptados para generar el desafío de primer factor que va a ser ofrecido a los usuarios. El desafío de primer factor es típicamente en forma de imágenes, es decir, el usuario que ha iniciado sesión en el sistema 100 tiene el desafío de identificar su PID (identificador de imagen).

Por lo general, durante la fase de registro en el sistema 100, al usuario se le pediría que seleccionara al menos una ID de imagen que posteriormente sería utilizada para autenticar al usuario. Durante la fase de autenticación, el usuario está provisto de un conjunto de imágenes, incluyendo el conjunto de imágenes la ID de imagen que fue seleccionada previamente por él / ella. El usuario es llamado a identificar su ID de imagen del conjunto de imágenes y, basándose en la ID de imagen seleccionada por el usuario, él / ella será autenticado. Alternativamente, el desafío de primer factor podría ser en forma de captura. En tal caso, el usuario es llamado a mirar la captura e introducir el contenido de la captura en el motor de autenticación 18 para probar su identidad. Alternativamente, el desafío de

primer factor también puede ser en forma de desafío de bio-matriz, es decir, se puede pedir al usuario que pruebe su identidad proporcionando correspondientes credenciales biométricas únicas. Alternativamente, los desafíos de primer factor también pueden incluir números aleatorios pre-generados. Los números aleatorios se generan utilizando sistemas de generación de números aleatorios convencionales y se transmiten al aparato de comunicación de petición del usuario. El usuario es llamado a introducir la secuencia de números aleatorios recibida en el motor de autenticación 18 a fin de determinar su identidad.

El desafío de primer factor se visualiza en el aparato de comunicación de petición pre-registrado asociado al usuario. Al aceptar y contestar el desafío de primer factor el usuario se autentica el servidor y recibe una confirmación en el sentido de que se está realmente comunicando con el sistema 100.

Posteriormente a la visualización del desafío de primer factor en el aparato de comunicación de petición asociado con el usuario, los medios de generación de desafíos 18A hacen uso de unos segundos medios (no mostrados en las figuras) para generar el desafío de segundo factor. El desafío de segundo factor es típicamente en forma de contraseña de una sola vez (OTP) de duración limitada. Las OTP, de conformidad con la presente divulgación, incluyen uno de los elementos seleccionados del grupo que consiste en secuencia de alfabetos, secuencia de números y secuencia de caracteres alfanuméricos. La contraseña de una sola vez, de duración limitada, se muestra en el aparato de comunicación de petición previamente registrado asociado con el usuario. La OTP se utiliza para reconocer apropiadamente al usuario que ha iniciado sesión en el sistema 100 tras completar el desafío de primer factor. Las OTP proporcionadas como desafío de segundo factor están basadas en sesión, es decir, son válidas sólo para la sesión de comunicación correspondiente y expiran después de una cantidad predeterminada de tiempo. Además de la generación de desafío de primer factor y desafío de segundo factor , los medios de generación de desafíos 18A hacen usos de unos terceros medios (no mostrados en las figuras) que están adaptados para generar opcionalmente desafío de tercer factor. El desafío de tercer factor ofrecido a los usuarios es típicamente en forma de ecuación algebraica simple, típicamente una ecuación de una sola vez (OTE). Por ejemplo, la ecuación algebraica podría ser en forma “Ax + By + C = D“; y el usuario es llamado a hacer uso de los valores asociados a las variables x, y y C para calcular el valor de D. Los valores de las variables x, y y C se proporcionan típicamente al usuario en su aparato de comunicación de petición, pre-registrado. El usuario es llamado a calcular el valor de OTE e introducir el valor calculado de la OTE al motor de autenticación 18 como parte de la respuesta al de tercer factor. De acuerdo con la presente divulgación, la forma en que el usuario elige la imagen de ID relevante de un grupo de imágenes y la forma en que el usuario responde a la ecuación de una sola vez ayuda en la obtención del rastreo de comportamiento correspondiente al usuario. el rastreo del comportamiento del usuario se determina en función de si elije la ID de imagen correcta y calcula el valor apropiado, normalmente utilizando el método a mano, que corresponde a la OTE.

De acuerdo con la presente divulgación, el desafío de primer factor ofrecido a los usuarios a través de los medios de generación de desafíos 18A se transmite en los navegadores de los aparatos de comunicación de petición pre-registrados asociados con los usuarios, por lo general en forma de cookies. Tan pronto como el usuario completa con éxito el desafío de primer factor , el desafío de segundo factor se transmite al navegador del aparato de comunicación de petición asociado con el usuario en forma de cookies. Para los fines de verificación, los desafíos en forma de cookies transmitidos al aparato de comunicación de petición asociado con el usuario se transmiten simultáneamente, a través de tramas de datos privadas basadas en SDH / SONET y también en forma de cookies, al servidor de aplicaciones al que el usuario busca acceso. La contraseña de una sola vez y la ecuación opcional de una sola vez transmitidas al aparato de comunicación de petición asociado con el usuario son encriptadas usando ya sea la norma avanzada de encriptación (AES) o el registro de desplazamiento de retroalimentación lineal (LFSR). Además, se pueden utilizar técnicas de criptografía cuántica también para la generación de claves cuánticas y la gestión de claves cuánticas para garantizar la seguridad incondicional a los datos que se transmiten. Posteriormente la contraseña de una sola vez tecleada por el usuario y los valores correspondientes a las variables contenidas en una ecuación de una sola vez se transmiten también al motor de autenticación 18 del aparato de comunicación de petición asociado con el usuario en un formato cifrado. La comunicación de datos entre el motor de autenticación 18 y el servidor de aplicaciones que al que el usuario desea acceder a tiene lugar en forma de tramas de datos privadas basadas en red óptica síncrona (SONET) / jerarquía digital síncrona (SDH). Las tramas SONET / SDH con patrones de sincronización de aplicaciones específicas que pueden no cumplir con las normas publicadas de la UIT (Unión Internacional de Telecomunicaciones). Otros varios procesos de secuencia de tramas dinámicos se pueden poner en marcha para hacer hacerlas tramas resistentes a piratas informáticos. Por lo tanto, cada trama es criptográficamente segura con gestión de claves dinámica y nueva ingeniería de entramado.

Los medios de generación de desafíos 18A, de acuerdo con la presente divulgación, están adaptados además para llevar a cabo la gestión de cookies de varios niveles con anticipación. El desafío de primer factor en forma de OTP puede ser generado utilizando un generador pseudo-aleatorio. El valor generado por el generador de números pseudo-aleatorio se puede utilizar como valor correspondiente a la OTP que debe proporcionarse a los usuarios. Del mismo modo, la OTE opcional proporcionada al usuario como desafío de tercer factor es también en forma de cookies. Tras una autenticación exitosa del usuario en función de los desafíos de múltiples factores, las cookies se eliminan del navegador web de los aparatos de comunicación de petición de los usuarios de tal manera que ninguna huella correspondiente a las cookies permanece en los aparatos de comunicación de petición de los usuarios.

De acuerdo con la presente divulgación, los medios de generación de desafíos 18A cooperan con unos medios de generación de imágenes (no mostrado en las figuras) que están adaptados para ofrecer al usuario una imagen cuando él / ella inicia sesión en el sistema 100 utilizando un ordenador de sobremesa o un ordenador portátil. La imagen se visualiza al usuario con el fin de asegurar al usuario que él / ella está introduciendo la OTP / OTE al sistema autorizado y no a un impostor o un pirata informático.

El motor de autenticación 18, de acuerdo con la presente divulgación, incluye medios de verificación 18B que verifican la identidad asociada con el usuario basándose en las respuestas (respuestas al desafío de primer factor, el desafío de segundo factor y el desafío de tercer factor opcional). Si los medios de verificación 18B, basándose en las respuestas proporcionadas por el usuario, determinan que el usuario ha respondido con éxito tanto el desafío de primer factor como desafío de segundo factor, entonces posteriormente comprueba las credenciales correspondientes al servidor de aplicaciones para el que el usuario está buscando acceso basándose en, al menos, la clave basada en infraestructura de clave simétrica y los certificados digitales basados en infraestructura de clave pública . Después de la autenticación del usuario, así como el servidor de aplicaciones al que el usuario pidió acceso, los medios de enlace 18C del motor de comunicación 18 conectan el aparato de comunicación de petición asociado con el cliente al servidor de aplicaciones usando ancho de banda privado, fuera de banda, proporcionado por los medios de telecomunicaciones híbridos 16.

De acuerdo con la presente divulgación, el motor de autenticación 18 se comunica con el usuario a través de la red de telecomunicaciones privada, fuera de banda, que puede estar en forma de:

- medios de internet de línea de cable: esto se utiliza típicamente para la comunicación entre el sistema 100 y un usuario que utiliza n ordenador de sobremesa o un ordenador portátil; y

- red de comunicación inalámbrica: el medio de comunicación ofrecido al usuario es una red inalámbrica en caso de que el usuario esté usando su teléfono móvil para acceder e iniciar sesión en el sistema 100.

el razonamiento que está detrás de ofrecer múltiples modos de comunicación es asegurarse de que un pirata informático o un adversario no será capaz de determinar el modo de comunicación utilizado por el usuario para comunicarse con el sistema 100.

