(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 680 152**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/35 (2013.01)
G06F 21/43 (2013.01)
H04L 9/32 (2006.01)
G06F 21/34 (2013.01)
G06F 21/60 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **02.08.2013 PCT/US2013/053433**

(87) Fecha y número de publicación internacional: **06.02.2014 WO14022778**

(96) Fecha de presentación y número de la solicitud europea: **02.08.2013 E 13748438 (2)**

(97) Fecha y número de publicación de la concesión europea: **25.04.2018 EP 2885904**

(54) Título: **Método y aparato de autenticación conveniente para el usuario usando una aplicación de autenticación móvil**

(30) Prioridad:

03.08.2012 US 201261679284 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.09.2018

(73) Titular/es:

ONESPAN INTERNATIONAL GMBH (100.0%)
World-Wide Business Center Balz-Zimmermannstrasse 7
8152 Glattbrugg, CH

(72) Inventor/es:

FORT, NICOLAS;
COULIER, FRANK y
TEIXERON, GUILLAUME

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método y aparato de autenticación conveniente para el usuario usando una aplicación de autenticación móvil

Campo de la invención

La invención se refiere a asegurar el acceso remoto a ordenadores y aplicaciones y transacciones remotas a través de redes informáticas. Más específicamente, la invención se refiere a métodos y aparatos para autenticar usuarios a servidores de aplicación remotos.

Antecedentes de la invención

A medida que el acceso remoto de los sistemas informáticos y aplicaciones crece en popularidad, el número y diversidad de transacciones a las que se accede remotamente a través de redes públicas tales como Internet ha aumentado drásticamente. Esta popularidad tiene subrayada una necesidad de seguridad; en particular: cómo asegurar que las personas que acceden remotamente a una aplicación son quien reivindican ser, cómo asegurar que las transacciones que se están realizando remotamente se inician por individuos legítimos, y cómo asegurar que los datos de transacción no se han modificado antes de recibirse en un servidor de aplicación.

En el pasado, los proveedores de aplicación se han basado en contraseñas estáticas para proporcionar la seguridad para aplicaciones remotas. En los últimos años se ha hecho evidente que las contraseñas estáticas no son suficientes y que se requiere tecnología de seguridad más avanzada.

Una tecnología de autenticación que ofrece un nivel de seguridad significativamente superior que las contraseñas estáticas se ofrece por 'dispositivos de testigo de autenticación fuertes'. Ejemplos típicos de testigos de autenticación fuertes son los productos de la línea DIGIPASS®, comercializados por Vasco Data Security Inc. de Chicago, Illinois (véase el sitio web http://www.vasco.com). Un testigo de autenticación fuerte es un dispositivo alimentado por batería autónomo, especializado para proporcionar funciones de autenticación y/o firma de transacción, normalmente de tamaño de bolsillo, con su propia pantalla y teclado numérico. En algunos casos el teclado numérico se reduce a un único botón o incluso se omite completamente, en otros casos el teclado numérico puede ser un teclado completo. La pantalla y el teclado numérico de un testigo de autenticación fuerte típico son no extraíbles, y no son utilizables para el usuario, controlados completamente por el testigo, e inmunes para interferencia por software malicioso en un ordenador anfitrión. Por lo tanto, se considera que los testigos de autenticación fuertes tienen una interfaz de usuario confiable en contraste a, por ejemplo, los PC donde hay siempre la posibilidad de que software malicioso tal como un virus o un troyano presente mensajes falsos al usuario, o capture lo que el usuario introduzca en el teclado numérico, o lea en memoria datos sensibles asociados con una aplicación de seguridad o modifique datos antes de que se firmen. El fin principal de un testigo de autenticación fuerte es generar valores de seguridad dinámicos que se denominan normalmente como 'Contraseñas de Un Solo Uso' (OTP) o contraseñas dinámicas. Típicamente estas OTP se generan combinando criptográficamente un secreto que se comparte entre el testigo y un servidor de verificación o de autenticación con un valor dinámico tal como un valor de tiempo, un valor de contador o un desafío de servidor que se proporciona al testigo, o una combinación de estos. Algunos testigos de actualización fuertes pueden usar también datos (tales como datos de transacción) que se han proporcionado al testigo como el valor dinámico o en combinación con cualquiera de los valores dinámicos anteriormente mencionados para generar un valor de seguridad. En estos casos el valor de seguridad resultante se pretende para indicar la aprobación del usuario de los datos y el valor de seguridad normalmente se denomina como una firma electrónica o Código de Autenticación de Mensaje (MAC). En algunos casos combinando criptográficamente el secreto con un valor dinámico comprende realizar una encriptación simétrica o algoritmo de desencriptación (tal como por ejemplo DES, 3DES o AES) a través de datos relacionados con el valor dinámico y usar el secreto como una encriptación simétrica o clave de desencriptación. En algunos casos combinando criptográficamente el secreto con un valor dinámico comprende realizar una función de troceo criptográfico (tal como por ejemplo SHA-1) que se codifica con el secreto y usar los datos relacionados con el valor dinámico como datos de entrada para la función de troceo. Algunos testigos de autenticación fuertes consisten en un dispositivo con una pantalla y un teclado numérico que puede comunicar con una tarjeta inteligente insertada mediante la cual la generación de las OTP o MAC se realiza parcialmente por el mismo dispositivo y parcialmente por la tarjeta inteligente insertada.

