(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 717 100**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 29/12 (2006.01)
G06Q 20/12 (2012.01)
G06Q 20/32 (2012.01)
G06Q 20/42 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **03.06.2014 PCT/EP2014/061519**

(87) Fecha y número de publicación internacional: **11.12.2014 WO14195332**

(96) Fecha de presentación y número de la solicitud europea: **03.06.2014 E 14736300 (6)**

(97) Fecha y número de publicación de la concesión europea: **20.02.2019 EP 3005651**

(54) Título: **Procedimiento de direccionamiento, autentificación y almacenamiento seguro de datos en sistemas informáticos**

(30) Prioridad:

05.06.2013 DE 102013105781

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.06.2019

(73) Titular/es:

SOMMER, RALF (100.0%)
Alte Rainsmühle 1
36391 Sinntal-Oberzell, DE

(72) Inventor/es:

SOMMER, RALF

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento de direccionamiento, autentificación y almacenamiento seguro de datos en sistemas informáticos

La invención se refiere a un procedimiento con el que se posibilita el direccionamiento seguro y la autentificación para el establecimiento de conexiones, así como el almacenamiento seguro de datos y la prevención de la divulgación de datos a terceros. Además, la invención permite el pago seguro a través de conexiones de datos. Por lo tanto, se refiere en particular con un procedimiento de direccionamiento, autentificación y almacenamiento de datos para redes de "Nube Privada" y a un pago seguro a través de conexiones de datos.

De acuerdo con el estado actual de la técnica, actualmente existen dos procedimientos comunes para el direccionamiento de sistemas informáticos en Internet, en concreto el servicio DNS o el direccionamiento de direcciones IP asignadas de forma fija. Las direcciones IP dinámicas, asignadas por la mayoría de los proveedores de servicios de Internet a los dispositivos de clientes, solo pueden ser utilizadas para el direccionamiento de un sistema informático determinado dando un rodeo por servicios de Internet (por ejemplo, DynDNS.org, NoIP.com, Selfhost.de, TZODNS.com o servicios de DNS dinámico del proveedor de servicios de Internet). En este contexto, por un sistema informático se ha de entender, por ejemplo, un enrutador de Internet, un teléfono inteligente, un servidor, un ordenador personal, un ordenador portátil, una agenda electrónica, una tableta PC, etc.

Los procedimientos anteriormente mencionados permiten que los atacantes potenciales de Internet ataquen los sistemas informáticos a través de DNS o de la dirección IP. En caso dado se puede obtener el control de los sistemas informáticos, o se pueden llevar a cabo los, así llamados, ataques DOS (Denegación de Servicio) en estos sistemas informáticos. En el caso de servicios DNS dinámicos también es posible un robo de los datos de acceso para el servicio DNS dinámico. De este modo, un atacante tendría la posibilidad de desviar la dirección DNS dinámica a otro sistema informático, para después espiar los accesos de los usuarios a esta dirección.

Si bien se conoce la transmisión de la dirección IP a través de una conexión telefónica, en este contexto no se puede descartar la utilización una identificación de llamada (número de teléfono) falsa. Sin embargo, este uso indebido no es reconocible, por lo que la transmisión de la dirección IP no es segura. Para la autentificación, actualmente se utilizan por regla general un nombre de usuario y una contraseña. En las operaciones bancarias se utilizan además tarjetas inteligentes y contraseñas de un solo uso, llamadas TAN o smsTAN. La desventaja de la autentificación mediante nombre de usuario y contraseña consiste en que el usuario ha de crear nombres de usuario y contraseñas propios para diferentes sistemas de destino. A menudo, con el fin de reducir el número de contraseñas se crea una contraseña común para diferentes sistemas de destino.

Con ello surge el problema de que, mediante el robo de esta contraseña común, un atacante puede acceder a varios sistemas de destino del usuario, por ejemplo para manipular o espiar datos o para realizar compras en nombre y por cuenta del usuario. Además, por regla general, el usuario no tiene forma de verificar con qué seguridad se almacenan los datos de acceso en el sistema de destino respectivo.

Las tarjetas inteligentes y las contraseñas de un solo uso (TAN/smsTAN) para operaciones bancarias también pueden ser objeto de uso indebido por medio de procedimientos técnicos. Ya existen casos conocidos en los que se han interceptado smsTAN y se ha hecho un uso indebido de las mismas. En las conexiones inalámbricas, como por ejemplo NFC, Bluetooth, WLAN, etc., existe el peligro de que el establecimiento de la conexión y la transmisión inalámbrica sean interceptados por atacantes. Como resultado de ello, existen numerosas posibilidades de ataque para acceder a los sistemas informáticos o para hacer un uso indebido de los datos.

De acuerdo con el estado actual de la técnica, con frecuencia se almacenan datos de usuarios en varios sistemas informáticos ajenos. Así, para comprar a través de Internet, por regla general se han de almacenar el nombre de usuario, la contraseña y los datos de la cuenta o de la tarjeta de crédito en el comercio en línea respectivo. En las redes sociales se transfieren en gran medida datos personales y privados a un sistema informático ajeno, en parte incluso con la condición de que el operador de la red social pueda utilizar estos datos. Sin embargo, continuamente se dan a conocer casos en los que piratas informáticos han robado datos de usuarios y han hecho un uso indebido de los mismos. Por ejemplo, en mayo de 2011, en un ataque de piratas informáticos a sistemas de procesamiento de datos de la firma Sony se robaron millones de datos personales, entre otras cosas también contraseñas y números de tarjetas de crédito.

En los procesos de pago a través de Internet, por regla general se han de transmitir datos de la cuenta o de la tarjeta de crédito al vendedor o a la tienda en línea. En la mayoría de los casos, estos datos se almacenan en los sistemas informáticos del vendedor. También en este caso, el usuario generalmente no tiene forma de verificar con qué seguridad se almacenan los datos en los sistemas informáticos del vendedor. Existen muchos casos en los que estos datos han sido robados y se ha hecho un uso indebido de los mismos. Los datos han sido robados tanto por atacantes ajenos estas empresas como por atacantes pertenecientes a éstas.

La presente invención tiene por objetivo superar las desventajas del estado anterior de la técnica arriba descrito y proporcionar un procedimiento que sea especialmente simple y económico de realizar y con el que se posibilite un direccionamiento y una autentificación seguros para conexiones entre diferentes sistemas informáticos tales como, por ejemplo, enrutadores de Internet, teléfonos inteligentes, servidores, ordenadores personales, etc., así como un

almacenamiento seguro de datos personales, con el fin de evitar una divulgación de datos a terceros. Además, la invención quiere posibilitar un pago seguro para compras en línea en Internet o compras en tiendas.

Este objetivo se logra de la siguiente manera: los sistemas informáticos, además de comunicarse a través de una interfaz de red, es decir, por ejemplo una interfaz de Ethernet, NFC, Bluetooth, WLAN, LAN, también se comunican a través de una interfaz de telefonía con número de llamada asociado. El procedimiento según la invención sirve para el direccionamiento, la autentificación y el almacenamiento seguro de datos en sistemas informáticos con al menos una interfaz de red y al menos una interfaz de telefonía, así como con al menos un espacio de memoria para información de gestión, en particular para números de llamada autorizados y PIN de abonados, de tal modo que los sistemas informáticos están programados con un programa que reproduce una lógica de control para controlar la interacción de las interfaces arriba mencionadas. El procedimiento comprende al menos las etapas consistentes en:

a) transmitir la información de conexión para la interfaz de red de un primer sistema informático a través de la interfaz de telefonía a un segundo sistema informático;

b) comprobar automáticamente un número de llamada del primer sistema informático con los números de llamada almacenados en el al menos un espacio de memoria en el segundo sistema informático y, si el resultado de la prueba es positivo, transmitir automáticamente al primer sistema informático la información de conexión para la interfaz de red del segundo sistema informático a través de la interfaz de telefonía y activar la interfaz de red del segundo sistema informático para aceptar conexiones sobre la base de la información de conexión del primer sistema informático;

c) comprobar el número de llamada del segundo sistema informático con los números de llamada almacenados en el al menos un espacio de memoria en el primer sistema informático y, si el resultado de la prueba es positivo, activar la interfaz de red del primer sistema informático para establecer una conexión sobre la base de la información de conexión del segundo sistema informático; en donde

d) la interfaz de red del segundo sistema informático está configurada de tal modo que solo están autorizadas conexiones con la información de conexión del primer sistema informático, y

e) la interfaz de red del primer sistema informático está configurada de tal modo que solo se autorizan conexiones con la información de conexión del segundo sistema informático, y

f) las interfaces de red del primer y del segundo sistema informático solo autorizan intentos de conexión con la información de conexión respectiva durante un breve período de tiempo predeterminado y, después del establecimiento de la conexión o después de la expiración del período de tiempo predeterminado sin que se haya establecido ninguna conexión, no son reconocibles ni accesibles para otros sistemas informáticos.

Gracias a la asignación claramente definida y la autentificación mutua a través de números de llamada o información del usuario almacenados, no se puede producir un uso indebido, por ejemplo mediante la utilización de números de llamada y/o direcciones IP falsos u obtenidos indebidamente de algún otro modo.