De acuerdo con la presente divulgación, el sistema 100 está adaptado para gestionar la comunicación de datos entre el motor de autenticación 18 y los servidores de aplicaciones. La comunicación de datos entre el motor de autenticación 18 y el servidor de aplicaciones correspondiente está basada en sesión. El sistema 100 se asegura de que la comunicación entre el motor de autenticación 18 y el servidor de aplicaciones correspondiente se lleva a cabo a través de túneles de comunicación autenticados y encriptados.

De acuerdo con la presente divulgación, con posterioridad a la verificación de las credenciales del servidor de aplicaciones al que el usuario ha pedido acceso, el motor de autenticación 18 inicia sesión del usuario en el servidor de aplicaciones correspondiente al que él / ella había planteado una petición de acceso. Una sesión de comunicación se establece posteriormente utilizando el ancho de banda privado, fuera de banda, proporcionado por los medios de telecomunicaciones híbridos 16 y entre los aparatos de comunicación de petición asociados con el usuario y el servidor de aplicaciones al que el usuario había pedido acceso.

De acuerdo con la presente divulgación, el sistema 100 puede comunicarse con el servidor de aplicaciones correspondiente mediante uno o más sistemas proxy. En el caso de que el servidor de aplicaciones al que se necesita acceder esté situado a distancia, el sistema 100 está adaptado para comunicarse con dicho servidor de aplicaciones situado a distancia utilizando uno o más proxies que están conectados al sistema 100 a través de red de comunicación segura y privada, inalámbrica/cableada. También es deseable que el sistema proxy que se encuentre en una ubicación geográfica cercana a la del servidor de aplicaciones pudiera ser físicamente cableado, por ejemplo usando cables de fibra óptica, al sistema 100. Mediante la adaptación de una infraestructura tal, el sistema 100 de la presente divulgación elimina la necesidad de servidores de aplicaciones ubicados será distancia sean físicamente cableados al sistema 100.

Haciendo referencia a la figura 2A, se muestra un diagrama de bloques que representa la conectividad entre el motor de autenticación 18 y el servidor de aplicaciones 20 asociado con proveedores de servicios sensibles. Haciendo referencia a la figura 2A, el servidor de aplicaciones 20 y el motor de autenticación 18 forman una parte de la red empresarial virtual (VEN). El servidor de aplicaciones 20 asociado con el proveedor de servicios sensibles podría ser un servidor bancario o un almacén de datos empresariales o de un terminal de punto de venta desde donde las transacciones monetarias se llevan a cabo o un servidor que facilita el comercio electrónico. Sin embargo, es posible que el servidor de aplicaciones 20 realice cualquier otra actividad especificada por proveedores de servicios sensibles. El motor de autenticación 18 identifica un servidor de aplicaciones 20 basándose en el nombre privado (no el nombre asignado al servidor de aplicaciones en el DNS) asociado con el servidor de aplicaciones 20. Los datos se intercambian entre el servidor de aplicaciones 20 y el motor de autenticación 18 en forma de tramas de datos basadas en SONET / SDH. Las tramas de datos objeto de intercambio se cifran utilizando estándares de encriptación seleccionados del grupo de estándares de encriptación que consiste en infraestructura de clave pública

(PKI), norma avanzada de encriptación (AES) y algoritmo de Diffie-Hellman. El motor de autenticación 18, con el propósito de verificación y con el fin de autenticar las credenciales asociadas con el servidor de aplicaciones, inicia el intercambio de clave basada en infraestructura de clave simétrica (SKI) con una frecuencia diaria. La clave se intercambia con una frecuencia diaria con el fin de permitir que el motor de autenticación 18 verifique adecuadamente la identidad del servidor de aplicaciones 20. Además, los datos, es decir, el desafío de primer factor, el desafío de segundo factor y el desafío de tercer factor opcional, enviados desde el motor de autenticación 18 al aparato de comunicación de petición del usuario se cifran típicamente usando esquemas de cifrado seleccionados entre el grupo de esquemas que consta de registro de desplazamiento de retroalimentación lineal (LFSR), infraestructura de clave pública (PKI) y el algoritmo de Diffie-Hellman. Posteriormente, los datos enviados de vuelta desde el aparato de comunicación de petición del usuario al motor de autenticación 18 también se cifran utilizando cualquiera de los esquemas de cifrado antes mencionados. El motor de autenticación 18 normalmente se comunica con el servidor de aplicaciones 20 a través de un túnel de comunicación seguro que está basado en sesión y que utiliza el ancho de banda privado, fuera de banda, proporcionado por los medios de telecomunicaciones híbridos 16.

Haciendo referencia a la figura 2B, se proporciona una representación gráfica de la forma en que el sistema 100 de la presente divulgación proporciona a los usuarios acceso seguro a servidores de aplicaciones. De acuerdo con la figura 2B, un primer usuario hace uso del teléfono móvil para acceder a un servidor de aplicaciones registrado en el sistema 100. La línea de comunicación cableada que es típicamente una línea simétrica digital asimétrica (ADSL) se conecta a través de un enrutador de borde a unos medios de conmutación 10. A diferencia de la configuración que se ve en la figura 1, en el caso de la figura 2 los usuarios se conectan a un conmutador 10 en lugar de establecer una conexión directa con el servidor de aplicaciones correspondiente a proveedor de servicios sensibles. Los medios de conmutación 10 están conectados a un centro de conmutación de servicios móviles desde donde se transmite la petición de acceso generada por el usuario a los medios de conmutación 10. Después de recibir la petición del usuario, el conmutador transfiere la petición de usuario desde la red de comunicación basada en ADSL convencional a una red / enlace de comunicación privada, fuera de banda. Posteriormente, una red / enlace de comunicación privada, fuera de banda, se establece a través del conmutador 10, entre el teléfono móvil asociado con el usuario y el motor de autenticación 18. El motor de autenticación 18 posteriormente autentica al usuario, ofreciendo desafíos de múltiples factores, a saber, el desafío de primer factor, el desafío de segundo factor y el desafío de tercer factor opcional. Basándose en la respuesta proporcionada por el usuario a los desafíos de factores múltiples, el motor de autenticación 18 establece selectivamente un enlace de comunicación privado, fuera de banda, entre el aparato de comunicación de petición asociado con el usuario (teléfono móvil en este caso) y el servidor de aplicaciones. En la figura 2B se muestra que la red de telecomunicaciones híbrida es proporcionada por “operadora C“. Los usuarios se conectan a los servidores de aplicaciones asociadas con proveedores de servicios sensibles que utilizan esta red de telecomunicaciones híbrida. De acuerdo con la figura 2B, el servidor de aplicaciones es un servidor asociado con un banco. Con posterioridad al establecimiento del enlace de fibra óptica, el resto de la comunicación se lleva a cabo a través del enlace de fibra óptica recientemente establecido en lugar del enlace ADSL convencional.

Haciendo referencia a la figura 2C, se muestra la aplicación de extremo trasero correspondiente al sistema 100. El sistema 100, como se ha explicado anteriormente, permite a varios usuarios acceder a peticiones a los servidores de aplicaciones utilizando varios aparatos de comunicación tales como teléfonos móviles, ordenadores portátiles y ordenadores de sobremesa. El sistema 100 incluye unos medios de telecomunicaciones híbridos (no mostrado) y medios de conmutación (conmutador híbrido) 10 y un armador 12. Los servidores de aplicaciones en el caso de esta figura en particular son los servidores asociados con organizaciones bancarias. Las peticiones de los múltiples usuarios se enrutan al sistema 100 a través de redes de telecomunicaciones convencionales y, posteriormente al enrutamiento de las peticiones al sistema 100, el usuario se conmuta desde la red de comunicación convencional a una red de telecomunicaciones privada, fuera de la banda. Los medios de conmutación 10 son capaces de traspasar la comunicación de usuario desde red de línea de cable, red inalámbrica y la red de comunicación móvil basada en GPRS/3G. Esta transferencia de la red de telecomunicaciones convencional, tal como la red de línea de cable / inalámbrica / GPRS / 3G se lleva a cabo a través de los medios de conmutación 10. El sistema 100 incluye además un armador SDH que transfiere datos en forma de paquetes de datos y entre el sistema 100 y servidores de aplicaciones. El sistema 100 también incluye un cortafuegos situado entre el sistema 100 y los servidores de aplicaciones con el fin de bloquear cualquier acceso no autorizado al servidor de aplicaciones. Los servidores de aplicaciones están conectados al sistema 100 a través de una red entre pares.

Haciendo referencia a la figura 3, se muestra el flujo de datos a través del sistema previsto por la presente divulgación. Como se muestra en la figura 3, los usuarios desde ubicaciones geográficas diversificadas se conectan al sistema de la presente divulgación. El conmutador “L2“ asociado con el sistema permite que un número múltiple de usuarios se conecten simultáneamente en el sistema.

Posteriormente, el conmutador L2 segrega los usuarios según sus necesidades y les proporciona acceso al motor de autenticación de la presente divulgación que ofrece desafíos de identificación de múltiples factores (IMF) a los usuarios. Las respuestas proporcionadas por los usuarios a los desafíos de identificación de múltiples factores se alimentan a un armador que está conectado a través de una red óptica pasiva (PON). El armador está adaptado para recibir los datos correspondientes a los desafíos de identificación de múltiples factores realizados por el usuario y, si la identificación de múltiples factores resulta ser exitosa, entonces se proporciona automáticamente al usuario el acceso al servidor de aplicaciones pedido que típicamente también puede ser un servidor de banco. La conexión

entre el armador y el servidor de aplicaciones es también a través de una red óptica pasiva.