Una manera típica de proporcionar datos a un testigo de autenticación fuerte es dejando que el usuario introduzca los datos manualmente en el teclado numérico del testigo. Cuando la cantidad de datos que ha de introducirse de esta manera supera unas pocas docenas de caracteres, este proceso puede percibirse por los usuarios como demasiado engorroso.

Una manera típica de proporcionar las OTP o MAC generadas desde el testigo de autenticación al sistema que necesita verificarlas, consiste en visualizar el testigo la OTP o MAC generada en su pantalla y copiar el usuario la OTP o MAC visualizada en su PC (u otro dispositivo de acceso a Internet) que transmite esta OTP o MAC a la aplicación o servidor de autenticación donde puede a continuación verificarse la validez de la OTP o MAC. Sin embargo, esto también requiere algunas acciones del usuario que pueden percibirse como inconvenientes.

Los testigos de autenticación fuertes normalmente se basan en mecanismos criptográficos simétricos para generar OTP o MAC usando claves secretas simétricas que se han de compartir entre un testigo de autenticación fuerte y un

servidor de verificación. Esto puede ser un problema si un usuario desearía usar su testigo con varias aplicaciones puesto que todos estos servidores de aplicación tendrían entonces que compartir la clave o claves secretas del testigo que a su vez tiene el potencial de crear riesgos de seguridad.

Otro aspecto de testigos de autenticación fuerte de hardware especializado es que inevitablemente tienen un cierto coste mínimo que no es cero. Esto puede hacer en ocasiones a los testigos de autenticación fuertes de hardware especializado menos atractivos para un número de aplicaciones para las que el coste por usuario puede en ocasiones ser un factor crítico.

El documento WO2009/101549 A2 describe un sistema donde el testigo de autenticación fuerte es un dispositivo móvil del usuario, que genera credenciales de usuario para servicios que se accede por un terminal remoto.

Lo que es necesario es un mecanismo de autenticación que ofrezca, por un lado, el mismo nivel de seguridad que los testigos de autenticación fuertes, pero que por otra parte sea muy conveniente para el usuario y pueda usarse fácilmente con varias aplicaciones o proveedores de aplicación y sea muy económico.

Descripción de la invención

La invención se define en las reivindicaciones 1, 14 y 17, respectivamente. Se exponen realizaciones particulares en las reivindicaciones dependientes.

Los aspectos de la presente invención están basados en una combinación de ideas por los inventores tales como, por ejemplo, la idea de los inventores de que pueden asegurarse varias diferentes aplicaciones con el mismo testigo de autenticación fuerte sin la necesidad de que estas diferentes aplicaciones compartan todas los secretos del testigo si estas aplicaciones pueden basarse en la verificación de las OTP y MAC generadas por ese testigo en un servidor de autenticación de terceros que es confiable por las aplicaciones y que tiene acceso a los testigos secretos.

Una idea adicional en la que están basados los aspectos de la invención es que el proceso de autenticación puede hacerse muy conveniente para el usuario si el dispositivo del usuario que genera las OTP o MAC comprende interfaces de comunicación para intercambiar datos con dispositivos informáticos mediante los cuales estas interfaces de comunicación puede suponerse que están omnipresentes con respecto a las aplicaciones dirigidas (p. ej. aplicaciones basadas en web) y los dispositivos de acceso típicos, p. ej. Ordenadores Personales (PC) o portátiles, que puede esperarse que los usuarios usen para acceder a estas aplicaciones sin requerir que los usuarios participen en etapas técnicas potencialmente complicadas y propensas a errores tales como son instalar controladores para estas interfaces de comunicación.