El procedimiento también se puede utilizar en sistemas con tres sistemas informáticos. Si, en una variante preferente del procedimiento, dos sistemas informáticos previstos para la comunicación ya están conectados con un tercer sistema informático y si se ha de establecer a través de la lógica de control en el tercer sistema informático una conexión directa a través de la interfaz de red, el procedimiento comprende ventajosamente las etapas adicionales consistentes en:

g) transmitir al segundo sistema informático la información de conexión para la interfaz de telefonía y la interfaz de red del primer sistema informático con un mensaje de sistema a través de la conexión existente con el tercer sistema informático;

h) comprobar un número de llamada del primer sistema informático con números de llamada almacenados en el espacio de memoria en el segundo sistema informático y, si el resultado de la prueba es positivo, transmitir al primer sistema informático la información de conexión para la interfaz de telefonía y la interfaz de red del segundo sistema informático a través de la conexión existente con el tercer sistema informático, y activar la interfaz de red del segundo sistema informático para aceptar conexiones sobre la base de la información de conexión del primer sistema informático, e

i) comprobar el número de llamada del segundo sistema informático con los números de llamada almacenados en el espacio de memoria en el primer sistema informático y, si el resultado de la prueba es positivo, activar la interfaz de red del primer sistema informático para establecer conexiones sobre la base de la información de conexión del segundo sistema informático;

en donde

j) la interfaz de red del segundo sistema informático solo autoriza conexiones con la información de conexión del primer sistema informático,

k) la interfaz de red del primer sistema informático solo autoriza conexiones con la información de conexión del segundo sistema informático, y

l) las interfaces de red del primer y del segundo sistema informático solo autorizan intentos de conexión con la información de conexión respectiva durante un breve período de tiempo predeterminado y, después del establecimiento de la conexión o después de la expiración del período de tiempo predeterminado sin que se haya establecido ninguna conexión, no son reconocibles ni accesibles para otros sistemas informáticos.

El procedimiento se perfecciona ventajosamente de la siguiente manera: en las etapas b) y/o h) se activa la interfaz de red del segundo y/o del tercer sistema informático para establecer conexiones sobre la base de la información de conexión del primer sistema informático, y en las etapas c) y/o i) se activa la interfaz de red del primer sistema informático para aceptar conexiones sobre la base de la información de conexión del segundo y/o del tercer sistema informático.

En una variante del procedimiento que se considera favorable está previsto que, después del establecimiento de la conexión, el segundo y/o el tercer sistema informático soliciten una identificación del primer sistema informático, que la comparen con las etiquetas de identificación almacenadas en el espacio de memoria del segundo y/o del tercer sistema informático y, si el resultado de la prueba es positivo, que la conexión permanezca activada y, si el resultado de la prueba es negativo, que la conexión se cierre y, en particular, que se emita un aviso de alarma.

El procedimiento también se perfecciona de la siguiente manera: después de un número configurable, en particular entre 1 y 15, preferiblemente entre 2 y 12, de forma particularmente preferible entre 3 y 10 intentos de identificación negativos, la lógica de control marca como bloqueado el número de llamada del primer sistema informático en el espacio de memoria del segundo y/o del tercer sistema informático y ya no se acepta ninguna información de conexión más para el primer sistema informático con este número de llamada.

De acuerdo con la invención está previsto que la etiqueta de identificación consista en un texto, un identificador biométrico, una llave electrónica o una llave mecánica, cuya información clave se lee mediante un dispositivo de lectura en el primer sistema informático.

En una forma de realización preferente del procedimiento está previsto que el primer sistema informático suministre un testigo de seguridad junto con la información de conexión al segundo y/o al tercer sistema informático, y que dicho testigo de seguridad se transmita durante el establecimiento de la conexión a través de la interfaz de red y se compruebe en respuesta mediante la lógica de control en el primer sistema informático y, si el resultado de la prueba es positivo, que la conexión permanezca activada y, si el resultado de la prueba es negativo, que la conexión se cierre y se emita un aviso de alarma.

Se considera ventajoso que, después de un número predeterminado de intentos de conexión negativos, la lógica de control marque como bloqueado el número de llamada del segundo y/o del tercer sistema informático en el espacio de memoria del primer sistema informático y ya no se acepte ningún intento de conexión para el segundo y/o el tercer sistema informático con este número de llamada.

Resulta ventajoso que un primer y un segundo sistema informático, que ya están conectados con un tercer sistema informático y han establecido una conexión directa, solo se autentifiquen entre sí a través del tercer sistema informático común y que, en este contexto, el procedimiento comprenda las siguientes etapas adicionales:

m) el primer sistema informático solicita un testigo de seguridad al tercer sistema informático a través de la conexión y lo envía al segundo sistema informático a través de la conexión directa;

n) el segundo sistema informático transmite el testigo de seguridad al tercer sistema informático a través de la conexión;

o) el tercer sistema informático compara los dos testigos de seguridad y envía en cada caso un mensaje de sistema con el resultado de la comparación al primer y al segundo sistema informático, y

p) la lógica de control respectiva del primer y del segundo sistema informático comprueba el mensaje de sistema con el resultado de la comparación y, si el resultado de la prueba es positivo, deja abierta la conexión y, si el resultado de la prueba es negativo, cierra la conexión directa y emite un mensaje de alarma.

De acuerdo con una forma de realización del procedimiento anteriormente descrito, un primer y un segundo sistema informático están previstos respectivamente para realizar un proceso de pago de un comprador a través de un primer sistema informático y de un vendedor a través de un segundo sistema informático. El proceso de pago también se puede realizar por ejemplo a través de un tercer sistema informático, por ejemplo un servicio de pago. En esta variante, el procedimiento comprende ventajosamente las etapas adicionales, en las que

q) la lógica de control en el sistema informático del vendedor genera un testigo de seguridad, y el comprador o el sistema informático del comprador recibe a través de la conexión directa el testigo de seguridad, preferiblemente junto con una información de pago, procedente del vendedor o del sistema informático del vendedor;

r) el vendedor o el sistema informático del vendedor transmite la información de pago junto con el testigo de seguridad a través de la conexión a un servicio de pago o a un sistema informático del servicio de pago;

s) el comprador o el sistema informático del comprador transmite la información de pago junto con el testigo de seguridad a través de la conexión a un servicio de pago o al sistema informático del servicio de pago;

t) el comprador o el sistema informático del comprador autoriza el proceso de pago a través de la conexión en el servicio de pago o en el sistema informático del servicio de pago con un PIN o similar, y

u) una lógica de control en el servicio de pago o en el sistema informático del servicio de pago compara el testigo de seguridad del vendedor o del sistema informático del vendedor y del comprador o del sistema informático del comprador y valida el PIN del comprador o del sistema informático del comprador y, si el resultado de la prueba es positivo, concluye el proceso de pago y envía de vuelta un mensaje de sistema positivo al vendedor o al sistema informático del vendedor y al comprador o al sistema informático del comprador. En cambio, si el resultado de la prueba es negativo, el proceso de pago se cancela y se envía un mensaje de sistema negativo al vendedor o al sistema informático del vendedor y al comprador o al sistema informático del comprador.

El procedimiento tal como se describe más arriba se perfecciona de la siguiente manera: la conexión para el proceso de pago entre el vendedor o el sistema informático del vendedor y el comprador o el sistema informático del comprador en una tienda o similar se establece a través de NFC, Bluetooth, LAN inalámbrica o LAN por cable.

En este contexto resulta ventajoso que la información de pago para el proceso de pago entre el vendedor o el sistema informático del vendedor y el comprador o el sistema informático del comprador en una tienda o en una tienda en línea se transmita, en lugar de a través de una conexión directa, a través de una señal óptica (por ejemplo código Q/R, código de barras, secuencias de caracteres, ...), una señal acústica (por ejemplo tonos de módem, voz, ...) o mediante introducción manual entre el vendedor o el sistema informático del vendedor y el comprador o el sistema informático del comprador. En el caso de la compra en línea también se puede utilizar un segundo dispositivo (1a2 - por ejemplo un teléfono inteligente) para recibir y transmitir la información de pago de un primer dispositivo (1a1 - por ejemplo un PC o un ordenador portátil). El primer dispositivo (por ejemplo un PC o un ordenador portátil) asume en este contexto la función de un terminal del vendedor o del sistema informático del vendedor.

En un perfeccionamiento ventajoso del procedimiento está previsto que la lógica de control también pueda transmitir, por ejemplo a través de conexiones de red existentes que no han sido creadas tal como se ha indicado anteriormente, los datos para el proceso de pago entre el vendedor o el sistema informático del vendedor y el servicio de pago o el sistema informático del servicio de pago, o entre el comprador o el sistema informático del comprador y el servicio de pago o el sistema informático del servicio de pago.

Ventajosamente, para el cifrado, la identificación por PIN, el testigo de seguridad y la autorización se utiliza un texto, un identificador biométrico, una llave electrónica o una llave mecánica, cuya información clave se lee mediante un dispositivo de lectura en los sistemas informáticos.

Resulta ventajoso que, para pequeñas cantidades de datos, en particular para un proceso de pago, la lógica de control transmita al menos una parte de los datos adquiridos en las etapas precedentes a través de la interfaz de telefonía.

También se considera favorable que la lógica de control, con la activación de una señal predeterminada, transmita datos, en particular correos electrónicos, SMS y FAX, a sistemas informáticos sin ayuda de otros servicios de Internet, como DNS y DynDNS.

En una forma de realización del procedimiento está previsto que la lógica de control compruebe automáticamente si el número de llamada mostrado coincide con la línea de abonado real.

En una forma de realización del procedimiento está previsto que las solicitudes de conexión de un primer sistema informático sean distribuidas por la lógica de control en un segundo y/o un tercer sistema informático entre diferentes sistemas informáticos segundo y/o tercero de acuerdo con un criterio predeterminado, en particular un número de conexiones y/o un índice de ocupación y/o una disponibilidad del segundo y/o del tercer sistema informático y/o un número de llamada y/o un emplazamiento geográfico.