En referencia a la figura 4A y 4B, se muestra un diagrama de flujo que describe las etapas implicadas en el método implementado por ordenador para proporcionar a los usuarios el acceso a servidores de aplicaciones de una manera segura. El método, de conformidad con la presente divulgación, incluye las siguientes etapas:

• recibir al menos una petición de un aparato de comunicación de petición asociado con un usuario, en el que la petición corresponde a una petición para acceder a al menos un servidor de aplicaciones 200;

• rastrear la ubicación del aparato de comunicación de petición y rastrear el tipo de canal de comunicación utilizado por el aparato de comunicación de petición para transmitir la petición 201;

• asignar ancho de banda de comunicación privado, fuera de banda, al aparato de comunicación de petición y establecer un enlace de comunicación privado, fuera de banda, con el aparato de comunicación de petición 202;

• utilizar el ancho de banda de comunicación privado, fuera de banda, para transmitir desafíos de múltiples factores incluyendo desafío de primer factor, desafío de segundo factor y desafío de tercer factor, al aparato de comunicación de petición 203;

• verificar el usuario asociado con el aparato de comunicación de petición en base a dicha respuesta de usuario a por lo menos uno de dichos desafíos de múltiples factores, y verificar la autenticidad del servidor de aplicaciones cuyo acceso fue pedido por el usuario, basándose en al menos certificados digitales asociados con el servidor de aplicaciones 204; y

• usar el ancho de banda de comunicación privado, fuera de de banda, para establecer un enlace privado de comunicación, fuera de banda, entre dicho aparato de comunicación de petición y el servidor de aplicaciones sólo en el caso de que el usuario y el servidor de aplicaciones se verifiquen con éxito 205.

De acuerdo con la presente divulgación, la etapa de establecer un enlace de comunicación privado, fuera de banda, con el aparato de comunicación de petición incluye además la etapa de conmutar automáticamente el aparato de comunicación de petición al enlace de comunicación privado, fuera de banda.

De acuerdo con la presente divulgación, la etapa de utilizar el ancho de banda de comunicación privado, fuera de banda, para transmitir desafíos de múltiples factores incluye además las siguientes etapas:

• generar un desafío de primer factor que incluye un identificador seleccionado del grupo de identificadores que consta de identificadores de imagen, capturas e identificadores biométricos;

• generar un desafío de segundo factor en forma de contraseña de una sola vez de duración limitada, en el que la contraseña de un solo uso incluye elementos seleccionados del grupo de elementos que consiste en la secuencia de alfabetos, la secuencia de números y la secuencia de caracteres alfanuméricos; y

• opcionalmente, generar un desafío de tercer factor en forma de ecuación de una sola vez con duración limitada.

De acuerdo con la presente divulgación, la etapa de utilizar el ancho de banda de comunicación privado, fuera de banda, para establecer un enlace de comunicación privado, fuera de banda, para el aparato de comunicación de petición, incluye además la etapa de iniciar un apretón de manos en SSL (capa seguro de receptáculo) con el aparato de comunicación de petición.

De acuerdo con la presente divulgación, la etapa de usar el ancho de banda de comunicación privado, para establecer un enlace de comunicación privado, fuera de banda, incluye además la etapa de terminar automáticamente el enlace de comunicación privado, fuera de banda, al completar la comunicación entre el aparato de comunicación de petición y el servidor de aplicaciones.

Haciendo referencia a la figura 5, se muestra un diagrama de flujo que representa la manera en que el sistema 100 de la presente divulgación ofrece ancho de banda privado seguro inalámbrico a usuarios que desean iniciar sesión en los servidores de aplicaciones. Como se observa en la figura 5, los usuarios utilizan su dispositivo móvil / ordenador personal para iniciar sesión en la aplicación de banca electrónica correspondiente, que a su vez les permite acceder a los servidores de aplicaciones asociados con, por ejemplo, “BANCO A" y "BANCO B“. Al contrario que los sistemas de la técnica anterior representados en las figuras 1A y 1B, la llamada de datos desde el teléfono móvil / ordenador personal del usuario se traspasa al motor de telecomunicaciones híbrido que proporciona al usuario ancho de banda inalámbrico privado seguro a través de una "torre híbrida". La llamada de datos se traspasa desde el Centro de Conmutación Móvil (MSC) a los medios de telecomunicaciones híbridos. Todas las llamadas de datos se agregan en el motor de telecomunicaciones híbrido y se transfiere sobre una WAN privada a través del ancho de banda privado seguro inalámbrico a un motor de autenticación que ofrece un desafío de primer factor (en

forma de identificadores de imagen / capturas / identificadores biométricos), un desafío de segundo factor (en forma de contraseña de una sola vez con duración limitada) y un desafío de tercer factor (ecuación de una sola vez con duración limitada) sobre el ancho de banda privado seguro inalámbrico para autenticar al usuario. Con posterioridad a la autenticación exitosa, la llamada de datos desde el teléfono móvil / ordenador personal del usuario se envía al servidor de aplicaciones correspondiente (en este caso, los servidores de aplicaciones del banco A y el banco B, respectivamente).

Avances técnicos

Los avances técnicos del sistema y el método previstos en la presente divulgación incluyen los siguientes:

• la presente divulgación proporciona a los usuarios canal de comunicación privado y seguro protegido y resistente a piratas informáticos para enlazar con servidores de aplicaciones;

• la presente divulgación proporciona una solución de única ventana para la comunicación entre todos los proveedores de servicios móviles disponibles de servicios sensibles y sus respectivos usuarios;

• la presente divulgación proporciona un sistema que garantiza que el nivel de seguridad a disposición de todos los proveedores de servicios sensibles y sus respectivos usuarios es de naturaleza uniforme;

• la presente divulgación proporciona un sistema que garantiza que al menos el usuario está debidamente autenticado (es quien es) antes del comienzo de una transacción;

• la presente divulgación proporciona un sistema que garantiza que los usuarios, así como servidores de aplicaciones asociados con proveedores de servicios sensibles, se autentican antes del comienzo de transacciones;

• la presente divulgación proporciona un sistema que hace uso de múltiples técnicas de comunicación para garantizar que las transacciones realizadas a través del sistema son resistentes a piratas informáticos;

• la presente divulgación pone a disposición un sistema que ofrece un modo de comunicación “fuera de banda“ y privado entre servidores de aplicaciones asociados con proveedores de servicios sensibles y sus respectivos usuarios;

• la presente divulgación proporciona un sistema que hace uso de un mecanismo de “desafío de múltiples factores " para identificar / autenticar apropiadamente al usuario;

• la presente divulgación proporciona un sistema que ofrece una fácil retro-adaptación en términos de despliegue;

• la presente divulgación proporciona un sistema que deja huella cero a pesar de que se acceda al sistema desde entornos web no seguros incluyendo cibercafés, zonas Wi-Fi y similares;

• la presente divulgación pone a disposición un sistema que proporciona al usuario acceso a servidores de aplicaciones asociados con proveedores de servicios sensibles sólo después de que el usuario se ha autenticado con el sistema;

• la presente divulgación proporciona un sistema que hace uso de técnicas de “rastreo de geo-localización“ para identificar la ubicación del usuario que intenta acceder al sistema;

• la presente divulgación pone a disposición sistema que proporciona al usuario credenciales comunes correspondientes a varios proveedores de servicios sensibles;

• la presente divulgación proporciona un sistema que es altamente escalable, robusto y rentable;

• la presente divulgación ofrece un sistema que es resistente a los futuros conmutadores de corte total debido a la utilización de ancho de banda privado;

• la presente divulgación ofrece un sistema que autentica a los usuarios utilizando autenticación basada en desafíos;

• la presente divulgación ofrece un sistema que proporciona anonimato en internet a los usuarios ofreciendo conectividad punto a punto en el laberinto de Internet y proporcionando credenciales de identidad basándose en la identificación de factores múltiples de los usuarios; y

• la presente divulgación ofrece un sistema que resiste elementos de guerra cibernética y conflictos cibernéticos garantizando que un pirata informático no tendrá ninguna información correspondiente a la comunicación privada, fuera de banda, entre un servidor de aplicaciones y el usuario correspondiente.

Aunque en el presente documento se ha puesto considerable énfasis sobre las características particulares de esta divulgación, se apreciará que se pueden hacer varias modificaciones, y que se pueden hacer muchos cambios en la realización preferida sin salir de los principios de la divulgación. Estas y otras modificaciones en la naturaleza de la divulgación o las realizaciones preferidas serán evidentes para los expertos en la técnica a partir de la divulgación de este documento, por lo que se ha de entender claramente que la materia descriptiva que antecede debe interpretarse simplemente como ilustrativa de la divulgación y no como una limitación.

