(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 707 533**

(51) Int. CI.:

H04L 9/30 (2006.01)
H04L 9/00 (2006.01)
G06F 21/30 (2013.01)
H04L 29/06 (2006.01)
H04W 12/06 (2009.01)
G06F 21/31 (2013.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.03.2015 PCT/AU2015/000149**

(87) Fecha y número de publicación internacional: **24.09.2015 WO15139072**

(96) Fecha de presentación y número de la solicitud europea: **16.03.2015 E 15764675 (3)**

(97) Fecha y número de publicación de la concesión europea: **07.11.2018 EP 3120493**

(54) Título: **Sistema de autenticación persistente que incorpora códigos de acceso de un solo uso**

(30) Prioridad:

16.03.2014 AU 2014900894

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.04.2019

(73) Titular/es:

HAVENTEC PTY LTD (100.0%)
Level 27, 1 Market Street
Sydney NSW 2000, AU

(72) Inventor/es:

RICHARDSON, RIC B

(74) Agente/Representante:

PONS ARIÑO, Ángel

DESCRIPCIÓN

Sistema de autenticación persistente que incorpora códigos de acceso de un solo uso

La presente invención hace referencia a un sistema de autenticación que incorpora códigos de acceso de un solo uso y más en particular, pero no exclusivamente, un sistema de este tipo que no requiere que un usuario del sistema introduzca y re-introduzca un nombre de usuario y una contraseña correspondiente para una sesión de usuario iniciada por el usuario. La invención se define en las reivindicaciones adjuntas.

Antecedentes

El uso de nombres de usuario y contraseñas es bien conocido en el arte. Existe un problema creciente en el que el almacenamiento de contraseñas en el lado del servidor se está volviendo más propenso al ataque y la carga sobre los usuarios para utilizar contraseñas diferentes y seguras a través de múltiples sitios web ha introducido inconvenientes, una excesiva complicación y la exposición continua de la seguridad.

Los intentos para resolver este problema incluyen dispositivos de hardware para el registro de huella digital u otra autenticación multifactorial biométrica. Estos métodos se utilizan en un intento de reforzar la seguridad y reducir la exposición de los problemas asociados con los sistemas de autenticación estándar de nombre de usuario y contraseña. Sin embargo, habitualmente estos únicamente añaden más etapas de complejidad e inconveniencia a un proceso ya engorroso.

Un ejemplo de dicho intento es el documento US 5875296 de IBM, cuyo contenido se incorpora en la presente memoria como referencia cruzada. Su solución se resume en la reivindicación 1 de la misma que dice:

Un método de autenticación de un cliente para un servidor Web que puede conectarse a un sistema de archivos distribuidos de un entorno informático distribuido, donde el entorno informático distribuido incluye un servicio de seguridad para devolver una credencial a un usuario autenticado para acceder al sistema de archivos distribuidos, que comprende las etapas de:

> en respuesta a la recepción por parte del servidor Web de una id y contraseña de usuario del cliente, ejecutar un protocolo de inicio de sesión con el servicio de seguridad y almacenar una credencial resultante del mismo;
>
> devolver al cliente un objeto de estado del cliente persistente que tenga un identificador en el mismo; y
>
> hacer que el cliente utilice el objeto de estado del cliente persistente que incluye el identificador en lugar de una id y contraseña de usuario para obtener el posterior acceso a los documentos Web en el sistema de archivos distribuidos.

Esta disposición puede ser interpretada como utilizar una “cookie” como el objeto de estado de cliente persistente. Esta disposición sufre de problemas de seguridad significativos.

Entre los ejemplos del arte previo adicionales (todos los cuales se incluyen como referencia cruzada) se incluyen:

> la patente US8447977 de Canon KK cuya reivindicación principal dice:
>
> Un método de autenticación de un dispositivo con un servidor sobre una red, donde el método comprende las etapas de:
>
> establecer, por parte del dispositivo, una conexión segura con el servidor;
>
> comunicar, por parte del dispositivo, información de identificación del dispositivo al servidor, en donde la información de identificación identifica únicamente el dispositivo al servidor y es pre-almacenado en el dispositivo;
>
> determinar, por parte del servidor, la credibilidad del dispositivo utilizando la información de identificación comunicada por el dispositivo; y
>
> en un caso en el que el servidor determina que el dispositivo es fiable:
>
> > crear, por parte del servidor, un primer testigo de autenticación para el dispositivo, donde dicho primer testigo de autenticación indica que el dispositivo es fiable;

almacenar, por parte del servidor, el primer testigo de autenticación;

transferir, por parte del servidor, el primer testigo de autenticación al dispositivo utilizando la conexión segura; y almacenar, por parte del dispositivo, el primer testigo de autenticación;

en donde el método además comprende las etapas de:

establecer, por parte del dispositivo, una reconexión segura con el servidor ; y

autenticar, por parte del servidor y sobre la re-conexión segura, el dispositivo utilizando el primer testigo de autenticación almacenado por el dispositivo.

La patente US6668322 de Sun MicroSystems cuya reivindicación principal dice

Una credencial de sesión para su uso en un acceso de control de la arquitectura de seguridad a uno o más recursos de información, donde la credencial de la sesión comprende:

un identificador principal identificando únicamente un principal; y

una codificación de autorización concedida por la arquitectura de seguridad después de la autenticación previa de una credencial de inicio de sesión correspondiente al principal, donde el identificador principal y la codificación de autorización están aseguradas criptográficamente y permiten que la arquitectura de seguridad evalúe la suficiencia de la autorización para el acceso a dicho uno o más recursos de información sin la re-autenticación de las credenciales de inicio de sesión.