En una forma de realización del procedimiento está previsto que un sistema informático en una función de servidor en la red procese mediante la lógica de control solicitudes de conexión o solicitudes de resolución de nombre (por ejemplo, solicitudes DNS, ...) de otros sistemas informáticos en la red, y que la lógica de control del primer sistema informático lleve a cabo el intercambio de la información de conexión con un segundo y/o un tercer sistema informático, realizados tal como se indica más arriba, y a continuación establezca la conexión o envíe de vuelta los parámetros de conexión (por ejemplo dirección IP, número de puerto, ...) a los sistemas informáticos solicitantes.

En una forma de realización del procedimiento está previsto que la lógica de control de un sistema informático también transmita los parámetros de conexión determinados de acuerdo con las reivindicaciones precedentes al menos a otro sistema servidor (por ejemplo cortafuegos,…) y que éste autorice después las conexiones del sistema

informático o de sistemas informáticos de la red con estos parámetros de conexión.

En una forma de realización del procedimiento está previsto que la lógica de control del segundo y/o del tercer sistema informático automáticamente transmita al primer sistema informático o ponga a disposición del mismo información y datos de control en función de la información de conexión.

En una forma de realización del procedimiento está previsto que el número de llamada del segundo y/o del tercer sistema informático se utilice para un servicio de telefonía diferente o existente, en particular un servicio de FAX y/o un contestador automático, y que la lógica de control del segundo y/o del tercer sistema informático compare el número de llamada del primer sistema informático con los números de llamada almacenados en el espacio de memoria del segundo y/o del tercer sistema informático y que, en caso de coincidencia, no active el servicio de telefonía, sino que transmita los datos de conexión para el segundo y/o el tercer sistema informático al primer sistema informático.

En un perfeccionamiento preferente del procedimiento está previsto que el elemento designado como interfaz de telefonía alternativamente también sea proporcionado por medio de señales ópticas (por ejemplo código Q/R, código de barras, secuencias de caracteres), señales acústicas (por ejemplo, tonos de módem, voz), mediante entradas manuales o mediante conexiones seguras establecidas previamente de otro modo (por ejemplo NFC, Bluetooth, WLAN, USB,...) con el mismo efecto. Para los sistemas informáticos 1, 1a, 1a1, 1a2, 1b geográficamente cercanos entre sí, la información de conexión para la interfaz de red 11 se puede transmitir entonces a través de estas señales ópticas (por ejemplo código Q/R, código de barras, secuencias de caracteres), señales acústicas (por ejemplo tonos de módem, voz, o similares), entradas manuales o mediante conexiones seguras establecidas previamente de otro modo (por ejemplo NFC, Bluetooth, WLAN, USB) entre los sistemas informáticos 1, 1a, 1a1, 1a2, 1b. Entonces preferiblemente también puede tener lugar una transmisión bidireccional.

De acuerdo con la invención también está prevista la utilización del procedimiento anteriormente descrito con protocolos de otras interfaces orientadas a la conexión, en particular con protocolos NFC, Bluetooth y WLAN.

Mediante una lógica de control para la interacción de interfaces de telefonía y de red, la invención proporciona una variante nueva y segura para establecer conexiones entre sistemas informáticos, en especial también en el campo de la comunicación inalámbrica como NFC, Bluetooth, WLAN, etc. Muchos de los sistemas informáticos anteriormente mencionados tienen ya tienen actualmente los dos tipos de conexión, es decir, interfaces de telefonía y de red, o se pueden equipar con éstas por medio de módulos adicionales en *hardware* y/o *software*.

Un aspecto esencial de la solución según la invención consiste en que, para el direccionamiento y la autentificación se transmite una parte de la información de conexión a través del sistema de telefonía. La información de conexión puede consistir, por ejemplo, en direcciones TCP/IP, puertos TCP/IP, nombres de usuario, emplazamientos, etc. Para ello, la invención utiliza los respectivos protocolos y servicios de telefonía, como por ejemplo en caso de RDSI el canal D, una conexión de sonido/módem, SMS y/o servicios de FAX. Los sistemas informáticos anteriormente mencionados utilizan esta información de conexión para comprobar si los datos han sido transmitidos con un número de llamada autorizado. A continuación, después de un resultado positivo de la prueba, se puede establecer una conexión de datos.

Para los sistemas informáticos que solo disponen de una dirección IP dinámica o para sistemas inalámbricos, la invención ofrece una nueva posibilidad de acceder a estos sistemas informáticos sin ayuda de un servicio adicional, como por ejemplo DynDNS o procedimientos de establecimiento de conexiones inalámbricas vulnerables. Para sistemas informáticos sin requisitos de seguridad especiales, como por ejemplo páginas de información de una empresa, este procedimiento también se puede utilizar sin autentificación adicional para posibilitar accesos a estos sistemas informáticos.

Otro aspecto esencial de la solución según la invención también consiste en que los oyentes de la interfaz de red solo se activan durante un breve período de tiempo (unos pocos segundos) y solo reaccionan a los datos de conexión que previamente han sido transmitidos a través de la interfaz de telefonía. En este contexto, por un oyente se ha de entender una interfaz o servicio con el que un sistema informático puede establecer una conexión. Después del establecimiento de la conexión o después de la expiración de un período de tiempo predeterminado ("tiempo de espera") sin que se haya establecido ninguna conexión, los sistemas informáticos no son reconocibles ni accesibles para otros sistemas informáticos.

Una comprobación de los números de llamada del sistema informático respectivo por medio de la lógica de control ofrece una preselección adicional de accesos autorizados. Mediante la marcación mutua de los números de llamada por medio de los sistemas informáticos también se puede evitar que un número de llamada transmitido que no coincida con un abonado conduzca al establecimiento de una conexión. Esto evita en la mayor medida posible los intentos de acceso no autorizado por parte de atacantes a través de la interfaz de telefonía o la interfaz de red.

Además, en caso de instalaciones mayores, a través de la lógica de control puede tener lugar una distribución de sistemas informáticos entre diferentes segundos sistemas informáticos según un criterio predeterminado, como por ejemplo el número de conexiones, el índice de ocupación, la disponibilidad de los segundos sistemas informáticos, el número de llamada y/o un emplazamiento geográfico.

Mediante la evaluación de los datos geográficos o relacionados con el emplazamiento a partir de los datos de conexión, la lógica de control de un sistema informático puede seleccionar una conexión óptima, como por ejemplo Bluetooth, WLAN, Internet, etc., o permitir al usuario seleccionar las posibles conexiones.

La invención proporciona al menos tres procedimientos para establecer la conexión, que se explicarán más abajo con mayor detalle con referencia a las figuras adjuntas. Las partes iguales o equivalentes están provistas de las mismas referencias numéricas.

Se muestran:

la Figura 1 una representación esquemática de una conexión cliente-servidor según la invención con un servidor y un cliente;

la Figura 2 muestra una representación esquemática de una conexión cliente-servidor según la invención con un servidor y dos clientes; y

la Figura 3 muestra una representación esquemática de una conexión cliente-servidor según la invención con dos clientes para explicar un proceso de compra.

La figura 1 muestra una representación esquemática de una conexión cliente-servidor según la invención, con un servidor 1, 1b, previamente designado también como segundo y/o tercer sistema informático en el sentido de la invención, y un cliente 1, 1a, previamente designado también como primer sistema informático en el sentido de la invención. La conexión del servidor se establece mediante una lógica de control 10, en la que el primer sistema informático 1a transmite inicialmente la información de conexión del primer sistema informático 1a al segundo sistema informático 1b por medio de una interfaz de telefonía 12 y una primera conexión 101 a través de la red telefónica 4. El segundo sistema informático 1b, después de una comprobación con resultado positivo, transmite la información de conexión del segundo sistema informático 1b al primer sistema informático 1a a través de una segunda conexión 102. Después de una comprobación con resultado positivo, el primer sistema informático 1a activa una interfaz de red 11. La interfaz de red 11 del primer sistema informático 1a solo permanece activa hasta la tercera conexión 103 del segundo sistema informático 1b o hasta la expiración de un tiempo de espera. El segundo sistema informático 1b establece la tercera conexión 103 con la interfaz de red 11 del primer sistema informático 1a. Cuando el segundo sistema informático 1b lo solicita, el primer sistema informático 1a transmite un PIN.

La conexión del cliente tiene lugar entonces de tal modo que el primer sistema informático 1a transmite la información de conexión del primer sistema informático 1a al segundo sistema informático 1b a través de una primera conexión 101. El segundo sistema informático 1b transmite al primer sistema informático 1a, después de una comprobación con resultado positivo, la información de conexión del segundo sistema informático 1b a través de una segunda conexión 102. El segundo sistema informático 1b activa la interfaz de red 11, que solo permanece activa hasta la cuarta conexión 104 del primer sistema informático 1a o hasta la expiración de un tiempo de espera. El primer sistema informático 1a, después de una comprobación con resultado positivo, establece la cuarta conexión 104 con la interfaz de red 11 del segundo sistema informático 1b. Cuando el segundo sistema informático 1b lo solicita, el primer sistema informático 1a transmite un PIN.