REIVINDICACIONES

1. Un sistema implementado por ordenador para proporcionar a los usuarios acceso seguro a servidores de aplicaciones, comprendiendo dicho sistema:

• un motor de comunicación (12) que se comunica con un conjunto de aparatos de comunicación, configurado dicho motor de comunicación (12) para recibir al menos una petición de un aparato de comunicación de petición, en el que dicha petición corresponde a una petición para acceder al menos a un servidor de aplicaciones (20);

caracterizado porque el sistema también incluye:

• medios de telecomunicaciones híbridos (16) para proporcionar conectividad de red, dichos medios de telecomunicaciones híbridos (16) están cooperando con dicho motor de comunicación y están adaptados para establecer un enlace de comunicación privada, fuera de banda, con el aparato de comunicación de petición y asignar ancho de banda de comunicación privado, fuera de banda, al aparato de comunicación de petición, en el que el tipo de dicho enlace de comunicación privado, fuera de banda, está determinado basándose en el tipo de canal de comunicación asociado con anterioridad con el aparato de comunicación de petición, en el que dicho sistema incluye un motor de autenticación (18) que se comunica con el aparato de comunicación de petición por medio de un enlace de comunicación privado, fuera de banda, comprendiendo dicho motor de autenticación:

medios de generación de desafíos (18A) adaptados para usar dicho ancho de banda de comunicación privado, fuera de banda, para transmitir desafíos de múltiples factores que incluyen desafío de primer factor, desafío de segundo factor y desafío de tercer factor, al aparato de comunicación de petición;

medios de verificación (18B) adaptados para verificar la identidad del usuario asociado con el aparato de comunicación de petición basándose en la respuesta de dicho usuario a al menos uno de dichos desafíos de múltiples factores, adaptados además dichos medios de verificación (18B) para verificar la autenticidad de dicho servidor de aplicaciones (20) cuyo acceso fue pedido por dicho usuario, basándose en al menos certificados digitales asociados con dicho servidor de aplicaciones (20); y

medios de enlace (18C) adaptados para usar dicho ancho de banda de comunicación privado, fuera de banda, para establecer un enlace de comunicación privado, fuera de banda, entre el aparato de comunicación de petición y dicho servidor de aplicaciones solo en caso de que dicho usuario y dicho servidor de aplicaciones (20) se verifiquen exitosamente mediante dichos medios de verificación (18B).

2. El sistema implementado por ordenador según la reivindicación 1, en el que dichos medios de telecomunicaciones híbridos incluyen además medios de conmutación adaptados para conmutar automáticamente el aparato de comunicación de petición a dicho enlace de comunicación privada, fuera de banda.

3. El sistema implementado por ordenador según la reivindicación 1, en el que dicho motor de autenticación (18) incluye un repositorio adaptado para almacenar al menos uno de varios números aleatorios, varios identificadores de imágenes, varias capturas, credenciales biométricas únicas que corresponden a los usuarios, varios caracteres alfanuméricos y varias ecuaciones.

4. El sistema implementado por ordenador según la reivindicación 1, en el que dichos medios de generación de desafíos (18A) incluyen terceros medios que cooperan con dicho repositorio y adaptados para generar opcionalmente un desafío de tercer factor en forma de ecuación de una sola vez con duración limitada.

5. El sistema implementado por ordenador según la reivindicación 1, en el que dicho ancho de banda de comunicación privada, fuera de banda, está asignado por medio de enlace de comunicación privada, fuera de banda, seleccionado del grupo que consiste en enlace de comunicación cableado privado, enlace de comunicación inalámbrico privado y conexión de red privada basada en GPRS.

6. El sistema implementado por ordenador según la reivindicación 1, en el que dicho sistema incluye además medios de terminación adaptados para terminar automáticamente dicho enlace de comunicación privado, fuera de banda, al completar la comunicación entre el aparato de comunicación de petición y el servidor de aplicaciones cuyo acceso fue pedido por dicho usuario.

7. Un método implementado por ordenador para proporcionar a los usuarios acceso seguro a servidores de aplicaciones (20), incluyendo dicho método las siguientes etapas:

• recibir al menos una petición de un aparato de comunicación de petición asociado con un usuario, en el que dicha petición corresponde a una petición para acceder al menos a un servidor de aplicaciones (20);

• rastrear la ubicación del aparato de comunicación de petición y rastrear el tipo de canal de comunicación utilizado por el aparato de comunicación de petición para transmitir dicha petición;

• asignar ancho de banda de comunicación privado, fuera de banda, al aparato de comunicación de petición y establecer un enlace de comunicación privado, fuera de banda, con el aparato de comunicación de petición;

• usar dicho ancho de banda de comunicación privado, fuera de banda, para transmitir desafíos de múltiples factores que incluyen desafío de primer factor, desafío de segundo factor y desafío de tercer factor, al aparato de comunicación de petición;

• verificar el usuario asociado con el aparato de comunicación de petición basándose en la respuesta de dicho usuario al menos a uno de dichos desafíos de múltiples factores, y verificar la autenticidad del servidor de aplicaciones (20) cuyo acceso fue pedido por dicho usuario, basándose en al menos certificados digitales asociados con dicho servidor de aplicaciones (20); y

• usar dicho ancho de banda de comunicación privado, fuera de banda, para establecer un enlace de comunicación privado, fuera de banda, entre el aparato de comunicación de petición y dicho servidor de aplicaciones (20) solo en caso de que dicho usuario y dicho servidor de aplicaciones (20) se verifiquen exitosamente.

8. El método implementado por ordenador según la reivindicación 7, en el que la etapa de establecer un enlace de comunicación privado, fuera de banda, con el aparato de comunicación de petición incluye además la etapa de conmutación automática del aparato de comunicación de petición en dicho enlace de comunicación privada, fuera de banda.

9. El método implementado por ordenador según la reivindicación 7, en el que la etapa de usar dicho ancho de banda de comunicación privada, fuera de banda, para establecer un enlace de comunicación privada, fuera de banda, con el aparato de comunicación de petición incluye además la etapa de iniciar un apretón de manos SSL (Secured Socket Layer) con el aparato de comunicación de petición.

10. El método implementado por ordenador según la reivindicación 7, en el que la etapa de usar dicho ancho de banda de comunicación privada, fuera de banda, para establecer un enlace de comunicación privada, fuera de banda, con el aparato de comunicación de petición incluye además la etapa de terminar automáticamente dicho enlace de comunicación privada, fuera de banda, al completar la comunicación entre el aparato de comunicación de petición y el servidor de aplicaciones (20).

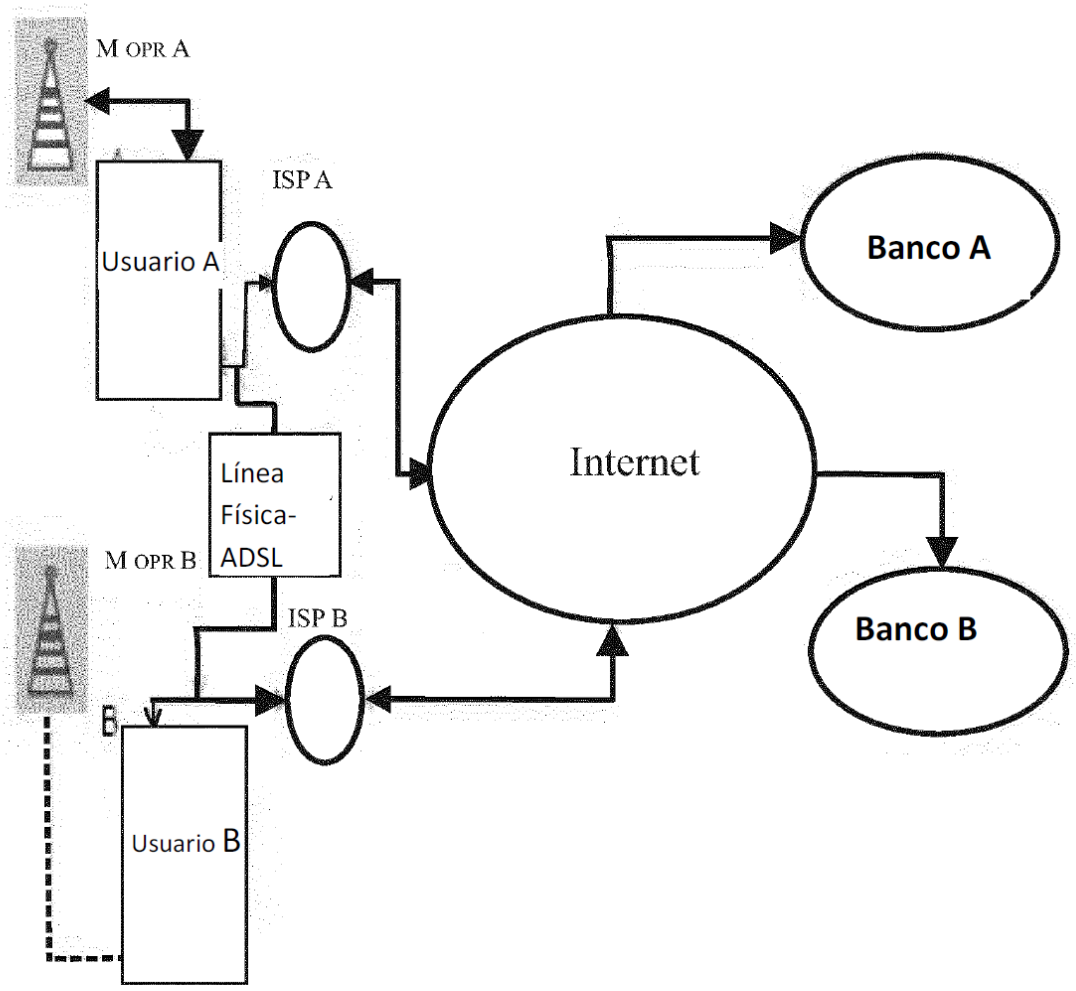
M OPR A
ISP A
Usuario A
Banco A
Internet
Línea
Física-
ADSL
M OPR B
ISP B
Banco B
B
Usuario B