La patente US6421768 de First Data cuya reivindicación principal dice

Un método para la autenticación transferible, por el cual un usuario que accede a un primer ordenador puede ser autenticado para un segundo ordenador remoto con respecto a dicho primer ordenador, sin necesariamente requerir que el usuario explícitamente se identifique a dicho segundo ordenador, que comprende las etapas de:

en un ordenador de usuario, acceder a dicho primer ordenador;

autenticar dicho usuario a dicho primer ordenador;

recibir de dicho primer ordenador una cookie que incluye un certificado digital de dicho primer ordenador de una característica de usuario, donde dicho certificado es asegurado criptográficamente por dicho primer ordenador, donde dicha característica de usuario es cifrado e incorporado en dicho certificado digital por dicho primer ordenador utilizando una clave pública del lado del cliente confidencial para dicho primer ordenador y dicho segundo ordenador, pero desconocida para dicho usuario, donde dicha clave pública del lado del cliente es asegurada criptográficamente utilizando una clave asimétrica de al menos uno de entre dicho primer ordenador y dicho segundo ordenador;

transmitir dicha clave pública del lado del cliente asegurada criptográficamente a dicho segundo ordenador a través de dicho ordenador del usuario; y

enviar al menos una parte de dicha cookie, que incluye dicho certificado, a dicho segundo ordenador configurado para:

autenticar dicho certificado sin requerir necesariamente que dicho usuario se identifique él mismo explícitamente ante dicho ordenador;

extraer dicha característica de usuario de dicho certificado; y

realizar una acción basada en dicha característica de usuario.

Tal como se ha expuesto anteriormente, las cookies presentan problemas de seguridad particulares y su utilización tiene continuos problemas para su adopción hoy en día.

También se divulgan los siguientes documentos que describen formas alternativas para buscar sistemas seguros sin el uso de una introducción repetitiva de una contraseña y una comunicación explícita de la contraseña de una máquina a otra. Estos sistemas pueden ser más complejos incluyendo el uso de una máquina de terceros para realizar una verificación/autenticación.

US4578531 de AT&T

US6134592 de Netscape

US6205480 de Computer Assoc

US7523490 de Microsoft

US20110320820 de IBM

US20130219472 A1 de QSAN

Las realizaciones de la presente invención están diseñadas para abordar estos problemas.

Notas

El término “comprender” (y las variaciones gramáticas del mismo) se utiliza en esta especificación en el sentido inclusivo de “tener” o “incluir”, y no en el sentido exclusivo de “consistir en”.

La anterior discusión del arte previo en los antecedentes de la invención, no es una admisión de que cualquier información discutida en la misma sea arte previo citable o parte del conocimiento común general de los expertos en el arte en cualquier país.

Breve descripción de la invención

En líneas generales, el concepto que encierran las realizaciones de la presente invención es depender de dos elementos de información para un proceso de autenticación persistente y el correspondiente sistema y aparato:

En una forma preferida y detallada, se genera un nuevo par de claves por el cliente y se pasan al servidor para cada sesión. La comunicación para una sesión posterior se habilita únicamente si existe una coincidencia entre esta clave pública almacenada en el servidor y la clave pública en el cliente coincidente con dicho usuario (ID de usuario).

En líneas generales, expresado de otro modo, de acuerdo con una realización preferida se efectúa una cadena ininterrumpida de códigos de acceso de un solo uso para caracterizar al usuario cuando se utiliza la aplicación del lado del cliente que se comunica con el servidor. En una forma particular los códigos de acceso de un solo uso son en realidad las claves públicas de los pares de claves generados por el cliente. En una forma preferida en particular adicional, se habilita un aspecto de renovación por el cual los códigos de acceso de un solo uso continúan siendo reemplazados a intervalos regulares (en una forma preferida, preferiblemente una vez por sesión de conexión al menos).

Por consiguiente, en una forma amplia de la invención se proporciona un método para mantener una autenticación continua del usuario de una aplicación sin la necesidad de introducir y re-introducir un nombre de usuario y una contraseña correspondiente para cada sesión iniciada entre una aplicación del lado del cliente que reside en una plataforma del lado del cliente y un servidor; y en donde la contraseña no se almacena en el servidor; donde el método comprende utilizar una cadena ininterrumpida de códigos de acceso de un solo uso; donde cada código de acceso en la cadena es único para el nombre de usuario y la aplicación del lado del cliente; cada código de acceso renovado periódicamente y preferiblemente al menos una vez durante cada sesión.

Preferiblemente, el código de acceso comprende una clave pública del lado del cliente que se mantiene persistente tanto en la plataforma del lado del cliente y el servidor hasta que se reemplaza por la siguiente clave pública del lado del cliente en la cadena de códigos de acceso.

Preferiblemente, la clave pública del lado del cliente comprende una clave pública de un par de claves PKI (del inglés “Public Key Infrastructure”, Infraestructura de Clave Pública).

Preferiblemente, la correspondiente clave privada del lado del cliente no se comparte con el servidor.

En una forma amplia adicional de la invención se divulga un dispositivo que incluye un procesador en comunicación con una memoria adaptada para ejecutar una aplicación; donde dicho dispositivo mantiene una autenticación continua del usuario de una aplicación ejecutable en el dispositivo sin la necesidad de introducir y re-introducir un nombre de usuario y una contraseña correspondiente para cada sesión iniciada entre una aplicación del lado del cliente que reside en una plataforma del lado del cliente en el dispositivo y un servidor remoto; y en donde la contraseña no se almacena en el servidor; donde el método comprende utilizar una cadena ininterrumpida de códigos de acceso de un solo uso; siendo cada código de acceso en la cadena único para el nombre de usuario y la aplicación del lado del cliente; cada código de acceso renovado al menos una vez durante cada dicha sesión.

Preferiblemente, el código de acceso comprende una clave pública del lado del cliente que se mantiene persistente tanto en la plataforma del lado del cliente como en el servidor, hasta que es reemplazada por la siguiente clave pública del lado del cliente en la cadena de códigos de acceso.

Preferiblemente, la clave pública del lado del cliente comprende una clave pública de un par de claves PKI.

Preferiblemente, la correspondiente clave privada del lado del cliente no se comparte con el servidor.

En una forma general adicional de la invención se proporciona un sistema que incluye un dispositivo que tiene un procesador en comunicación con una memoria adaptada para ejecutar una aplicación; donde dicho dispositivo mantiene una autenticación continua del usuario de una aplicación ejecutable en el dispositivo sin necesidad de introducir y re-introducir un nombre de usuario y una contraseña correspondiente para cada sesión iniciada entre una aplicación del lado del cliente que reside en una plataforma del lado del cliente en un dispositivo y un servidor remoto, donde el sistema deriva un primer y un segundo elemento de datos; dicho primer elemento de datos que comprende:

"Algo que tienes" que en una forma preferida es una clave pública del lado del cliente,

El segundo elemento de datos que comprende "Algo que sabes".