Otra idea en la que están basados los aspectos de la invención es que la solución puede ser muy rentable y es posible re-utilizar un dispositivo, tal como por ejemplo un teléfono móvil, que el usuario ya tiene de cualquier manera en lugar de tener que distribuir nuevos dispositivos de hardware especializados.

Dispositivos de autenticación

En algunas realizaciones de la invención se proporciona a cada usuario de una pluralidad de usuarios con un dispositivo de autenticación. En algunas realizaciones el dispositivo de autenticación es un dispositivo de hardware especializado tal como un testigo de autenticación fuerte especializado. En otras realizaciones el dispositivo de autenticación comprende un dispositivo de cliente electrónico móvil, tal como, por ejemplo, un teléfono inteligente o un asistente digital personal (PDA). En algunas realizaciones el dispositivo de cliente electrónico móvil portátil está equipado con una aplicación de software de autenticación. En algunas realizaciones el dispositivo de autenticación se ha personalizado con al menos un valor secreto que el dispositivo de autenticación puede usar, directa o indirectamente, en la generación de valores de seguridad dinámicos como se explica a continuación.

Generación de valores de seguridad dinámicos.

En algunas realizaciones el dispositivo de autenticación está adaptado para generar valores de seguridad dinámicos. En algunas realizaciones los valores de seguridad dinámicos generados pueden comprender contraseñas de un solo uso o dinámicas, y/o respuestas a desafíos y/o firmas electrónicas en datos de transacción. En algunas realizaciones el dispositivo de autenticación está adaptado para presentar valores de seguridad dinámicos generados al usuario. En algunas realizaciones los valores de seguridad dinámicos se generan combinando criptográficamente al menos un valor secreto (tal como una clave criptográfica) con al menos una variable dinámica (tal como un valor de tiempo y/o un valor de contador y/o un desafío y/o datos relacionados con transacción o cualquier combinación de estos). En algunas realizaciones la combinación criptográfica comprende realizar un algoritmo criptográfico. En algunas realizaciones el algoritmo criptográfico puede comprender una encriptación simétrica o algoritmo de desencriptación tal como DES, 3DES o AES. En algunas realizaciones el algoritmo criptográfico puede comprender un troceo o algoritmo de troceo con clave tal como SHA-1.

En algunas realizaciones el dispositivo de autenticación puede usar también una aplicación que identifica el elemento de datos, por ejemplo un identificador de aplicación, cuando se genera un valor de seguridad dinámico. En

algunas realizaciones el dispositivo de autenticación combina criptográficamente el identificador de aplicación con el al menos un valor secreto y posiblemente otros datos, tales como la al menos una variable dinámica para generar un valor de seguridad dinámico.

Manejo de PIN.

En algunas realizaciones el dispositivo de autenticación está adaptado para recibir un PIN o valor de contraseña proporcionado por el usuario. En algunas realizaciones el dispositivo de autenticación está adaptado para pasar un PIN o valor de contraseña proporcionado por el usuario a un segundo dispositivo de seguridad (tal como una tarjeta inteligente) para verificación. En algunas realizaciones el dispositivo de autenticación está adaptado para eliminar de su memoria cualquier copia en cualquier formato de un valor de PIN de este tipo una vez que se ha verificado ese valor de PIN. En algunas realizaciones el dispositivo de autenticación se ha adaptado para borrar o sobrescribir de manera activa las localizaciones de memoria donde un valor de PIN de este tipo se ha almacenado temporalmente después de que se ha verificado el valor de PIN. En algunas realizaciones el dispositivo de autenticación almacena un valor de referencia que está relacionado matemáticamente con un valor correcto para el PIN o contraseña que se espera que se proporcione por el usuario y el dispositivo de autenticación está adaptado para comparar un PIN o valor de contraseña proporcionado por un usuario a ese valor de referencia. En algunas realizaciones el dispositivo de autenticación está adaptado para generar el valor secreto usando un PIN o valor de contraseña proporcionado por el usuario. En algunas realizaciones el dispositivo de autenticación almacena un valor que comprende el valor secreto que está encriptado con una clave de encriptación que se deriva desde un PIN o valor de contraseña proporcionado por el usuario y el dispositivo de autenticación está adaptado para derivar un valor de clave de encriptación desde un PIN o valor de contraseña proporcionado por el usuario y usar ese valor de clave de encriptación para desencriptar el valor secreto encriptado que puede usarse a continuación p. ej. para generar un valor de seguridad dinámico.