Figura 1A

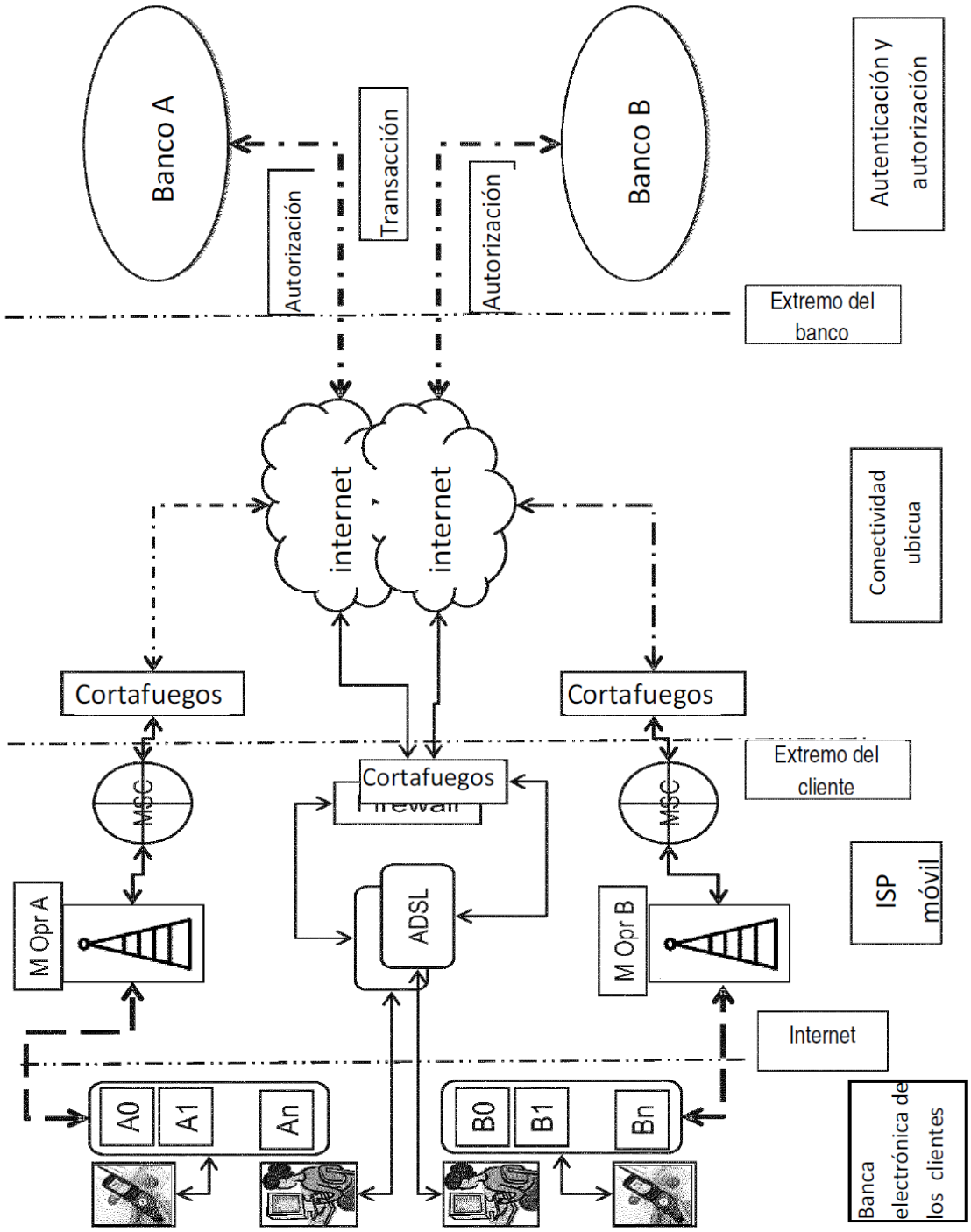
Banco A
Banco B
Autenticación y autorización
Autorización
Transacción
Autorización
Extremo del banco
internet
internet
Conectividad ubicua
Cortafuegos
Cortafuegos
Extremo del cliente
MBC
Cortafuegos
firewall
MBC
ISP móvil
M Opr A
ADSL
M Opr B
Internet
A0
A1
An
B0
B1
Bn
Banca electrónica de los clientes

Figura 1B

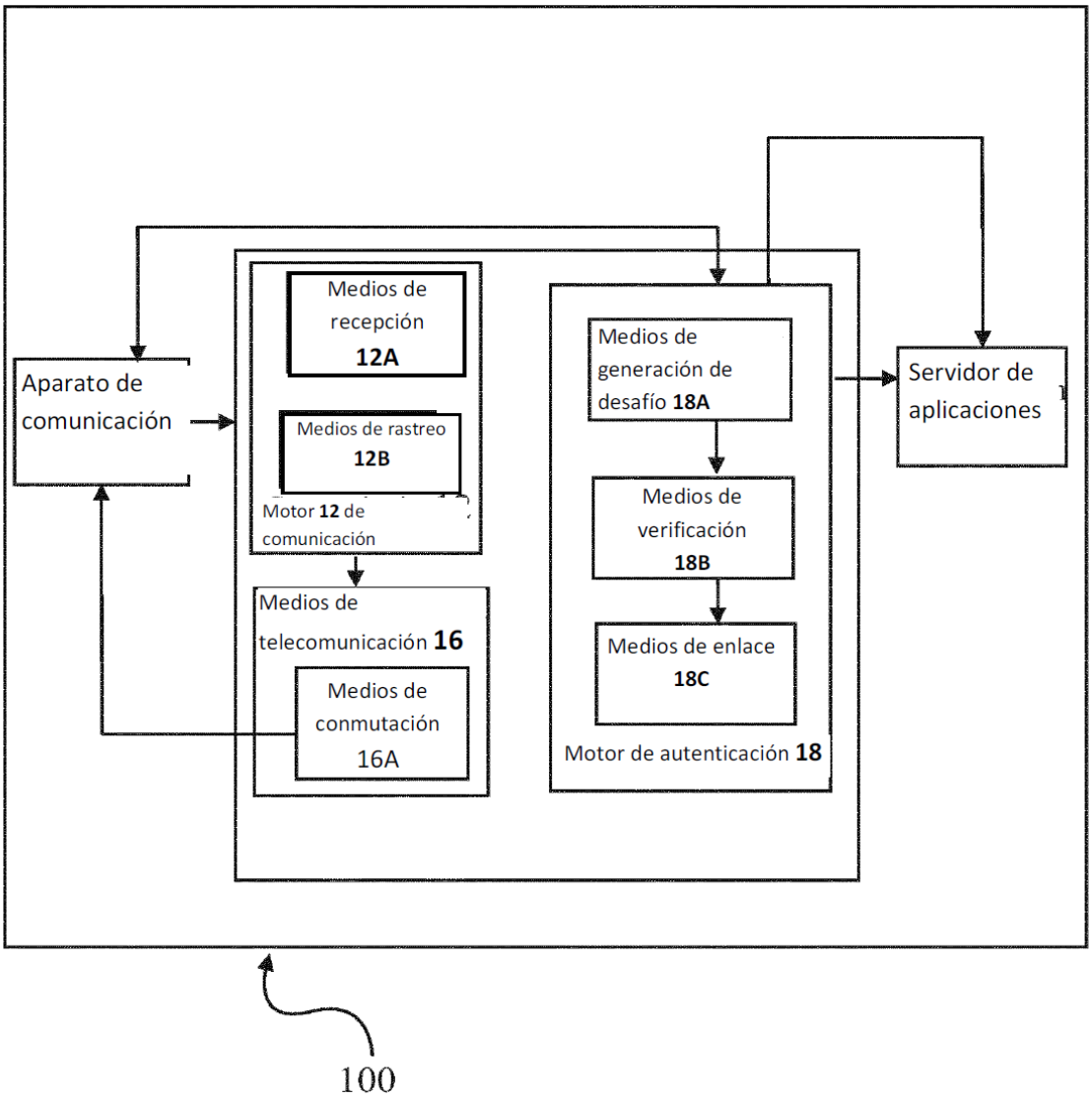
Aparato de comunicación
Medios de recepción 12A
Medios de rastreo 12B
Motor 12 de comunicación
Medios de telecomunicación 16
Medios de conmutación 16A
Medios de generación de desafío 18A
Medios de verificación 18B
Medios de enlace 18C
Motor de autenticación 18
Servidor de aplicaciones
100