Preferiblemente, dicho segundo elemento de datos comprende un PIN/contraseña de usuario que se utiliza para crear una clave pública para cualquier sesión dada.

Preferiblemente, dicho segundo elemento de datos comprende cualquier forma de información que pueda identificarse personalmente, incluyendo pero sin limitarse a huellas del pulgar u otro tipo de biométrica que se utilice para crear una clave privada para cualquier sesión dada.

Preferiblemente, se genera un nuevo par de claves por parte del cliente y se pasan al servidor para cada sesión y en donde la comunicación para una sesión posterior es habilitada únicamente si existe una coincidencia entre esta clave pública almacenada por el servidor y la clave pública en el cliente coincidente con ese usuario (ID de usuario).

En aún una forma general adicional de la invención se proporciona una plataforma que incluye al menos un procesador en comunicación con una memoria que ejecuta un código para realizar un método de autenticación de un usuario; donde dicho método comprende efectuar una cadena ininterrumpida de códigos de acceso de un solo uso para caracterizar el usuario cuando se utiliza una aplicación del lado del cliente que se ejecuta en dicha plataforma, la cual se comunica con un servidor remoto por Internet.

Preferiblemente, los códigos de acceso de un solo uso son la clave pública del par de claves generado por el cliente.

En aún una forma general adicional de la invención se proporciona un sistema para mantener una autenticación continua del usuario de una aplicación sin la necesidad de introducir y re-introducir un nombre de usuario y una contraseña correspondiente para cada sesión iniciada entre la aplicación del lado del cliente que reside en una plataforma del lado del cliente y un servidor, donde dicho sistema utiliza una secuencia de códigos de acceso de un solo uso que son renovables y en donde la renovación se efectúa reemplazando los códigos de acceso en intervalos regulares.

En una forma preferida un intervalo comprende un intervalo de conexión de una vez por sesión.

Dibujos

Figura 1 – Componentes principales del ejemplo de realización

Figura 2 – Proceso de control para un uso inicial del ejemplo de realización

Figura 3 – Proceso de control para un uso no inicial del ejemplo de realización

Figura 4 – es un diagrama de bloques de un método de construcción de una clave privada de acuerdo con una realización adicional.

Descripción detallada de las realizaciones preferidas

En líneas generales, la idea es depender de dos elementos de información para una autenticación inicial y continuada: En una forma preferida y detallada, una nueva clave pública es generada por el cliente y pasada al servidor para cada sesión. La comunicación para una sesión posterior es habilitada únicamente si existe una coincidencia entre esta clave pública almacenada por el servidor y la clave pública en el cliente coincidente con ese usuario (ID de usuario).

En líneas generales, expresado de otra forma, de acuerdo con una realización preferida se efectúa una cadena ininterrumpida de códigos de acceso de un solo uso para caracterizar al usuario cuando se utiliza la aplicación del lado del cliente que se comunica con el servidor. En una forma en particular, los códigos de acceso de un solo uso son en realidad claves públicas. En una forma preferida adicional en particular, se habilita un aspecto de renovación por el que los códigos de acceso de un solo uso continúan siendo reemplazados a intervalos regulares (una vez por sesión al menos).

Se divulga un ejemplo de realización que utiliza una cadena ininterrumpida de códigos de acceso de un solo uso como un sustituto de una contraseña en un sistema tradicional de autenticación por nombre de usuario y contraseña.

La Figura 1 muestra los componentes clave de un ejemplo de realización. Cuando un usuario, utilizando una única ID de usuario 23, se conecta con un servidor, se utiliza habitualmente un sistema de cifrado y autenticación tal como un Intercambio de cifrado de clave pública.

Habitualmente, el usuario tiene una aplicación 24 del lado del cliente que produce un par de claves 10 que se utiliza para comunicarse con el servidor que utiliza su propio par de claves 11. En la práctica conocida de criptografía de claves públicas la clave privada 12 de los clientes se utiliza con la clave pública del servidor 14 para cifrar un mensaje y el servidor utiliza la clave pública del cliente 13 y la clave privada del servidor 15 para descifrar el mensaje enviado.

Una vez que la identidad del emisor 10 y del receptor 11 ha sido verificada, las dos partes comparten una contraseña 17 secreta que se utiliza para el cifrado y descifrado de alta velocidad de un mensaje 16 cifrado.

Habitualmente, el mensaje 16 cifrado utiliza una contraseña 17 secreta que es utilizada únicamente para la duración de la sesión de comunicación, después de lo cual la contraseña 17 se descarta y ya no se utiliza más.

En el ejemplo de realización, el anterior proceso de intercambio de claves y cifrado es expandido para incluir un segundo conjunto 18 de par de claves que es generado por el cliente. Esta generación 18 de par de claves se utiliza para enlazar únicamente la sesión actual autenticada con el siguiente sistema de autenticación entre el cliente y el servidor.

Este par de claves 18 incluye una clave privada 20 que es almacenada localmente en el dispositivo del cliente y una clave pública 19 que también es almacenada localmente. La clave pública del cliente almacenada también es compartida con y transferida al servidor 25 que a continuación enlaza una referencia almacenada a la única ID de usuario 21 de la persona que actualmente está utilizando el cliente con una copia almacenada de la clave pública 22 del cliente.

Durante posteriores conexiones entre el cliente y el servidor, la clave pública 19, 22 del cliente compartida, la clave pública 14 del servidor y la clave privada almacenada en el cliente 20 se utilizan como los actuales pares de claves públicas y un par de clave adicional se genera a continuación y se almacena para la siguiente sesión.

La Figura 2 divulga el proceso de control de la sesión inicial del ejemplo de realización. Un usuario utiliza una aplicación en el lado del cliente 30 de la comunicación para interactuar con un servidor 31.

Inicialmente, el usuario se conecta a un servidor que utiliza claves persistentes de un solo uso con ID 32 únicas. Inicialmente, el servidor y el cliente utilizan una sesión 33 de cifrado de clave pública tradicional para asegurar las comunicaciones entre el cliente 30 y el servidor 31.