La figura 2 muestra una representación esquemática de una conexión cliente-servidor según la invención con un tercer sistema informático designado como servidor 1, 1b y dos sistemas informáticos designados como clientes 1, 1a1, 1, 1a2, en concreto un primer 1, 1a1 y un segundo sistema informático 1, 1a2. Un primer sistema informático 1, 1a1 quiere establecer una conexión 203 con un segundo sistema informático 1, 1a2. Los dos sistemas informáticos 1, 1a1, 1, 1a2 ya están conectados con un tercer sistema informático 1, 1b común a través de una conexión 200 existente. Los dos sistemas informáticos 1, 1a1, 1, 1a2 ya han recibido desde este tercer sistema informático 1, 1b común al menos una parte de la información de conexión respectiva a través de un mensaje de sistema del tercer sistema informático 1, 1b.

El primer sistema informático 1, 1a1 envía un mensaje de sistema con la información de conexión completa del primer sistema informático 1, 1a1 al segundo sistema informático 1, 1a2 a través del tercer sistema informático 1, 1b. El segundo sistema informático 1, 1a2, después de una comprobación con resultado positivo, envía de vuelta a través del tercer sistema informático 1, 1b la información de conexión completa (con testigo de seguridad opcional) del segundo sistema informático 1, 1a2 y espera la conexión directa del primer sistema informático 1, 1a1 a través de la interfaz de red 11. Por último, el segundo sistema informático 1, 1a2 activa la interfaz de red 11.

La interfaz de red 11 del segundo sistema informático 1, 1a2 solo permanece activa hasta la conexión 203 del primer sistema informático 1, 1a1 o hasta la expiración de un tiempo de espera. El primer sistema informático 1, 1a1, después de una comprobación con resultado positivo, establece la conexión directa 203 con el segundo sistema informático 1, 1a2, en caso dado suministrando el primer sistema informático 1, 1a1 al mismo tiempo el testigo de seguridad opcional, que es comprobado por el segundo sistema informático 1, 1a2. Opcionalmente, el segundo sistema informático 1, 1a2 puede solicitar la introducción de un PIN para el primer sistema informático 1, 1a1.

Las ventajas de este procedimiento consisten, entre otras cosas, en la posibilidad de una restricción de acceso a números de llamada previamente registrados. Además, la interfaz de red 11 solo está activa durante un tiempo

breve y solo responde a los datos de conexión transmitidos a través de la interfaz de telefonía 12, como por ejemplo direcciones IP, puertos, datos de interfaz para NFC, Bluetooth, WLAN, etc. De este modo no es posible ningún acceso no autorizado. En particular, no es posible ningún ataque DOS, ya que la interfaz de red 11 solo está activa durante un tiempo breve y solo responde a datos de conexión previamente transmitidos, como por ejemplo direcciones IP, puertos, datos de interfaz para NFC, Bluetooth, WLAN, etc. Además, tanto el primer como el segundo sistema informático 1a, 1a1, 1a2 y el tercer sistema informático 1, 1b no tienen interfaces de red 11 constantemente activas y, por lo tanto, no son reconocibles ni accesibles para ataques desde Internet. En las conexiones de Personal Private Network Cloud (Nube de Red Privada Personal), en las que solo se conectan en red dispositivos de una persona, no hay ninguna posibilidad de acceso a los datos por parte de terceros.

La Figura 3 muestra una representación esquemática de una conexión cliente-servidor según la invención con dos clientes para explicar un proceso de compra. Para procesos de pago, la invención utiliza una combinación de los procedimientos anteriormente mencionados para establecer una conexión. En este contexto, un sistema informático designado como servicio de pago 1b actúa como tercer sistema informático 1, 1b de los procedimientos anteriormente mencionados, en el que previamente se han de registrar un primer sistema informático designado como vendedor 1a1 y un segundo sistema informático designado como comprador 1a2. Durante el proceso de pago, la lógica de control 10 establece un anillo de comunicación vendedor 1a1 <=> comprador 1a2 <=> servicio de pago 1b <=> vendedor 1a1".

En este contexto, el procedimiento de pago en Internet 3 se desarrolla por ejemplo de tal modo que el comprador 1a2 realiza una compra en una tienda en línea de un vendedor 1a1, en la que se crea un carrito de compras. Para el proceso de pago, el comprador 1a2 se autentifica por teléfono en el servicio de pago 1b, y el vendedor 1a1 transmite un testigo de seguridad y la información de pago para el proceso de pago al comprador 1a2 a través de una conexión de Internet. Posteriormente, el comprador 1a2 autoriza el proceso de pago con un PIN en el servicio de pago 1b y el vendedor 1a1 se autentifica en el servicio de pago 1b. El vendedor 1a1 también transmite el testigo de seguridad y la información de pago al servicio de pago 1b. Por último, el servicio de pago 1b valida el testigo de seguridad del comprador 1a2 y del vendedor 1a1 y el PIN del comprador 1a2. Si el resultado de la prueba es positivo, el servicio de pago 1b envía una respuesta al comprador 1a2 y al vendedor 1a1 para la autorización del pago. El proceso de pago ha concluido.

El procedimiento de pago en una tienda física se desarrolla de tal modo que el comprador 1a2 realiza una compra y se autentifica en el servicio de pago por teléfono (móvil) para el proceso de pago en caja. El vendedor 1a1 transmite un testigo de seguridad para el proceso de pago y la información de pago al comprador 1a2, por ejemplo con NFC, Bluetooth o LAN inalámbrica, en caso dado también a través de LAN por cable. El comprador 1a2 autoriza el proceso de pago con un PIN en el servicio de pago 1b y el vendedor 1a1 se autentifica en el servicio de pago 1b. El vendedor 1a1 también transmite el testigo de seguridad y la información de pago al servicio de pago 1b, que a su vez valida el testigo de seguridad de comprador/vendedor 1a1, 1a2 y el PIN del comprador 1a2. Si resultado de la prueba es positivo, el servicio de pago 1b envía una respuesta al comprador 1a2 y al vendedor 1a1 para la autorización del pago, con lo concluye que el proceso de pago. Para el cifrado, la identificación por PIN, el testigo de seguridad y la autorización se puede utilizar un texto, un identificador biométrico, una llave electrónica o una llave mecánica, cuya información clave se lee en los sistemas informáticos 1a, 1a1, 1a2, 1b, por ejemplo mediante un dispositivo de lectura.

Las ventajas de este procedimiento consisten, entre otras cosas, en que a lo largo de todo el procedimiento de pago no se transmite al vendedor 1a1, ni el vendedor 1a1 almacena, ningún dato específico del pago, como el código bancario, el número de cuenta, el número de la tarjeta de crédito, el PIN, etc. En consecuencia, dichos datos no pueden ser robados.

Además, en el servicio de pago 1b han de estar registrados y conectados dos puestos independientes (comprador 1a2 y vendedor 1a1). Esto evita procesos de pago a terceros desconocidos. Por lo tanto, el proceso de pago es seguro tanto para el comprador 1a2 como para el vendedor 1a1. No existe ninguna posibilidad de que terceros influyan en el anillo de comunicación o hagan un uso indebido del mismo de forma desapercibida.

Por lo tanto, la invención proporciona un procedimiento de direccionamiento, autentificación y almacenamiento seguro de datos en sistemas informáticos 1, 1a1, 1a2, 1b con una interfaz de red 11 y una interfaz de telefonía 12 y un espacio de memoria 2 para información de gestión, en particular para números de llamada autorizados y PIN de abonados, de tal modo que los sistemas informáticos 1, 1a1, 1a2, 1b están programados con un programa que reproduce una lógica de control 10 para controlar la interacción de las interfaces 11 arriba mencionadas, y el procedimiento comprende las etapas consistentes en: a) transmitir la información de conexión para la interfaz de red 11 de un primer sistema informático 1a a través de la interfaz de telefonía 12 a un segundo y/o un tercer sistema informático 1b; b) comprobar un número de llamada del primer sistema informático 1a con los números de llamada almacenados en el espacio de memoria 2 en el segundo y/o en el tercer sistema informático 1b y, si el resultado de la prueba es positivo, transmitir al primer sistema informático 1a la información de conexión para la interfaz de red 11 del segundo y/o del tercer sistema informático 1b a través de la interfaz de telefonía 12, y activar la interfaz de red 11 del segundo y/o del tercer sistema informático 1b para aceptar conexiones 104 sobre la base de la información de conexión del primer sistema informático 1a; c) comprobar el número de llamada del segundo y/o del tercer sistema informático 1b con los números de llamada almacenados en el espacio de memoria 2 en el primer sistema

informático 1a y, si el resultado de la prueba es positivo, activar la interfaz de red 11 del primer sistema informático 1a para establecer una cuarta conexión 104 sobre la base de la información de conexión del segundo y/o del tercer sistema informático 1b.

De acuerdo con la invención está previsto que d) la interfaz de red 11 del segundo y/o del tercer sistema informático 1b solo autorice conexiones 104 con la información de conexión del primer sistema informático 1a, y e) la interfaz de red 11 del primer sistema informático 1 solo autorice conexiones 104 con la información de conexión del segundo y/o del tercer sistema informático 1b, y f) las interfaces de red 11 del primer y del segundo y/o del tercer sistema informático 1a, 1b solo autoricen intentos de conexión con la información de conexión respectiva durante un breve período de tiempo predeterminado y, después del establecimiento de la conexión o después de la expiración del período de tiempo predeterminado sin que se haya establecido ninguna conexión, no sean reconocibles ni accesibles para otros sistemas informáticos.