FIGURA 2

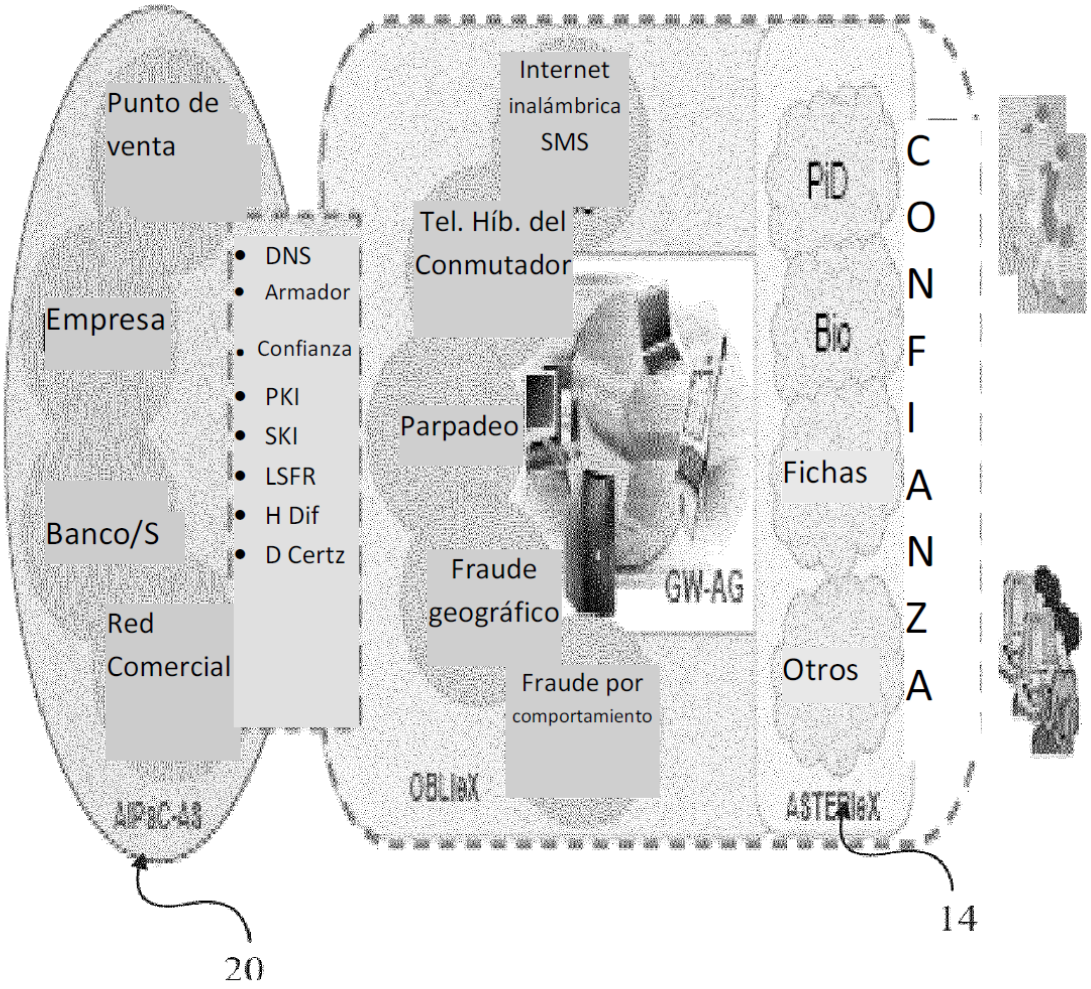
Punto de venta
Empresa
Banco/S
Red Comercial
DNS
Armador
Confianza
PKI
SKI
LSFR
H Dif
D Certz
Internet inalámbrica SMS
Tel. Híb. del Conmutador
Parpadeo
Fraude geográfico
Fraude por comportamiento
GW-AG
PID
Bio
Fichas
Otros
CONFIANZA
20
14

FIGURA 2A

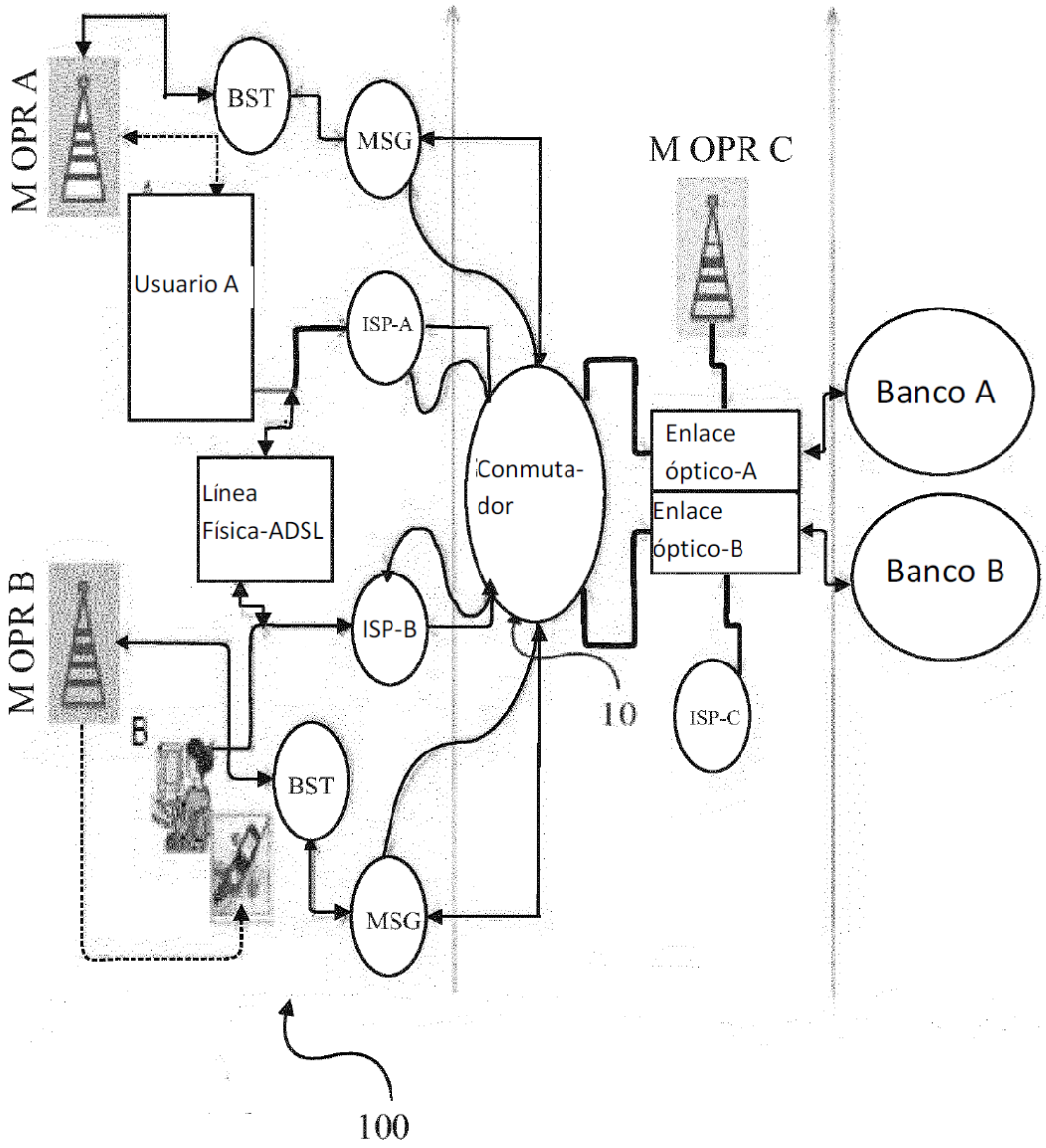
M OPR A
BST
MSG
M OPR C
Usuario A
ISP-A
Banco A
Enlace
óptico-A
Línea
Física-ADSL
Conmuta-
dor
Enlace
óptico-B
Banco B
M OPR B
ISP-B
10
ISP-C
BST
MSG
100