A continuación, se confirma que el usuario quiere utilizar códigos 34 de un solo uso persistentes y la ID única de los usuarios es capturada o recuperada del usuario o del almacenamiento en el cliente y enviada al servidor 35.

Posteriormente, el servidor solicita que el cliente genere un par de claves públicas para su uso en la siguiente sesión 36. El cliente genera a continuación un par de claves públicas 37 que se almacena de forma segura en el cliente para su uso en la siguiente sesión 38 y la clave pública del par de claves es compartida con el servidor 39.

La clave pública de los clientes que va a ser utilizada para la siguiente sesión es almacenada en el servidor utilizando la ID 40 única de los usuarios. Una vez se haya confirmado esta etapa, la SSL, TLS o una conexión similar existente se utiliza para asegurar la comunicación en curso entre el cliente y el servidor hasta que la sesión se termina o se interrumpe 41.

La Figura 3 divulga el proceso de control de las sesiones no iniciales del ejemplo de realización. Un usuario utiliza una aplicación en el lado del cliente 60 de la comunicación para interactuar con un servidor 61.

Inicialmente, el usuario se conecta a un servidor que utiliza claves de un solo uso persistentes con ID 62 únicas. Inicialmente, el servidor y el cliente utilizan una sesión 63 de cifrado de clave pública tradicional para asegurar las comunicaciones entre el cliente 60 y el servidor 61.

A continuación la ID única es capturada o recuperada del usuario o del almacenamiento en el cliente 64. A continuación, el par de claves del cliente almacenado, que fue almacenado durante la sesión previa, se recupera utilizando la ID 65 de usuario única de los usuarios. A continuación la ID única de los usuarios y la clave pública del cliente almacenada se comparten con el servidor 66.

El servidor a continuación busca en su propia base de datos del usuario la ID única de los usuarios y recupera la clave pública 67 del cliente guardada previamente para su comparación con la clave pública del cliente compartida del cliente 68. Si las dos claves no coinciden el servidor informa al usuario y sugiere diversas medidas para abordar el problema 70. Si tiene lugar una coincidencia 69, entonces el servidor solicita 71 que sea generado un segundo par de claves por el cliente 72 y el par de claves se almacena 73 posteriormente. Adicionalmente, la clave pública del par de claves que se acaba de generar 72 se comparte con el servidor para su uso en la siguiente sesión 74. El servidor entonces almacena la siguiente clave pública del cliente que va a ser utilizada con la ID 75 única de los usuarios y los actuales pares de claves tanto del cliente como del servidor se utilizan para la comunicación en curso entre el cliente y el servidor hasta que la sesión se termina o se interrumpa 76.

El resultado es una cadena persistente de códigos de un solo uso en forma de claves públicas del cliente que pueden ser utilizadas para establecer y perpetuar una conexión segura entre un sistema cliente y un sistema servidor durante sesiones múltiples y en curso.

Realizaciones alternativas

El ejemplo de realización utiliza la generación y el enlace de una serie de claves públicas del lado del cliente que se almacenan tanto en el lado del cliente como en el lado del servidor como un identificador persistente para los propósitos de autenticación. Una realización alternativa podría utilizar una cadena de claves de sesión TLS tal como códigos de acceso AES compartidos como un identificador persistente. En este caso cada vez que se utiliza una clave pública compartida del lado del cliente, se genera una clave consecutiva y se almacena en ambos lados para su utilización en la siguiente sesión. La ventaja de utilizar una clave pública del lado del cliente como el identificador persistente es que la clave privada del lado del cliente no se comparte con el servidor, a diferencia del caso de una clave de sesión TLS, y por lo tanto añade un nivel de seguridad al sistema.

En el ejemplo de realización el cliente se utiliza para generar pares de claves para el proceso que va a ser utilizado. En una realización alternativa el servidor podría ser utilizado para generar pares de claves y compartirlas con el cliente para su uso en sesiones sucesivas.

El ejemplo de realización comparte una copia almacenada en el servidor de la siguiente clave pública del cliente, con una copia compartida de la clave pública del cliente que viene del cliente durante la sesión actual. Una realización alternativa podría utilizar cualquier equivalente de la clave pública del cliente con propósitos de comparación que incluye, pero no se limita a, una suma de verificación (checksum) o una función resumen (hash) de la clave pública del cliente.

Realización adicional

En referencia a la figura 4 y en una forma preferida en particular, una realización de la presente invención depende de dos elementos de información de acuerdo con un método de construcción de una clave privada de acuerdo con una realización adicional.

"Algo que tienes" que en una forma preferida es la clave pública del lado del cliente. “Algo que sabes” que en una forma preferida es el PIN/contraseña de usuario que se utiliza para crear una clave privada para una sesión dada.

En una mejora adicional del ejemplo de realización la clave privada del par de claves del cliente pueden estar enlazada a un usuario específico del dispositivo del cliente para ejecutar una autenticación de dos factores. Esto se logra requiriendo que el usuario introduzca un PIN u otra “cosa que el usuario debe saber” con “una cosa que el usuario debe tener” en este caso una clave privada requerida de un par de claves de cliente válido en una autenticación de dos factores, utilizando el ejemplo de realización.

En esta mejora la clave privada 100 del par de claves 101 del cliente se rompe en dos componentes 102 103. El primer componente es un PIN 102 que es elegido por el usuario para verificar su identidad en futuras sesiones. Este PIN 102 se sustrae de una clave privada 100 completa para producir un elemento 103 de clave diferencial. El elemento 103 de clave diferencial no puede ser utilizado como una clave privada 100 exitosa en un par de claves 101 del cliente, a menos que el usuario añada un PIN 102 correcto al elemento 103 de clave diferencial correcto para producir una clave privada 100 utilizable del par de claves 101 utilizable.

El elemento de clave diferencial puede ser almacenado 104 de forma segura en el dispositivo del cliente para su uso en la siguiente sesión porque el elemento 104 no puede ser utilizado con éxito sin requerir el PIN 102.

En la práctica el PIN 102 sería solicitado al usuario al principio de cada sesión, a continuación se añadiría al elemento de clave 103 diferencial para establecer el cifrado y descifrado de datos de claves públicas exitoso.