En una forma de realización preferente de la invención está previsto que dos, es decir, en cada caso un primer y un segundo sistema informático 1a1, 1a2 ya estén conectados con un tercer sistema informático 1b, y que el primer y el segundo sistema informático 1a1, 1a2 establezcan a través de la lógica de control 10 en el tercer sistema informático 1b una conexión directa 203 a través de la interfaz de red 11, y que el procedimiento comprenda las etapas adicionales consistentes en: g) transmitir al segundo sistema informático 1a2 la información de conexión para la interfaz de telefonía 12 y la interfaz de red 11 del primer sistema informático 1a1 con un mensaje de sistema 201 a través de la conexión 200 existente con el tercer sistema informático 1b; h) comprobar un número de llamada del primer sistema informático 1a1 con números de llamada almacenados en el espacio de memoria 2 en el segundo sistema informático 1a2 y, si el resultado de la prueba es positivo, transmitir al primer sistema informático 1a1 la información de conexión 202 para la interfaz de telefonía 12 y la interfaz de red 11 del segundo sistema informático 1a2 a través de la conexión 200 existente con el tercer sistema informático 1b, y activar la interfaz de red 11 del segundo sistema informático 1a2 para aceptar conexiones 203 sobre la base de la información de conexión del primer sistema informático 1a1, e i) comprobar el número de llamada del segundo sistema informático 1a2 con los números de llamada almacenados en el espacio de memoria 2 en el primer sistema informático 1a1 y, si el resultado de la prueba es positivo, activar la interfaz de red 11 del primer sistema informático 1a1 para establecer conexiones 203 sobre la base de la información de conexión del segundo sistema informático 1a2.

En esta forma de realización, también está previsto de acuerdo con la invención que j) la interfaz de red 11 del segundo sistema informático 1a2 solo autorice conexiones 203 con la información de conexión del primer sistema informático 1a1; k) la interfaz de red 11 del primer sistema informático 1a1 solo autorice conexiones 203 con la información de conexión del segundo sistema informático 1a2, y l) las interfaces de red 11 del primer y del segundo sistema informático 1a1, 1a2 solo autoricen intentos de conexión, en particular entre 1 y 15, preferiblemente entre 2 y 12 y de forma particularmente preferible entre 3 y 10 intentos de conexión con la información de conexión respectiva durante un breve período de tiempo predeterminado, en particular entre 1 y 10, preferiblemente entre 2 y 7, de forma particularmente preferible entre 3 y 5 segundos, y, después del establecimiento de la conexión o después de la expiración del período de tiempo predeterminado sin que se haya establecido ninguna conexión, no sean reconocibles ni accesibles para otros sistemas informáticos.

En otra forma de realización preferente de la invención está previsto que en las etapas b) y/o h) se active la interfaz de red 11 del segundo y/o del tercer sistema informático 1b, 1a2 para establecer conexiones sobre la base de la información de conexión del primer sistema informático 1a, 1a1, y que en las etapas c) y/o i) se active la interfaz de red 11 del primer sistema informático 1a, 1a1 para aceptar conexiones 103 sobre la base de la información de conexión del segundo y/o del tercer sistema informático 1b, 1a2.

En otra forma de realización preferente de la invención está previsto que el segundo y/o el tercer sistema informático 1b, 1a2 soliciten una identificación del primer sistema informático 1a, 1a1 después del establecimiento de la conexión, que la comparen con las etiquetas de identificación almacenadas en el espacio de memoria 2 del segundo y/o del tercer sistema informático 1b, 1a2 y, si el resultado de la prueba es positivo, que la conexión permanezca activada y, si el resultado de la prueba es negativo, que la conexión se cierre y se emita un aviso de alarma.

En otra forma de realización preferente de la invención está previsto que, después de un número predeterminado de intentos de identificación negativos, la lógica de control marque como bloqueado el número de llamada del primer sistema informático 1a, 1a1 en el espacio de memoria 2 del segundo y/o del tercer sistema informático 1b, 1a2 y ya no se acepte ninguna información de conexión más para el primer sistema informático 1a, 1a1 con este número de llamada.

En otra forma de realización preferente de la invención está previsto que la etiqueta de identificación consista en un texto, un identificador biométrico, una llave electrónica o una llave mecánica, cuya información clave se lee mediante un dispositivo de lectura en el primer sistema informático 1a, 1a1.

En otra forma de realización preferente de la invención está previsto que el primer sistema informático 1a, 1a1 suministre un testigo de seguridad junto con la información de conexión al segundo y/o al tercer sistema informático 1b, 1a2, y que dicho testigo de seguridad se transmita durante el establecimiento de la conexión a través de la interfaz de red 11 y se compruebe mediante la lógica de control 10 en el primer sistema informático 1a, 1a1 y, si el

resultado de la prueba es positivo, que la conexión permanezca activada y, si el resultado de la prueba es negativo, que la conexión se cierre y se emita un aviso de alarma.

En otra forma de realización preferente de la invención está previsto que, después de un número predeterminado de intentos de conexión negativos, la lógica de control 10 marque como bloqueado el número de llamada del segundo y/o del tercer sistema informático 1b, 1a2 en el espacio de memoria 2 del primer sistema informático 1a, 1a1 y ya no se acepte ningún intento de conexión para el segundo y/o el tercer sistema informático 1b, 1a2 con este número de llamada.

En otra forma de realización preferente de la invención está previsto que dos sistemas informáticos 1a1, 1a2, que ya están conectados con un tercer sistema informático 1b y han establecido una conexión 203 directa, solo se autentifiquen entre sí a través del tercer sistema informático 1b común y que el procedimiento comprenda las siguientes etapas adicionales: m) el primer sistema informático 1a1 solicita un testigo de seguridad al tercer sistema informático 1b a través de la conexión 200 y lo envía al segundo sistema informático 1a2 a través de la conexión 203 directa; n) el segundo sistema informático 1a2 transmite el testigo de seguridad al tercer sistema informático 1b a través de la conexión 200; o) el tercer sistema informático 1b compara los dos testigos de seguridad y envía en cada caso un mensaje de sistema con el resultado de la comparación al primer y al segundo sistema informático 1a1, 1a2, y p) la lógica de control 10 de estos sistemas informáticos 1a1, 1a2 comprueba el mensaje de sistema con el resultado de la comparación y, si el resultado de la prueba es positivo, deja abierta la conexión 203 y, si el resultado de la prueba es negativo, cierra la conexión 203 directa y emite un mensaje de alarma.

En otra forma de realización preferente de la invención está previsto que dos sistemas informáticos realicen un proceso de pago y que el procedimiento comprenda las siguientes etapas adicionales: q) la lógica de control 10 en el sistema informático 1, 1a1 de un vendedor genera un testigo de seguridad, y un sistema informático 1, 1a2 de un comprador recibe a través de la conexión 203 directa el testigo de seguridad junto con la información de pago, procedente del sistema informático 1, 1a1 del vendedor; r) el sistema informático 1, 1a1 del vendedor transmite la información de pago junto con el testigo de seguridad a través de la conexión 200 al sistema informático 1b del servicio de pago; s) el sistema informático 1, 1a2 del comprador transmite la información de pago junto con el testigo de seguridad a través de la conexión 200 al sistema informático 1b del servicio de pago; y t) el sistema informático 1, 1a2 del comprador autoriza el proceso de pago a través de la conexión 200 en el sistema informático 1b del servicio de pago con un PIN, y u) una lógica de control 10 en el sistema informático 1b del servicio de pago compara el testigo de seguridad del sistema informático 1, 1a1 del vendedor y del sistema informático 1, 1a2 del comprador y valida el PIN del sistema informático 1, 1a2 del comprador y, si el resultado de la prueba es positivo, concluye el proceso de pago y envía un mensaje de sistema positivo al sistema informático 1, 1a1 del vendedor y al sistema informático 1, 1a2 del comprador. Si el resultado de la prueba es negativo, el proceso de pago se cancela y se envía de vuelta un mensaje de sistema negativo al sistema informático 1, 1a1 del vendedor y al sistema informático 1, 1a2 del comprador.

En otra forma de realización preferente de la invención está previsto que la conexión 203 para el proceso de pago entre el vendedor y el comprador en una tienda se establezca a través de NFC, Bluetooth, LAN inalámbrica o LAN por cable.

En otra forma de realización preferente de la invención está previsto que la información de pago para el proceso de pago entre el sistema informático, 1, 1a1 del vendedor y el sistema informático 1, 1a2 del comprador en una tienda o tienda en línea se transmita, en lugar de a través de una conexión 203 directa, a través de una señal óptica (por ejemplo código Q/R, código de barras, secuencias de caracteres o similares), una señal acústica (por ejemplo tonos de módem, voz, o similares) o mediante entrada manual entre el vendedor y el comprador. Opcionalmente, para mejorar adicionalmente la autentificación y para aumentar adicionalmente la seguridad, la transmisión también puede tener lugar de forma bidireccional, es decir, se transmiten datos tanto desde el sistema informático 1, 1a1 del vendedor hasta el sistema informático 1, 1a2 del comprador como desde el sistema informático 1, 1a2 del comprador hasta el sistema informático 1, 1a1 del vendedor. En este contexto, en el caso de la compra en línea también se puede utilizar un segundo dispositivo (1a2 - por ejemplo un teléfono inteligente) para recibir y transmitir la información de pago de un primer dispositivo (1a1 - por ejemplo un PC o un ordenador portátil). El primer dispositivo (1a1 - por ejemplo un PC o un ordenador portátil) asume en este contexto la función de un terminal del vendedor (1a1).