FIGURA 2B

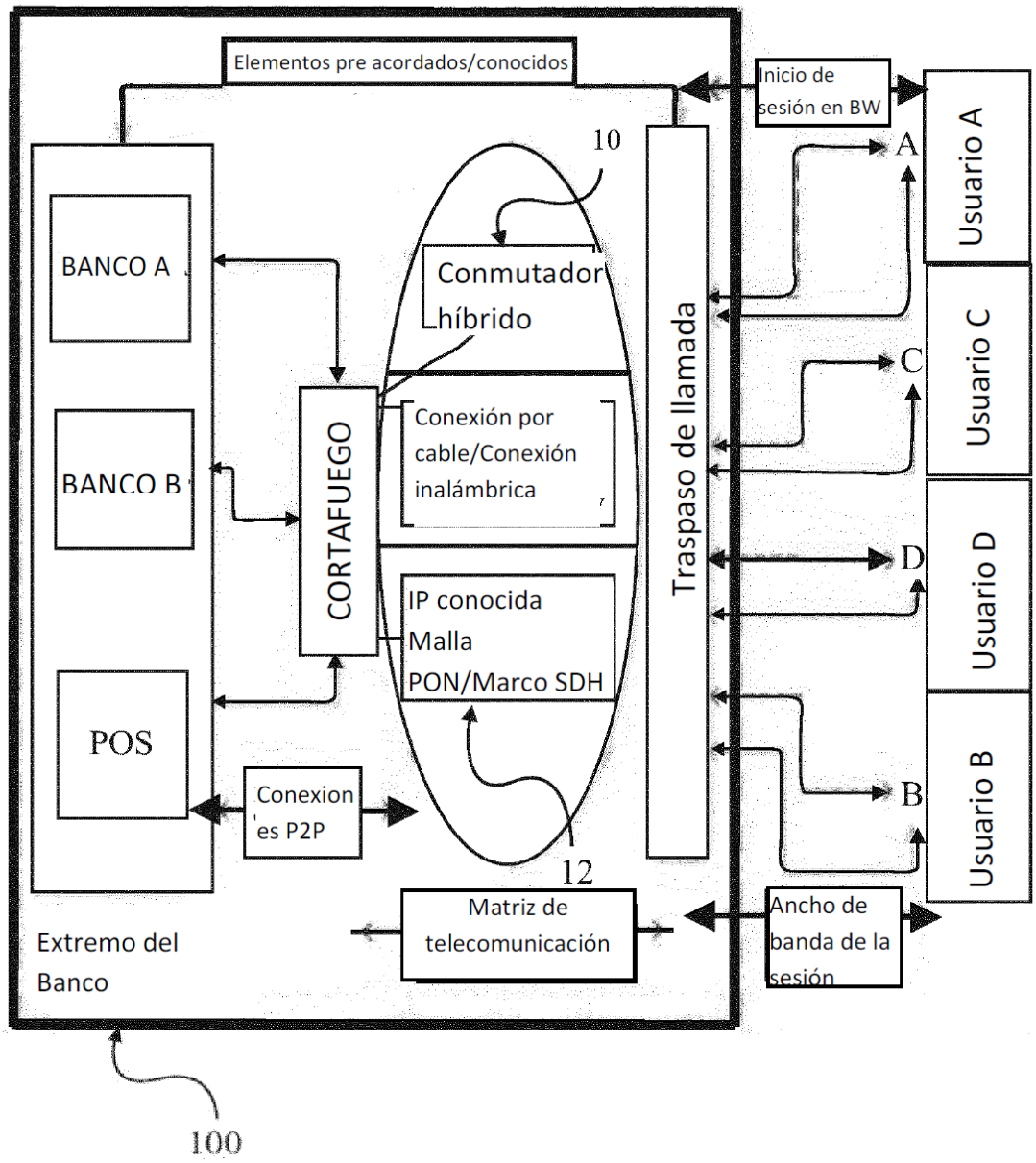
Elementos pre acordados/conocidos
Inicio de sesión en BW
Usuario A
Usuario C
Usuario D
Usuario B
10
BANCO A
BANCO B
POS
Conmutador híbrido
Conexión por cable/Conexión inalámbrica
IP conocida Malla PON/Marco SDH
CORTAFUEGO
Traspaso de llamada
A
C
D
B
Conexion es P2P
12
Matriz de telecomunicación
Ancho de banda de la sesión
Extremo del Banco
100

FIGURA 2C

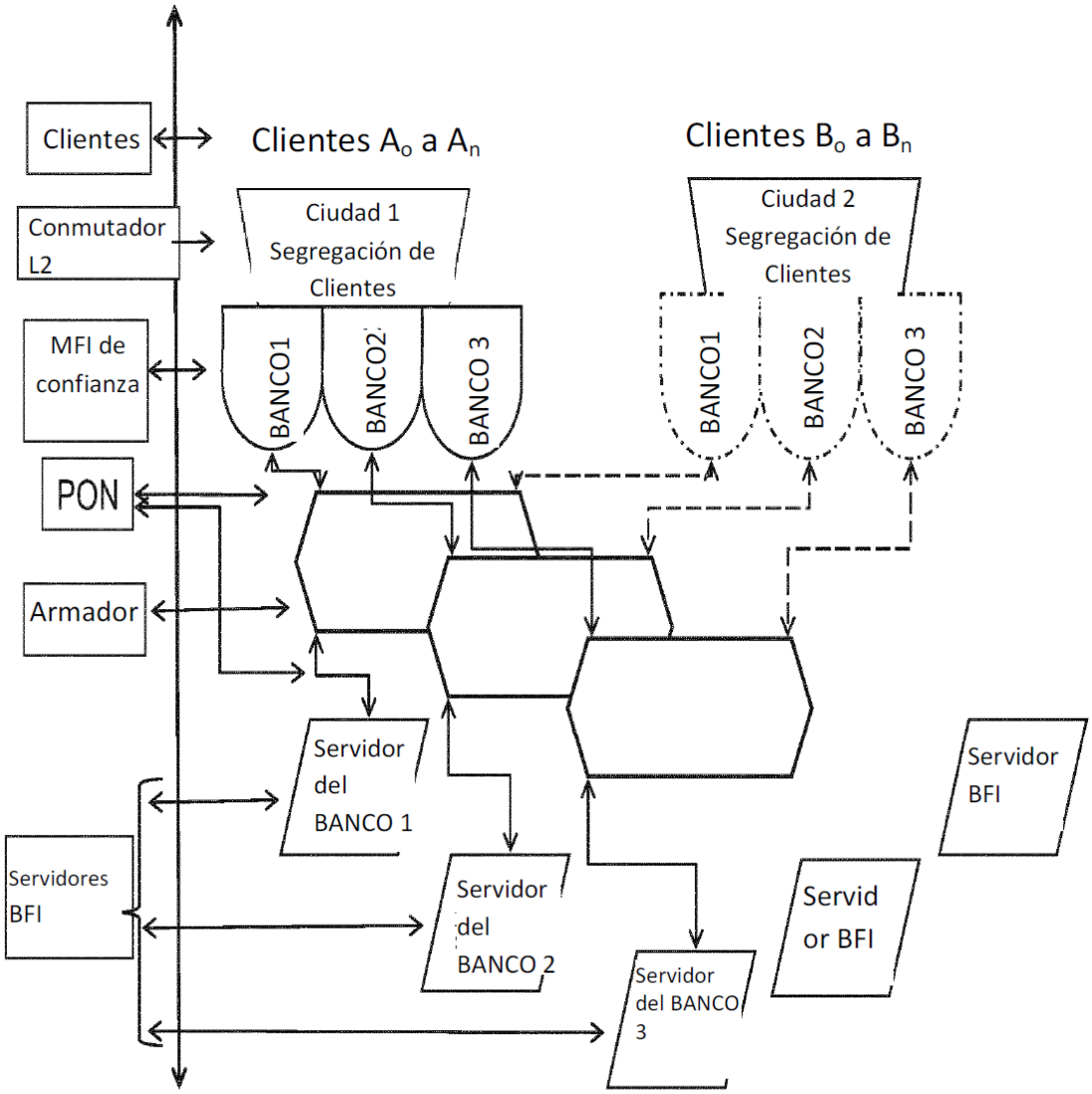
Clientes
Clientes A_o a A_n
Clientes B_o a B_n
Conmutador L2
Ciudad 1 Segregación de Clientes
Ciudad 2 Segregación de Clientes
MFI de confianza
BANCO1
BANCO2
BANCO 3
BANCO1
BANCO2
BANCO 3
PON
Armador
Servidor del BANCO 1
Servidor BFI
Servidores BFI
Servidor del BANCO 2
Servid or BFI
Servidor del BANCO 3

FIGURA 3

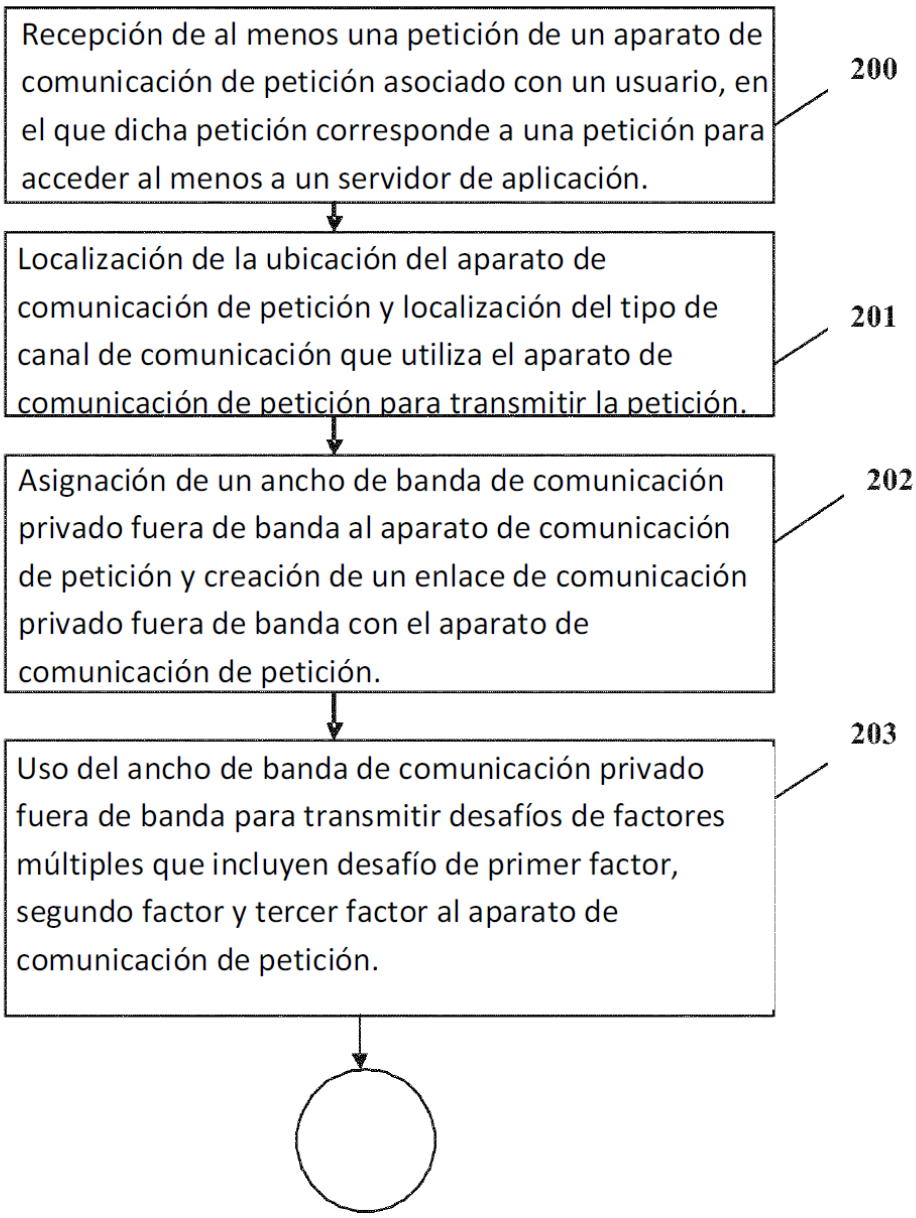
Recepción de al menos una petición de un aparato de comunicación de petición asociado con un usuario, en el que dicha petición corresponde a una petición para acceder al menos a un servidor de aplicación.
200
Localización de la ubicación del aparato de comunicación de petición y localización del tipo de canal de comunicación que utiliza el aparato de comunicación de petición para transmitir la petición.
201
Asignación de un ancho de banda de comunicación privado fuera de banda al aparato de comunicación de petición y creación de un enlace de comunicación privado fuera de banda con el aparato de comunicación de petición.
202
Uso del ancho de banda de comunicación privado fuera de banda para transmitir desafíos de factores múltiples que incluyen desafío de primer factor, segundo factor y tercer factor al aparato de comunicación de petición.
203