Además, el PIN 102 se almacenaría temporalmente en el cliente y a continuación sería utilizado para generar un elemento 103 de clave diferencial adecuada para la clave privada 20 de la siguiente sesión.

El ejemplo de realización muestra el uso de un PIN como una “cosa que el usuario debe saber” para lograr una autenticación de dos factores. Una realización alternativa podría utilizar cualquier forma de información identificable personalmente que incluye, pero no se limita a, huellas del pulgar u otro tipo de biométrica.

El ejemplo de realización utiliza la substracción para producir un elemento de clave diferencial sustrayendo un PIN de una clave privada de un par de claves del lado del cliente. Una realización alternativa podría ser cualquier cálculo que permita que el factor identificable personalmente sea combinado con un segundo elemento de archivo para producir una clave privada utilizable en un par de claves del lado del cliente.

Lo anterior describe únicamente algunas realizaciones de la presente invención y pueden realizarse en la misma modificaciones obvias para aquellos expertos en el arte de la misma, sin apartarse del alcance de la presente invención.

Aplicabilidad industrial

Las realizaciones de la invención pueden ser aplicadas en contextos en los que se requiere que la autenticación de un aparato o un aparato más una combinación de usuarios sea verificada antes de una comunicación adicional con dicho aparato.

REIVINDICACIONES

1. Un método para mantener una autenticación continuada del usuario de una aplicación sin la necesidad de introducir y re-introducir un nombre de usuario y una contraseña correspondiente para cada sesión iniciada entre una aplicación del lado del cliente que reside en una plataforma del lado del cliente y un servidor; y en donde la contraseña no se almacena en el servidor; donde el método comprende utilizar una cadena ininterrumpida de códigos de acceso de un solo uso; donde cada código de acceso en la cadena es único para el nombre de usuario y la aplicación del lado del cliente; cada código de acceso renovado al menos una vez durante cada dicha sesión.

2. El método según la reivindicación 1, en donde el código de acceso comprende una clave pública del lado del cliente que se mantiene persistente tanto en la plataforma del lado del cliente como en el servidor hasta que es reemplazada por la siguiente clave pública del lado del cliente en la cadena de los códigos de acceso.

3. El método según la reivindicación 1 o 2 en donde la clave pública del lado del cliente comprende una clave pública de un par de claves PKI.

4. El método según la reivindicación 1 o 2 o 3 en donde la correspondiente clave privada del lado del cliente no es compartida con el servidor.

5. El método según cualquiera de las reivindicaciones 1 a 4, en donde la cadena ininterrumpida de códigos de acceso de un solo uso comprende una secuencia de códigos de acceso de un solo uso que son renovables y en donde la renovación se efectúa reemplazando los códigos de acceso a intervalos regulares.

6. El método según la reivindicación 5 en donde un intervalo comprende una conexión de una vez por sesión.

7. El método según la reivindicación 5 o 6 en donde el par de claves incluye una clave privada que es almacenada localmente en el dispositivo del cliente y una clave pública 19 que también es almacenada localmente y en donde la clave pública del cliente almacenada también es compartida con y transferida al servidor, el cual a continuación enlaza una referencia almacenada a la ID de usuario única de la persona que actualmente está utilizando el cliente con una copia almacenada de la clave pública de los clientes.

8. El método según la reivindicación 7 en donde durante conexiones posteriores entre el cliente y el servidor, la clave pública del cliente compartida y almacenada, la clave pública de los servidores y la clave privada almacenada en el cliente 20 se utilizan como los actuales pares de claves públicas del lado del cliente, y se genera y almacena a continuación un par de claves adicional para la siguiente sesión.

9. El método según la reivindicación 8 en donde la ID única es capturada o recuperada del usuario o del almacenamiento en el cliente y a continuación el par de claves del cliente almacenado durante la sesión previa es recuperado utilizando la ID de usuario única de los actuales usuarios a continuación de lo cual la ID única de los usuarios y la clave pública del cliente almacenada previamente son compartidas con el servidor.

10. Un dispositivo que incluye un procesador en comunicación con una memoria adaptada para ejecutar una aplicación; donde dicho dispositivo mantiene una autenticación continuada del usuario de una aplicación ejecutable en el dispositivo sin la necesidad de introducir y re-introducir un nombre de usuario y una correspondiente contraseña para cada sesión iniciada entre una aplicación del lado del cliente que reside en una plataforma del lado del cliente en el dispositivo y un servidor remoto; y en donde la contraseña no se almacena en el servidor; donde el método comprende utilizar una cadena ininterrumpida de códigos de acceso de un solo uso; donde cada código de acceso en la cadena es único para el nombre de usuario y la aplicación del lado del cliente; cada código de acceso renovado al menos una vez durante cada dicha sesión.

11. El dispositivo según la reivindicación 10 en donde el código de acceso comprende una clave pública del lado del cliente que se mantiene persistente tanto en la plataforma del lado del cliente como en el servidor hasta que es reemplazada por la siguiente clave pública del lado del cliente en la cadena de códigos de acceso.

12. El dispositivo según la reivindicación 10 u 11 en donde la clave pública del lado del cliente comprende una clave pública de un par de claves PKI.

13. El dispositivo según la reivindicación 10 u 11 en donde la correspondiente clave privada del lado del cliente no es compartida con el servidor.