Interfaces de comunicación

En algunas realizaciones el dispositivo de autenticación puede estar en red. En algunas realizaciones el dispositivo de autenticación puede comprender una interfaz de comunicación de datos para intercambiar datos a través de una red informática. En algunas realizaciones la interfaz de comunicación puede comprender una interfaz de comunicación inalámbrica p. ej. para comunicar con una red de telefonía móvil. En algunas realizaciones el dispositivo de autenticación puede adaptarse para enviar y/o recibir datos relacionados con autenticación a un servidor a través de una red informática. En algunas realizaciones el dispositivo de autenticación está adaptado para comunicar datos a través de la Internet. En algunas realizaciones el dispositivo de autenticación comprende una pila de TCP/IP (Protocolo de Control de Transmisión / Protocolo de Internet). En algunas realizaciones el dispositivo de autenticación está adaptado para intercambiar datos a través de una conexión de SSL (Capa de Conexiones Segura) y/o TLS (Seguridad de Capa de Transporte). En algunas realizaciones el dispositivo de autenticación está adaptado para enviar y/o recibir mensajes de HTTP (Protocolo de Transferencia de Hipertexto) y/o HTTPS (Protocolo de Transferencia de Hipertexto Seguro)

Mensaje de iniciación de autenticación

En algunas realizaciones el dispositivo de autenticación puede estar adaptado para recibir un mensaje de iniciación de autenticación. En una realización de la invención el mensaje de iniciación de autenticación puede incluir un desafío (p. ej., un número aleatorio o troceo de datos de transacción que puede procesarse para fines de autenticación/validación). En otra realización de la invención el mensaje de iniciación de autenticación incluye datos relacionados con transacción que incluyen valores de transacción o información de contexto de transacción. En algunas realizaciones la información de contexto de transacción puede incluir etiquetas de datos de transacción y/o información con respecto al significado de los datos relacionados con transacción. En algunas realizaciones el mensaje de iniciación de autenticación incluye información relacionada con el flujo de aplicación. En algunas realizaciones la información relacionada con el flujo de aplicación puede incluir información con respecto al tipo de transacción. En algunas realizaciones la información relacionada con el flujo de aplicación puede guiar al dispositivo de autenticación con respecto a la manera en la que el dispositivo de autenticación debería manejar los datos relacionados con transacción recibidos y/o cómo el dispositivo de autenticación debería manejar el flujo de interacción de usuario, por ejemplo qué datos deberían presentarse al usuario para revisión y/o aprobación y si debería consultarse al usuario o proporcionarse la oportunidad para corregir datos o proporcionar manualmente datos adicionales y/o qué mensajes deberían presentarse al usuario.

En algunas realizaciones el dispositivo de autenticación puede comprender componentes ópticos para recibir información óptica. En algunas realizaciones el mensaje de iniciación de autenticación puede codificarse como una señal óptica emitida por el dispositivo de acceso del usuario (p. ej. como un patrón dinámico o estático visualizado en la pantalla del dispositivo de acceso) y recibirse y decodificarse por el dispositivo de autenticación del usuario. En algunas realizaciones el dispositivo de autenticación puede comprender una cámara y el mensaje de iniciación de autenticación puede codificarse como una o más instantáneas o imágenes visualizadas en la pantalla del dispositivo de acceso y capturarse por la cámara del dispositivo de autenticación. En algunas realizaciones el mensaje de iniciación de autenticación puede codificarse como un código de QR (Código de Respuesta Rápida) que el dispositivo de autenticación lee con su cámara y decodifica para obtener el mensaje de iniciación de autenticación

real. En algunas realizaciones el mensaje de iniciación de autenticación puede codificarse usando más de un código de QR. En algunas realizaciones el mensaje de iniciación de autenticación puede comprender o tomar la forma de un URL.