En otra forma de realización preferente de la invención, la lógica de control 10 también puede transmitir a través de otras conexiones de red, por ejemplo conexiones de red que no han sido creadas tal como se indicada más arriba, los datos para el proceso de pago entre el sistema informático 1, 1a1 del vendedor y el sistema informático 1b del servicio de pago, o entre el sistema informático 1, 1a2 del comprador y el sistema informático 1b del servicio de pago. En otra forma de realización preferente de la invención está previsto que para el cifrado, la identificación por PIN, el testigo de seguridad y la autorización se utilice un texto, un identificador biométrico, una llave electrónica o una llave mecánica, cuya información clave se lee mediante un dispositivo de lectura en los sistemas informáticos 1a, 1b, 1a1, 1a2.

En otra forma de realización preferente de la invención está previsto que, para pequeñas cantidades de datos, en particular para un proceso de pago, la lógica de control 10 transmita al menos una parte de los datos adquiridos en

las etapas precedentes a través de la interfaz de telefonía 12.

En otra forma de realización preferente de la invención está previsto que la lógica de control 10, con la activación de una señal predeterminada, transmita datos, en particular correos electrónicos, SMS y FAX, a sistemas informáticos 1 sin ayuda de otros servicios de Internet, como DNS y DynDNS.

En otra forma de realización preferente de la invención está previsto que la lógica de control 10 compruebe automáticamente si el número de llamada mostrado coincide con la línea de abonado real.

En otra forma de realización preferente de la invención está previsto que las solicitudes de conexión del primer sistema informático 1a, 1a1 sean distribuidas por la lógica de control 10 en un segundo y/o un tercer sistema informático 1b, 1a2 entre diferentes sistemas informáticos 1b, 1a2 segundo y/o tercero de acuerdo con un criterio predeterminado, en particular un número de conexiones y/o un índice de ocupación y/o una disponibilidad del segundo y/o del tercer sistema informático 1b, 1a2 y/o un número de llamada y/o un emplazamiento geográfico.

En otra forma de realización preferente de la invención está previsto que un primer sistema informático 1a, 1a1 en una función de servidor en la red procese mediante la lógica de control 10 solicitudes de conexión o solicitudes de resolución de nombre (por ejemplo, solicitudes DNS o similares) de otros sistemas informáticos en la red, y que la lógica de control 10 del primer sistema informático 1a, 1a1 lleve a cabo el intercambio de la información de conexión con un segundo y/o un tercer sistema informático 1b, 1a2, y a continuación establezca la conexión o envíe de vuelta los parámetros de conexión (por ejemplo dirección IP, número de puerto, o similares) a los sistemas informáticos solicitantes.

En otra forma de realización preferente de la invención está previsto que la lógica de control 10 de un sistema informático 1 también transmita los parámetros de conexión determinados a otro sistema servidor (por ejemplo cortafuegos o similares) y que éste autorice después las conexiones del sistema informático 1 o de sistemas informáticos de la red con estos parámetros de conexión.

En otra forma de realización preferente de la invención está previsto que la lógica de control 10 del segundo y/o del tercer sistema informático 1b, 1a2 automáticamente transmita al primer sistema informático 1a, 1a1 o ponga a disposición del mismo información y datos de control en función de la información de conexión.

En otra forma de realización preferente de la invención está previsto que el número de llamada del segundo y/o del tercer sistema informático 1b se utilice para un servicio de telefonía diferente o existente, en particular un servicio de FAX y/o un contestador automático, y que la lógica de control 10 del segundo y/o del tercer sistema informático 1b compare el número de llamada del primer sistema informático 1a con los números de llamada almacenados en el espacio de memoria 2 del segundo y/o del tercer sistema informático 1b y que, en caso de coincidencia, no active el servicio de telefonía, sino que transmita los datos de conexión para el segundo y/o el tercer sistema informático 1b al primer sistema informático 1a.

Preferiblemente, el procedimiento anteriormente descrito se puede utilizar junto con protocolos de otras interfaces orientadas a la conexión, en particular con protocolos NFC, Bluetooth y WLAN.

Listado de referencias numéricas

1	Sistemas informáticos
1a	Primer sistema informático (cliente)
1b	Tercer sistema informático (servidor)
1a1	Primer (cliente) sistema informático
1a2	Segundo (cliente) sistema informático
2	Espacio de memoria
3	Internet
4	Red telefónica
10	Lógica de control
11	Interfaz de red
12	Interfaz de telefonía
101	Primera conexión
102	Segunda conexión

103 Tercera conexión

104 Cuarta conexión

200 Conexión existente

201 Mensaje de sistema

202 Información de conexión

203 Conexión directa

REIVINDICACIONES

1. Procedimiento de direccionamiento, autentificación y almacenamiento seguro de datos en sistemas informáticos que incluyen al menos un primer, al menos un segundo y/o al menos un tercer sistema informático (1a1, 1a2, 1b) con al menos una interfaz de red (11) y al menos una interfaz de telefonía (12) y al menos un espacio de memoria (2) para información de gestión, en particular para al menos un número de llamada autorizado y/o al menos un PIN de abonado, de tal modo que los sistemas informáticos (1a1, 1a2, 1b) están programados con un programa que reproduce una lógica de control para controlar la interacción de las interfaces anteriormente mencionadas, comprendiendo el procedimiento las etapas consistentes en:

a) transmitir la información de conexión para la interfaz de red (11) de al menos un primer sistema informático (1a1) a través de la interfaz de telefonía (12) al menos a un segundo y/o un tercer sistema informático (1a2; 1b);

b) comprobar automáticamente un número de llamada del primer sistema informático (1a1) con los números de llamada almacenados en el espacio de memoria (2) en el segundo o en el tercer sistema informático (1a2, 1b) y, si el resultado de la prueba es positivo, transmitir al primer sistema informático (1a1) la información de conexión para la interfaz de red (11) del segundo y/o del tercer sistema informático (1a2, 1b) a través de la interfaz de telefonía (12), y activar la interfaz de red (11) del segundo y/o del tercer sistema informático (1a2, 1b) para aceptar conexiones (104) sobre la base de la información de conexión del primer sistema informático (1a1);

c) comprobar el número de llamada del segundo y/o del tercer sistema informático (1a2, 1b) con los números de llamada almacenados en el espacio de memoria (2) en el primer sistema informático (1a1) y, si el resultado de la prueba es positivo, activar la interfaz de red (11) del primer sistema informático (1a1) para establecer una conexión (101, 102, 103, 104) sobre la base de la información de conexión del segundo y/o del tercer sistema informático (1a2, 1b);

d) autorizar únicamente conexiones (104) con la información de conexión del primer sistema informático (1a1) a través de la interfaz de red (11) del segundo y/o del tercer sistema informático (1a2, 1b), y

e) autorizar únicamente conexiones (104) con la información de conexión del segundo y/o del tercer sistema informático (1a2, 1b) a través de la interfaz de red (11) del primer sistema informático (1a1), y en donde

f) las interfaces de red (11) del primer y del segundo y/o del tercer sistema informático (1a1, 1a2, 1b) solo autorizan intentos de conexión con la información de conexión respectiva durante un breve período de tiempo predeterminado, en particular entre 1 y 10, preferiblemente entre 2 y 7, de forma particularmente preferible entre 3 y 5 segundos, y, después del establecimiento de la conexión o después de la expiración del período de tiempo predeterminado sin que se haya establecido ninguna conexión, no son reconocibles ni accesibles para otros sistemas informáticos.

2. Procedimiento según la reivindicación 1, caracterizado por que al menos en cada caso el primer y el segundo sistema informático (1a1, 1a2) ya están conectados con el al menos un tercer sistema informático (1b), y el primer y el segundo sistema informático (1a1, 1a2) establecen en cada caso a través de la lógica de control (10) en el tercer sistema informático (1b) una conexión directa (203) a través de la interfaz de red (11), y el procedimiento comprende las etapas adicionales consistentes en:

g) transmitir al segundo sistema informático (1a2) la información de conexión para la interfaz de telefonía (12) y la interfaz de red (11) del primer sistema informático (1a1) con un mensaje de sistema (201) a través de la conexión (200) existente con el tercer sistema informático (1b);

h) comprobar un número de llamada del primer sistema informático (1a1) con números de llamada almacenados en el espacio de memoria (2) del segundo sistema informático (1a2) y, si el resultado de la prueba es positivo, transmitir al primer sistema informático (1a1) la información de conexión (202) para la interfaz de telefonía (12) y la interfaz de red (11) del segundo sistema informático (1a2) a través de la conexión (200) existente con el tercer sistema informático (1b), y activar la interfaz de red (11) del segundo sistema informático (1a2) para aceptar conexiones (203) sobre la base de la información de conexión del primer sistema informático (1a1), e

i) comprobar el número de llamada del segundo sistema informático (1a2) con los números de llamada almacenados en el espacio de memoria (2) en el primer sistema informático (1a1) y, si el resultado de la prueba es positivo, activar la interfaz de red (11) del primer sistema informático (1a1) para establecer conexiones (203) sobre la base de la información de conexión del segundo sistema informático (1a2); en donde

j) la interfaz de red (11) del segundo sistema informático (1a2) solo autoriza conexiones (203) con la información de conexión del primer sistema informático (1a1);

k) la interfaz de red (11) del primer sistema informático (1a1) solo autoriza conexiones (203) con la información de conexión del segundo sistema informático (1a2), y

l) las interfaces de red (11) del primer y del segundo sistema informático (1a1, 1a2) solo autorizan intentos de

conexión, en particular entre 1 y 15, preferiblemente entre 2 y 12 y de forma particularmente preferible entre 3 y 10 intentos de conexión con la información de conexión respectiva durante un breve período de tiempo predeterminado, en particular entre 1 y 10, preferiblemente entre 2 y 7, de forma particularmente preferible entre 3 y 5 segundos, y, después del establecimiento de la conexión o después de la expiración del período de tiempo predeterminado sin que se haya establecido ninguna conexión, no son reconocibles ni accesibles para otros sistemas informáticos.