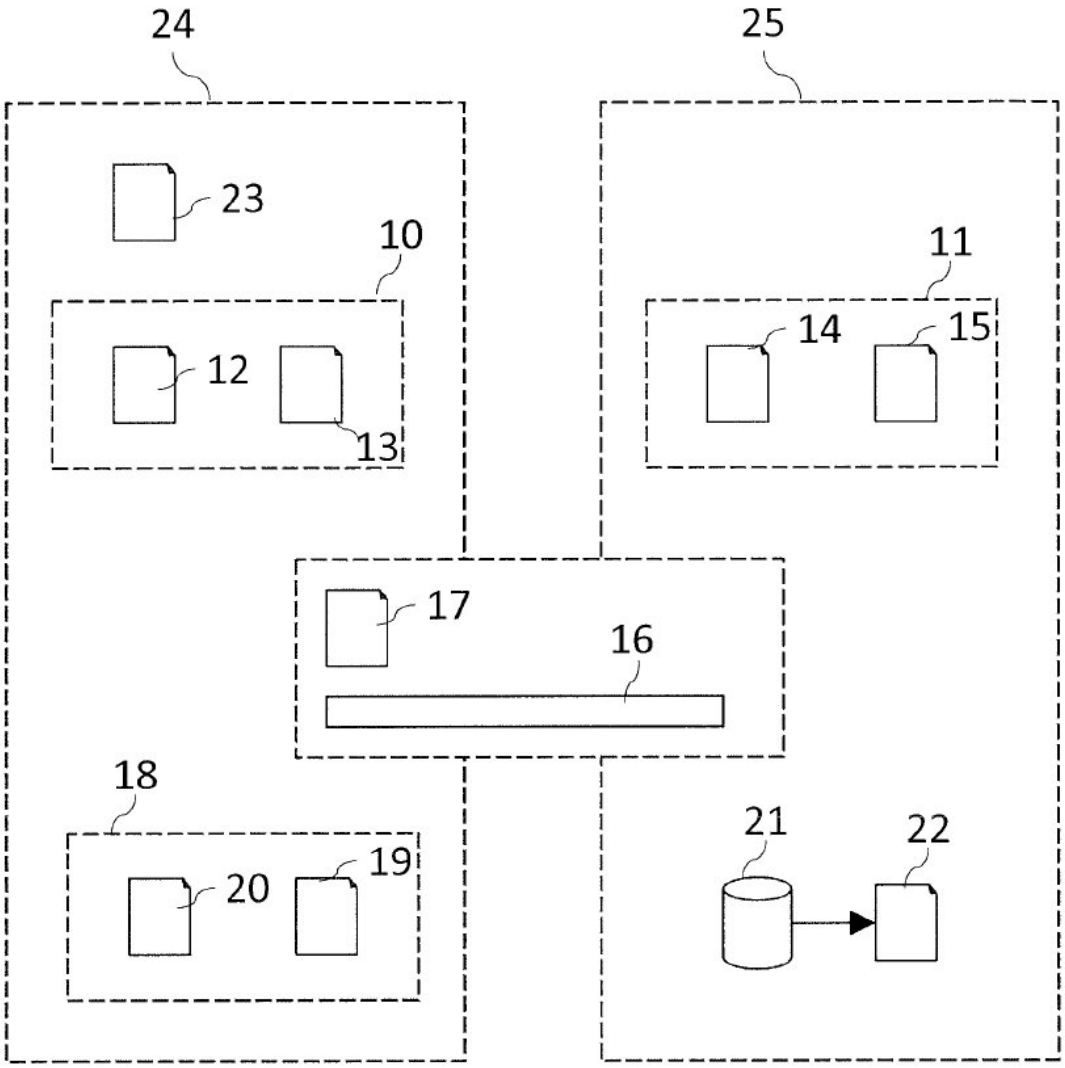
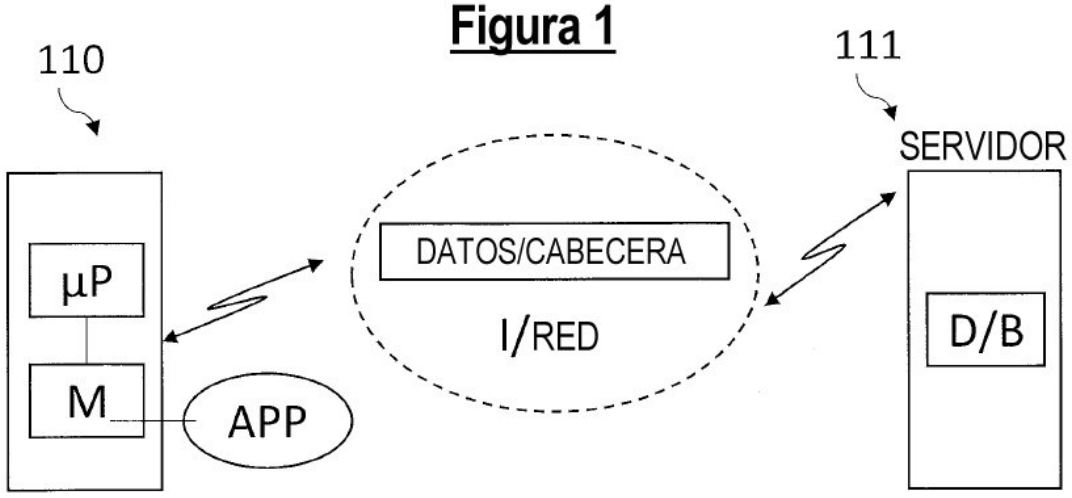