FIGURA 4A

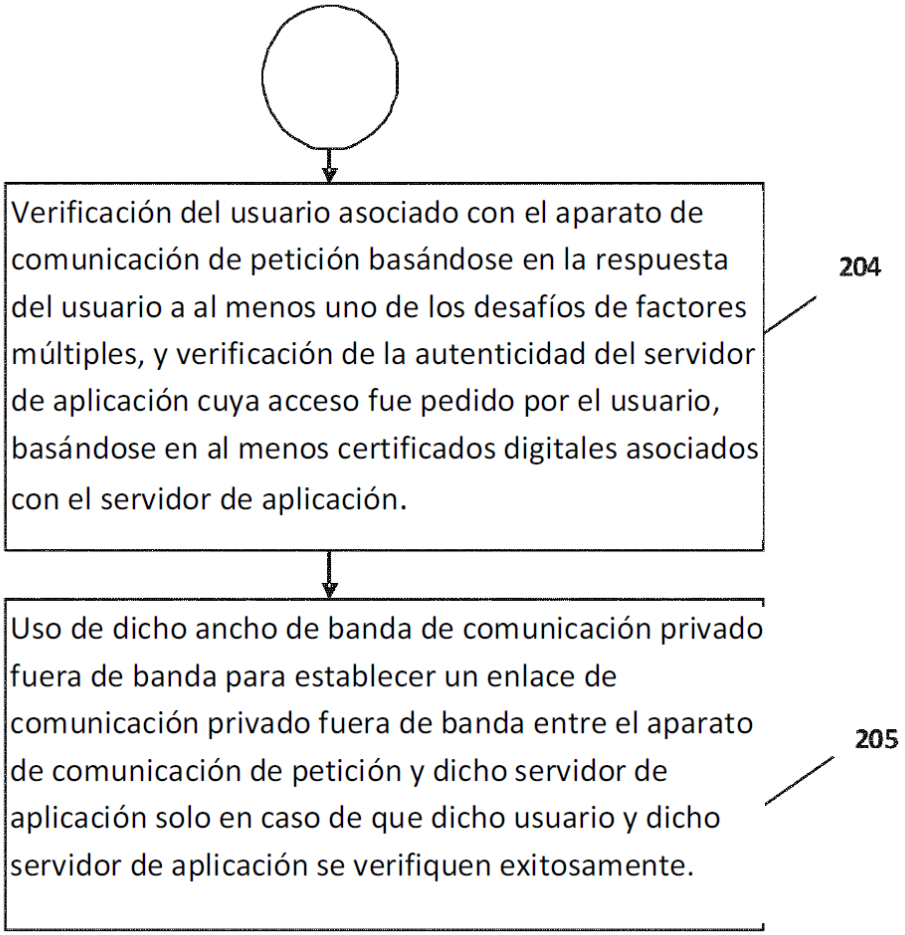
Verificación del usuario asociado con el aparato de comunicación de petición basándose en la respuesta del usuario a al menos uno de los desafíos de factores múltiples, y verificación de la autenticidad del servidor de aplicación cuya acceso fue pedido por el usuario, basándose en al menos certificados digitales asociados con el servidor de aplicación.
204
Uso de dicho ancho de banda de comunicación privado fuera de banda para establecer un enlace de comunicación privado fuera de banda entre el aparato de comunicación de petición y dicho servidor de aplicación solo en caso de que dicho usuario y dicho servidor de aplicación se verifiquen exitosamente.
205

FIGURA 4B

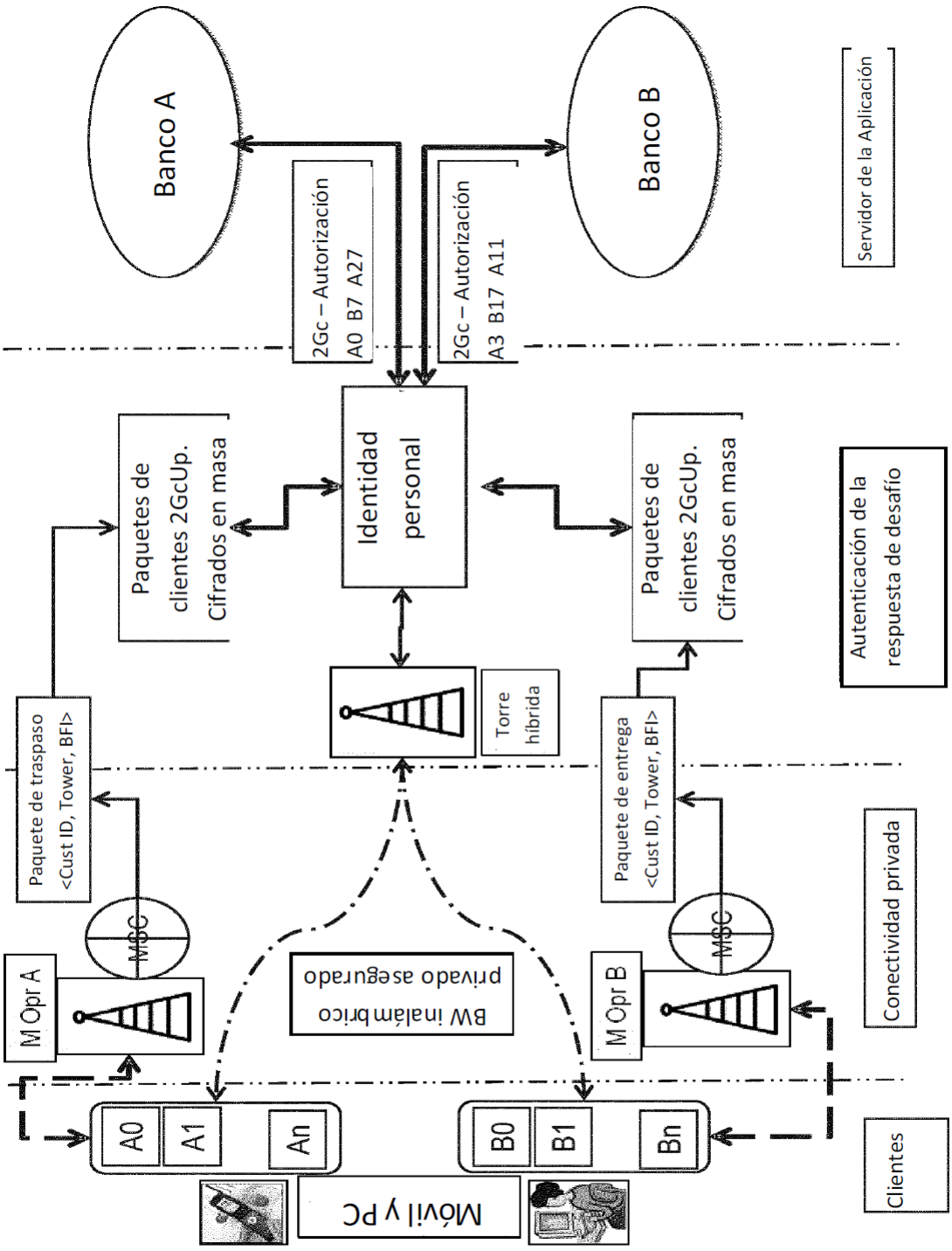
Banco A
Banco B
Servidor de la Aplicación
2Gc – Autorización A0 B7 A27
2Gc – Autorización A3 B17 A11
Identidad personal
Paquetes de clientes 2GcUp. Cifrados en masa
Paquetes de clientes 2GcUp. Cifrados en masa
Autenticación de la respuesta de desafío
Torre híbrida
Paquete de traspaso <Cust ID, Tower, BFI>
Paquete de entrega <Cust ID, Tower, BFI>
M Opr A
M Opr B
MSC
MSC
BW inalám brico privado asegurado
Conectividad privada
A0
A1
An
B0
B1
Bn
Móvil y PC
Clientes

FIGURA 5