3. Procedimiento según una de las reivindicaciones 1 o 2, caracterizado por que en las etapas b) y/o h) se activa la interfaz de red (11) del segundo sistema informático (1a2) para establecer conexiones sobre la base de la información de conexión del primer sistema informático (1a1), y por que en las etapas c) y/o i) se activa la interfaz de red (11) del primer sistema informático (1a1) para aceptar conexiones (103) sobre la base de la información de conexión del segundo sistema informático (1a2).

4. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que, después del establecimiento de la conexión, el segundo sistema informático (1a2) solicita una identificación del primer sistema informático (1a1), la compara con las etiquetas de identificación almacenadas en el espacio de memoria (2) del segundo sistema informático (1a2) y, si el resultado de la prueba es positivo, la conexión permanece activada y, si el resultado de la prueba es negativo, la conexión se cierra y se emite un aviso de alarma, en donde, en particular después de un número predeterminado de intentos de identificación negativos, en particular entre 1 y 15, preferiblemente entre 2 y 12, de forma particularmente preferible entre 3 y 10, la lógica de control (10) marca como bloqueado el número de llamada del primer sistema informático (1a1) en el espacio de memoria (2) del segundo sistema informático (1a2) y ya no se acepta ninguna información de conexión más para el primer sistema informático (1a1) con este número de llamada, o la etiqueta de identificación consiste en un texto, un identificador biométrico, una llave electrónica o una llave mecánica, cuya información clave se lee mediante un dispositivo de lectura en el primer, el segundo y/o el tercer sistema informático (1a1, 1a2, 1b).

5. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que el primer sistema informático (1a1) suministra un testigo de seguridad junto con la información de conexión al segundo sistema informático (1a2), que se transmite durante el establecimiento de la conexión a través de la interfaz de red (11) y se comprueba mediante la lógica de control (10) en el primer sistema informático (1a1) y, si el resultado de la prueba es positivo, la conexión permanece activada y, si el resultado de la prueba es negativo, la conexión se cierra y se emite un aviso de alarma, en donde, en particular después de un número predeterminado de intentos de conexión negativos, preferiblemente entre 1 y 15, preferiblemente entre 2 y 12, de forma particularmente preferible entre 3 y 10 intentos de conexión negativos, la lógica de control (10) marca como bloqueado el número de llamada del segundo sistema informático (1a2) en el espacio de memoria (2) del primer sistema informático (1a1) y ya no se acepta ningún intento de conexión para el segundo sistema informático (1a2) con este número de llamada.

6. Procedimiento según la reivindicación 2, caracterizado por que al menos el primer y el segundo sistema informático (1a1, 1a2), que ya están conectados con un tercer sistema informático (1b) y han establecido una conexión (203) directa, solo se autentifican entre sí a través del tercer sistema informático (1b) común, y el procedimiento comprende las siguientes etapas adicionales:

m) el primer sistema informático (1a1) solicita un testigo de seguridad al tercer sistema informático (1b) a través de la conexión (200) y lo envía al segundo sistema informático (1a2) a través de la conexión (203) directa;

n) el segundo sistema informático (1a2) transmite el testigo de seguridad al tercer sistema informático (1b) a través de la conexión (200);

o) el tercer sistema informático (1b) compara los dos testigos de seguridad y envía en cada caso un mensaje de sistema con el resultado de la comparación al primer y/o al segundo sistema informático (1a1, 1a2), y

p) la lógica de control (10) del primer y/o del segundo sistema informático (1a1, 1a2) comprueba el mensaje de sistema con el resultado de la comparación y, si el resultado de la prueba es positivo, deja abierta la conexión (203) y, si el resultado de la prueba es negativo, cierra la conexión (203) directa y emite un mensaje de alarma.

7. Procedimiento según la reivindicación 2 o la reivindicación 6, caracterizado por que un primer y un segundo sistema informático, con participación de un tercer sistema informático (1b), llevan a cabo un proceso de pago y el procedimiento comprende las siguientes etapas adicionales:

q) la lógica de control (10) genera un testigo de seguridad en el primer sistema informático (1a1), en particular en el sistema informático de un vendedor, y el segundo sistema informático (1a2), en particular el sistema informático de un comprador, recibe a través de la conexión (203) directa el testigo de seguridad junto con una información de pago, procedente del primer sistema informático (1a1), en particular del sistema informático del vendedor;

r) el primer sistema informático (1a1), en particular el sistema informático del vendedor, transmite la información de pago junto con el testigo de seguridad a través de la conexión (200) al tercer sistema informático (1b), en particular al sistema informático (1b) de un servicio de pago (1b);

s) el segundo sistema informático (1a2), en particular el sistema informático del comprador, transmite la información de pago junto con el testigo de seguridad a través de la conexión (200) al tercer sistema informático (1b), en particular al sistema informático (1b) del servicio de pago;

t) el segundo sistema informático (1a2), en particular el sistema informático del comprador, autoriza el proceso de pago a través de la conexión (200) en el tercer sistema informático (1b), en particular en el sistema informático (1b) del servicio de pago, con un PIN, y

u) una lógica de control (10) en el tercer sistema informático (1b), en particular en el sistema informático (1b) del servicio de pago, compara el testigo de seguridad del primer sistema informático (1a1), en particular del sistema informático del vendedor, y del segundo sistema informático (1a2), en particular del sistema informático del comprador, y valida el PIN del segundo sistema informático (1a2), en particular del sistema informático (1a2) del comprador, y, si el resultado de la prueba es positivo, concluye el proceso de pago y envía de vuelta un mensaje de sistema positivo al primer sistema informático (1a2) en particular al sistema informático del vendedor, y al segundo sistema informático (1a2), en particular al sistema informático del comprador, o, si el resultado de la prueba es negativo, cancela el proceso de pago y envía un mensaje de sistema negativo al primer sistema informático (1a1) en particular al sistema informático del vendedor, y al segundo sistema informático (1a2), en particular al sistema informático del comprador.

8. Procedimiento según la reivindicación 7, caracterizado por que la conexión (203) para el proceso de pago entre el primer sistema informático (1a1), en particular el sistema informático del vendedor, y el segundo sistema informático (1a2), en particular el sistema informático del comprador, preferiblemente en una tienda, se establece a través de NFC, Bluetooth, LAN inalámbrica o LAN por cable, y/o por que la información de pago para el proceso de pago entre el primer sistema informático (1a2), en particular el sistema informático del vendedor, y el segundo sistema informático (1a2), en particular el sistema informático del comprador, preferiblemente en una tienda o en una tienda en línea, se transmite, en lugar de a través de una conexión (203) directa, a través de una señal óptica, por ejemplo código Q/R, código de barras, secuencias de caracteres o similares, una señal acústica, por ejemplo tonos de módem, voz, o similares, o mediante entrada manual, en particular bidireccional, en particular en donde, en el caso de una compra en línea, también se utiliza un segundo dispositivo que constituye o que proporciona el segundo sistema informático (1a2), en particular un teléfono inteligente, para recibir y transmitir la información de pago de un primer dispositivo que constituye o que proporciona el primer sistema informático (1a1), en particular un PC o un ordenador portátil, en donde el primer dispositivo está previsto preferiblemente como terminal del primer sistema informático (1a2), en particular del sistema informático del vendedor.

9. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que la lógica de control (10) puede transmitir los datos para el proceso de pago entre el primer sistema informático (1a1), en particular el sistema informático del vendedor, y el tercer sistema informático (1b), en particular el sistema informático del servicio de pago, o entre el segundo sistema informático (1a2), en particular el sistema informático del comprador, y el tercer sistema informático (1b), en particular el sistema informático del servicio de pago, a través de otras conexiones de red, en particular conexiones de red diferentes a las definidas en las reivindicaciones 1 o 2, y/o por que para el cifrado, la identificación por PIN, el testigo de seguridad y la autorización se utiliza un texto, un identificador biométrico, una llave electrónica o una llave mecánica, cuya información clave se lee mediante un dispositivo de lectura en los sistemas informáticos (1a1, 1a2, 1b).

10. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que, para pequeñas cantidades de datos, en particular para un proceso de pago, la lógica de control (10) transmite al menos una parte de los datos adquiridos en las etapas precedentes a través de la interfaz de telefonía (12), y/o por que la lógica de control (10), con la activación de una señal predeterminada, transmite datos, en particular correos electrónicos, SMS y FAX, a sistemas informáticos (1, 1a1, 1a2, 1b) sin ayuda de otros servicios de Internet, como DNS y DynDNS, y/o por que la lógica de control (10) comprueba automáticamente si el número de llamada mostrado coincide con la línea de abonado real, y/o por que las solicitudes de conexión del primer sistema informático (1a1) son distribuidas por la lógica de control (10) en un segundo y/o un tercer sistema informático (1b, 1a2) entre diferentes sistemas informáticos segundo y/o tercero (1b, 1a2) de acuerdo con un criterio predeterminado, en particular un número de conexiones y/o un índice de ocupación y/o una disponibilidad del segundo y/o del tercer sistema informático (1b, 1a2) y/o un número de llamada y/o un emplazamiento geográfico.

11. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que un primer sistema informático (1a1) en una función de servidor en la red procesa mediante la lógica de control (10) solicitudes de conexión o solicitudes de resolución de nombre, por ejemplo solicitudes DNS o similares, de sistemas informáticos en la red, y la lógica de control (10) del primer sistema informático (1a1) lleva a cabo el intercambio de la información de conexión con un segundo y/o un tercer sistema informático (1b, 1a2) tal como se define en las reivindicaciones precedentes, y a continuación establece la conexión o envía de vuelta los parámetros de conexión, por ejemplo dirección IP, número de puerto, o similares, a los sistemas informáticos solicitantes.

12. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que la lógica de control (10) de al menos un sistema informático 1 también transmite los parámetros de conexión determinados tal como se define en las reivindicaciones precedentes al menos a otro sistema informático, en particular a un sistema servidor, como

por ejemplo un cortafuegos, y éste autoriza después las conexiones del primer sistema informático 1 o de los otros sistemas informáticos de la red con estos parámetros de conexión, y/o por que la lógica de control (10) del segundo y/o del tercer sistema informático (1b, 1a2) automáticamente transmite al menos al primer sistema informático (1a1) o pone a disposición del mismo información y datos de control en función de la información de conexión.

13. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que el número de llamada del segundo y/o del tercer sistema informático (1a2, 1b) se utiliza para un servicio de telefonía diferente o existente, en particular un servicio de FAX y/o un contestador automático, y la lógica de control (10) al menos del segundo y/o del tercer sistema informático (1a2, 1b) compara el número de llamada de al menos el primer sistema informático (1a1) con los números de llamada almacenados en el espacio de memoria (2) del segundo y/o del tercer sistema informático (1a2, 1b) y, en caso de coincidencia, no activa el servicio de telefonía, sino que transmite los datos de conexión para el segundo y/o el tercer sistema informático (1a2, 1b) al primer sistema informático (1a1).

14. Procedimiento según una de las reivindicaciones precedentes, caracterizado por que, para sistemas informáticos (1a1, 1a2, 1b) geográficamente cercanos entre sí, la información de conexión para la interfaz de red 11 se puede transmitir entre los sistemas informáticos (1a1, 1a2, 1b), en particular de forma bidireccional, alternativamente a través de señales ópticas, por ejemplo código Q/R, código de barras, secuencias de caracteres o similares, señales acústicas, por ejemplo tonos de módem, voz, o similares, mediante entradas manuales a través de conexiones seguras establecidas previamente de otro modo, por ejemplo NFC, Bluetooth, WLAN, USB o similares, que preferiblemente sirven como interfaz de telefonía (12).

15. Utilización del procedimiento según una de las reivindicaciones precedentes con protocolos de otras interfaces orientadas a la conexión, en particular con protocolos NFC, Bluetooth y WLAN.

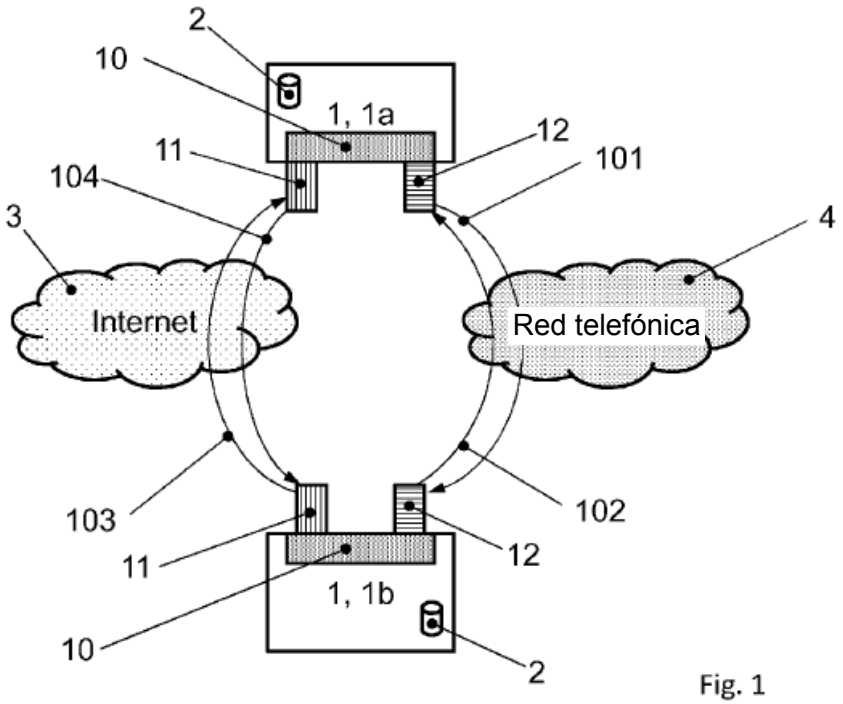
2
10
1, 1a
12
11
101
104
3
4
Internet
Red telefónica
103
102
11
12
1, 1b
10
2

Fig. 1

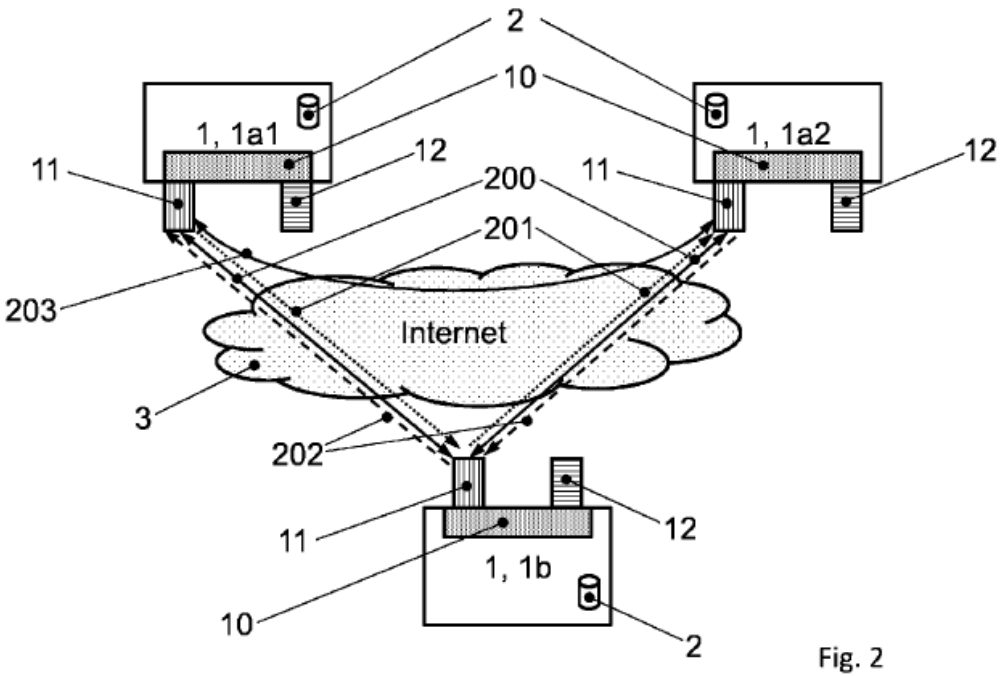

Fig. 2

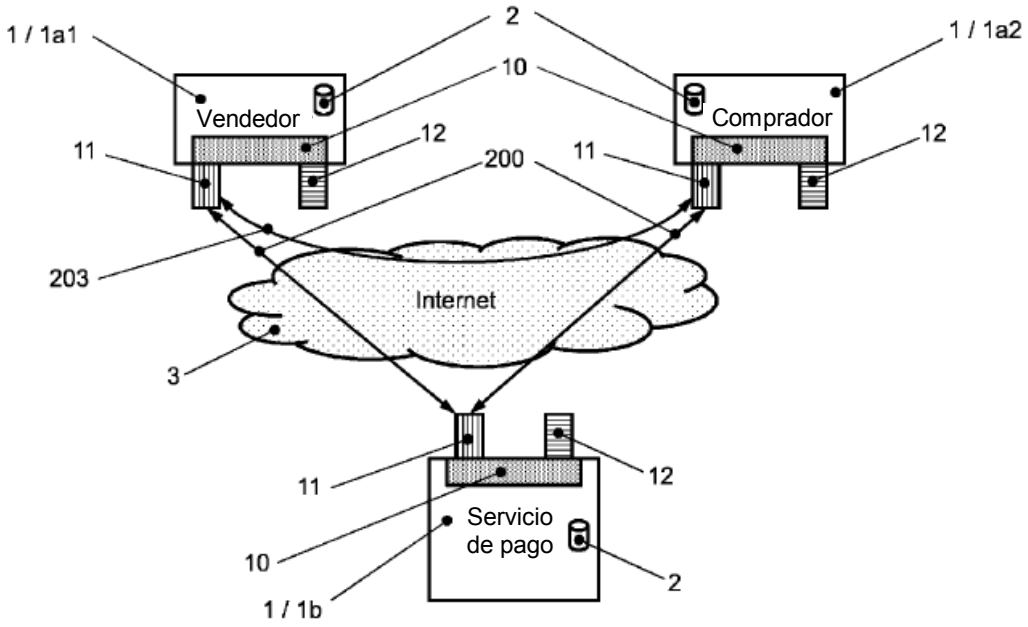
1 / 1a1
2
1 / 1a2
10
Vendedor
Comprador
11
12
11
12
200
203
Internet
3
11
12
Servicio
de pago
10
2
1 / 1b

Fig. 3