24
25
23
10
11
12
13
14
15
17
16
18
19
20
21
22

Figura 1


110
111
SERVIDOR
µP
M
APP
DATOS/CABECERA
I/RED
D/B

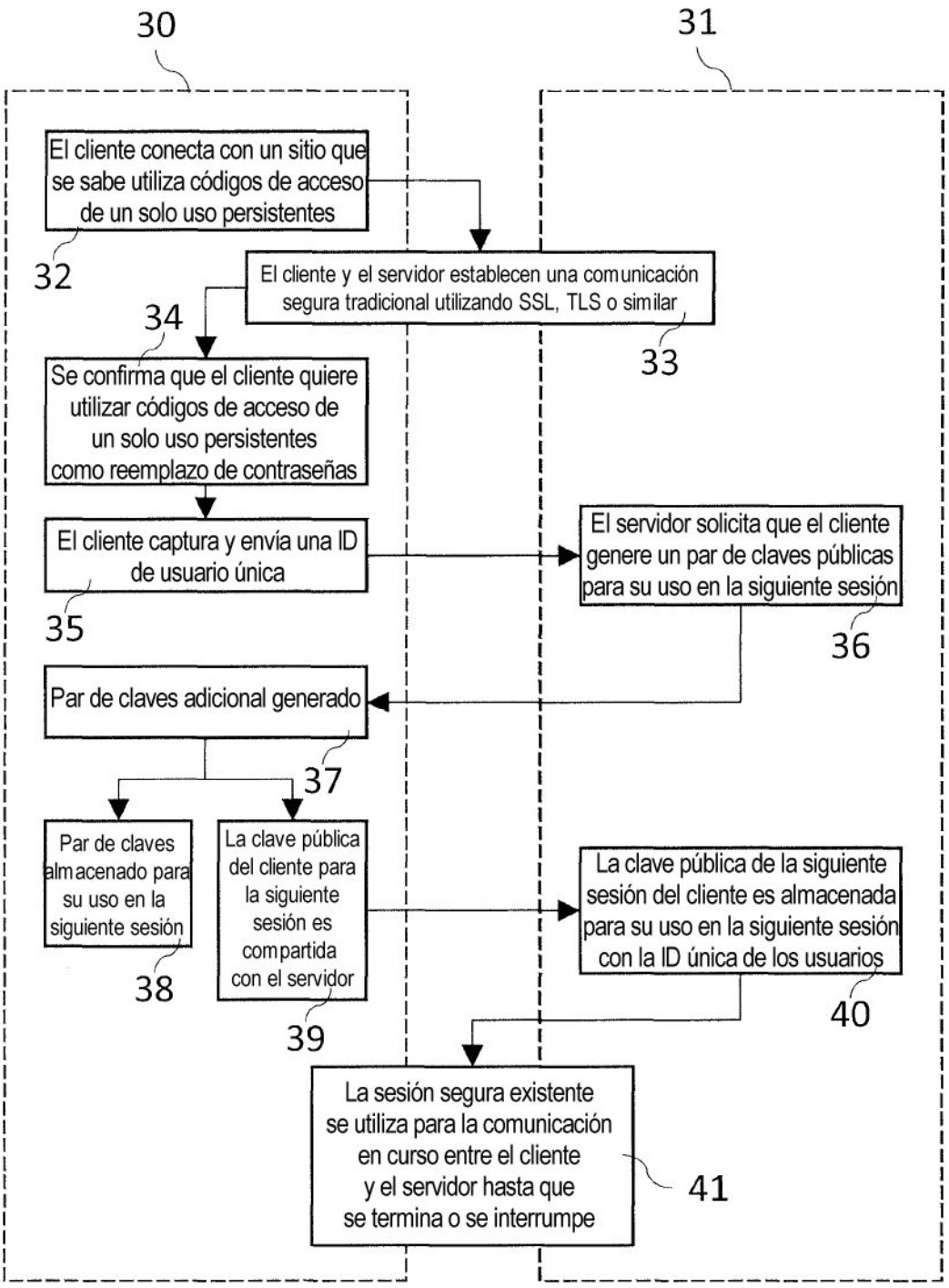

30
31
El cliente conecta con un sitio que se sabe utiliza códigos de acceso de un solo uso persistentes
32
El cliente y el servidor establecen una comunicación segura tradicional utilizando SSL, TLS o similar
33
34
Se confirma que el cliente quiere utilizar códigos de acceso de un solo uso persistentes como reemplazo de contraseñas
El cliente captura y envía una ID de usuario única
35
El servidor solicita que el cliente genere un par de claves públicas para su uso en la siguiente sesión
36
Par de claves adicional generado
37
Par de claves almacenado para su uso en la siguiente sesión
38
La clave pública del cliente para la siguiente sesión es compartida con el servidor
39
La clave pública de la siguiente sesión del cliente es almacenada para su uso en la siguiente sesión con la ID única de los usuarios
40
La sesión segura existente se utiliza para la comunicación en curso entre el cliente y el servidor hasta que se termina o se interrumpe
41

Figura 2

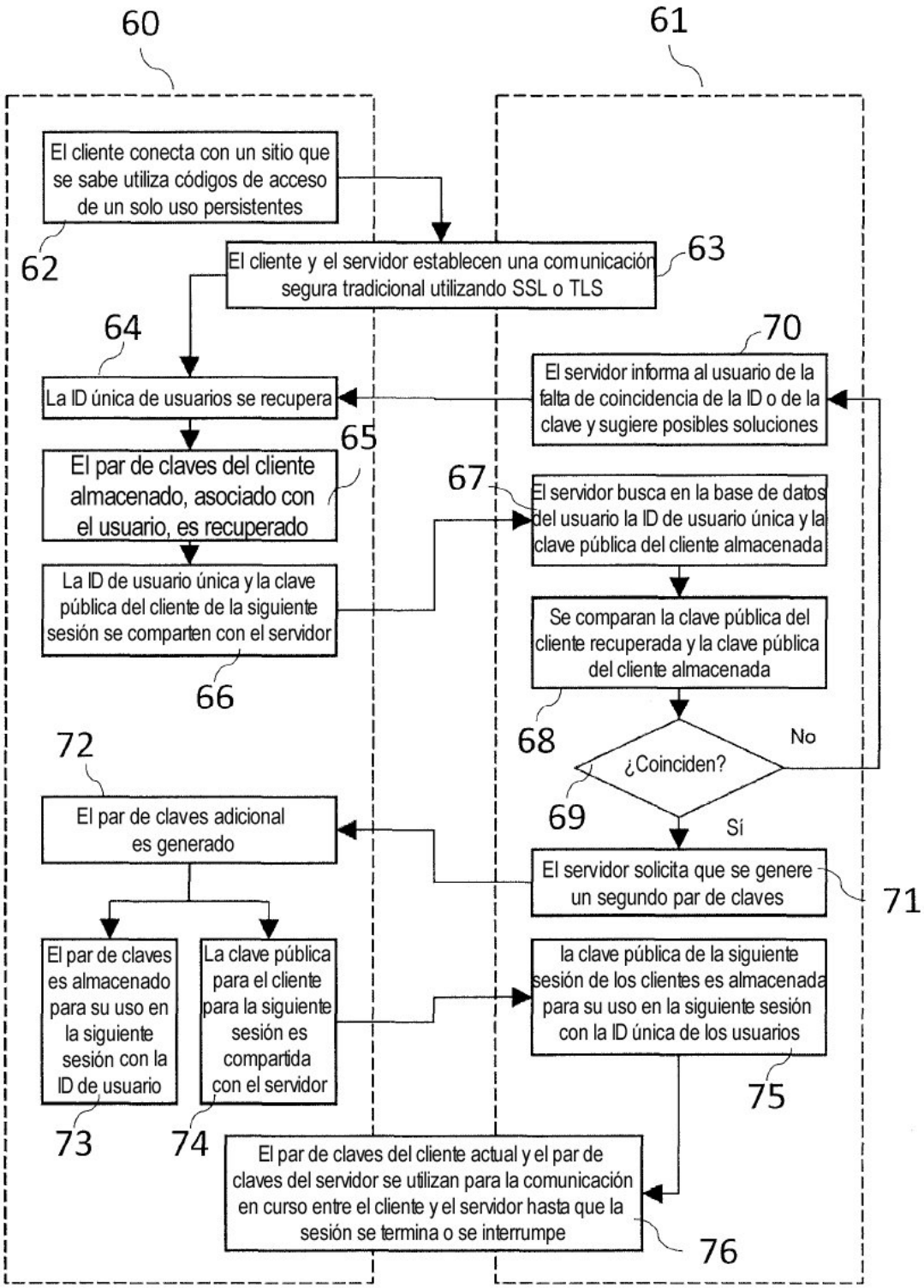

60
61
El cliente conecta con un sitio que se sabe utiliza códigos de acceso de un solo uso persistentes
62
El cliente y el servidor establecen una comunicación segura tradicional utilizando SSL o TLS
63
64
La ID única de usuarios se recupera
65
El par de claves del cliente almacenado, asociado con el usuario, es recuperado
La ID de usuario única y la clave pública del cliente de la siguiente sesión se comparten con el servidor
66
67
El servidor busca en la base de datos del usuario la ID de usuario única y la clave pública del cliente almacenada
Se comparan la clave pública del cliente recuperada y la clave pública del cliente almacenada
68
¿Coinciden?
69
No
Sí
70
El servidor informa al usuario de la falta de coincidencia de la ID o de la clave y sugiere posibles soluciones
El servidor solicita que se genere un segundo par de claves
71
72
El par de claves adicional es generado
El par de claves es almacenado para su uso en la siguiente sesión con la ID de usuario
73
La clave pública para el cliente para la siguiente sesión es compartida con el servidor
74
la clave pública de la siguiente sesión de los clientes es almacenada para su uso en la siguiente sesión con la ID única de los usuarios
75
El par de claves del cliente actual y el par de claves del servidor se utilizan para la comunicación en curso entre el cliente y el servidor hasta que la sesión se termina o se interrumpe
76

Figura 3

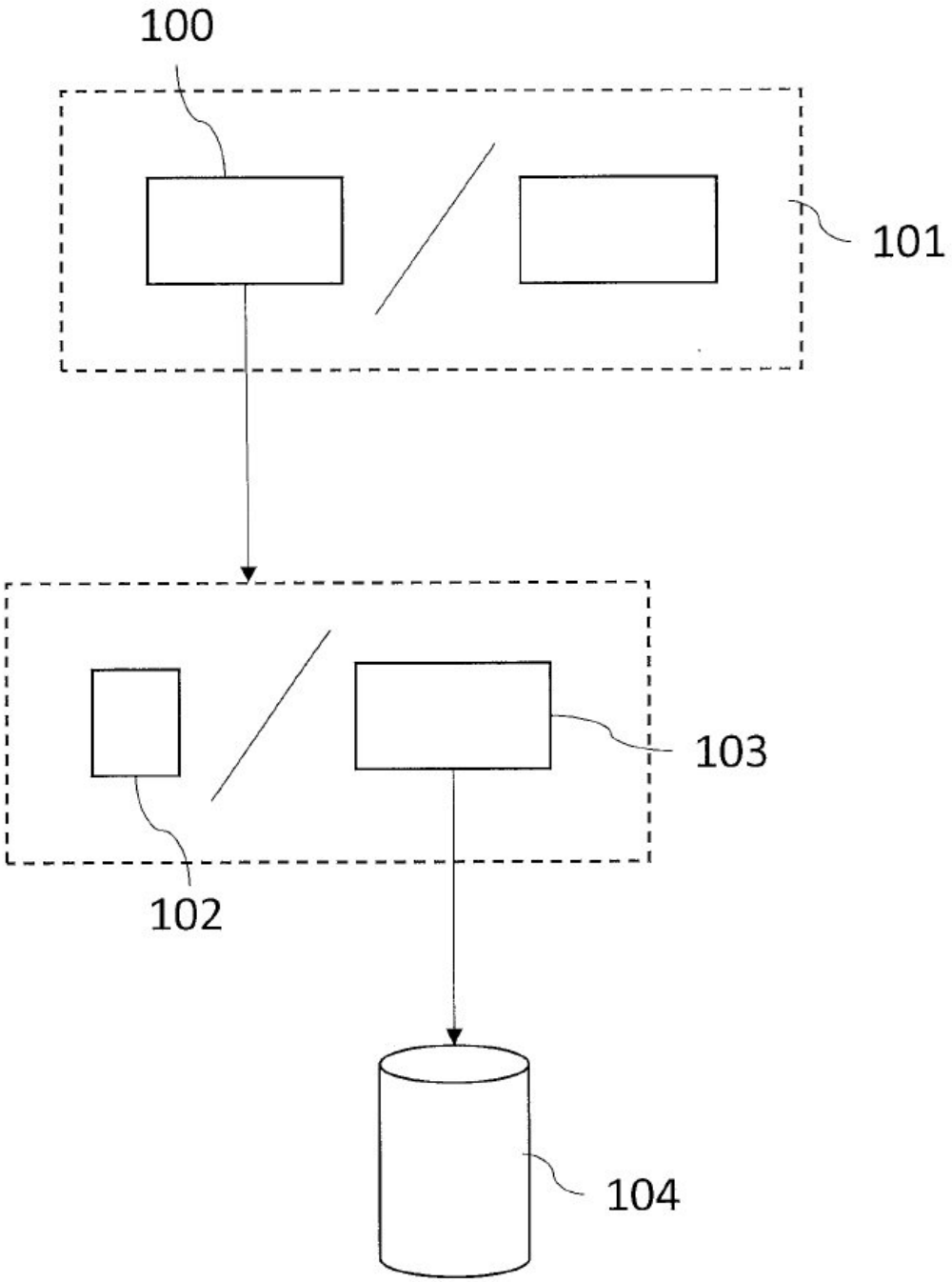


Figura 4