Credencial de servidor

En algunas realizaciones el mensaje de iniciación de autenticación puede incluir una credencial de servidor que se ha generado criptográficamente por un servidor (que puede ser por ejemplo un servidor de aplicación o el servidor de autenticación). En algunas realizaciones el servidor ha generado la credencial del servidor usando una clave criptográfica simétrica y una clave secreta que se comparte con el dispositivo de autenticación o un segundo dispositivo de seguridad con el que se comunica el dispositivo de autenticación. En algunas realizaciones el dispositivo de autenticación está adaptado para verificar la credencial del servidor. En algunas realizaciones el dispositivo de autenticación está adaptado para verificar la credencial del servidor en cooperación con un segundo dispositivo de seguridad. En algunas realizaciones la verificación de la credencial del servidor se hace usando un algoritmo criptográfico simétrico que usa una clave secreta compartida con el servidor. En algunas realizaciones la credencial del servidor comprende una contraseña de un solo uso de servidor. En algunas realizaciones la credencial del servidor comprende una firma de datos. En algunas realizaciones la credencial del servidor comprende un código de autenticación de mensaje (MAC). En algunas realizaciones la credencial del servidor comprende datos de entrada encriptados. En algunas realizaciones el fin de la credencial del servidor es autenticar un servidor o aplicación de servidor. En algunas realizaciones el fin de la credencial del servidor es autenticar datos de entrada (que pueden estar comprendidos en el mensaje de iniciación de autenticación) recibidos por el dispositivo de autenticación desde un servidor. En algunas realizaciones el fin de la credencial del servidor es proteger la integridad de datos de entrada (que pueden estar comprendidos en el mensaje de iniciación de autenticación) recibidos por el dispositivo de autenticación desde un servidor. En algunas realizaciones el fin de la credencial del servidor es proteger la confidencialidad de datos de entrada (que pueden estar comprendidos en el mensaje de iniciación de autenticación) recibidos por el dispositivo de autenticación desde un servidor. En algunas realizaciones el fin de la credencial del servidor es enlazar criptográficamente juntos los datos de entrada (que pueden estar comprendidos en el mensaje de iniciación de autenticación) recibidos por el dispositivo de autenticación desde un servidor. En algunas realizaciones la generación de valores de seguridad dinámicos por el dispositivo de autenticación puede estar condicionada a la verificación satisfactoria de la credencial del servidor.

Identificador de sesión de autenticación

En algunas realizaciones el mensaje de iniciación de autenticación puede incluir un elemento de datos para identificar la sesión de autenticación, por ejemplo un identificador de sesión de autenticación. En algunas realizaciones un identificador de sesión de autenticación de este tipo, o de manera corta ID de sesión, puede comprender un número de secuencia. En algunas realizaciones el ID de sesión puede comprender un número generado aleatoriamente. En algunas realizaciones el ID de sesión puede generarse por un servidor de aplicación. En algunas realizaciones el ID de sesión puede generarse por un servidor de autenticación. En alguna realización el ID de sesión puede usarse por un dispositivo de autenticación que recibe el mensaje de iniciación de autenticación en la generación de un valor de seguridad dinámico.

Identificador de aplicación

En algunas realizaciones el mensaje de iniciación de autenticación puede incluir un elemento de datos para identificar una aplicación o proveedor de aplicación, p. ej. un identificador de aplicación. En algunas realizaciones el identificador de aplicación puede identificar la aplicación o el proveedor de aplicación para los que se supone que el dispositivo de autenticación del usuario genera un valor de seguridad dinámico. En algunas realizaciones el dispositivo de autenticación está adaptado para usar un valor relacionado con un identificador de aplicación comprendido en un mensaje de iniciación de autenticación en el cálculo de un valor de seguridad dinámico. En algunas realizaciones el identificador de aplicación comprende una representación de la aplicación o el proveedor de aplicación que el usuario puede reconocer como que identifica la aplicación o el proveedor de aplicación y el dispositivo de autenticación está adaptado para presentar esa representación al usuario. En algunas realizaciones el identificador de aplicación comprende un elemento de datos digitales y el dispositivo de autenticación está adaptado para usar ese elemento de datos digitales para recuperar una representación de la aplicación de proveedor de aplicación que el usuario puede reconocer como que identifica la aplicación o el proveedor de aplicación y el dispositivo de autenticación está adaptado para presentar esa representación al usuario. En algunas realizaciones la representación puede comprender un nombre o un logo. En algunas realizaciones la representación puede comprender sonidos (p. ej. una representación de voz de un nombre que el usuario puede usar para identificar la aplicación o el proveedor de aplicación, o una melodía de identificación musical que el usuario puede asociar con la aplicación o el proveedor de aplicación). En algunas realizaciones el dispositivo de autenticación puede presentar la representación visualizando datos visuales en una pantalla. En algunas realizaciones el dispositivo de autenticación puede presentar la representación al usuario emitiendo sonidos de audio, que pueden comprender por ejemplo voz o música.

En algunas realizaciones el dispositivo de autenticación está adaptado para generar un valor de seguridad dinámico tras recibir un mensaje de iniciación de autenticación. El dispositivo de autenticación puede estar adaptado

adicionalmente para extraer un identificador de aplicación desde el mensaje de iniciación de autenticación y para presentar la correspondiente representación de aplicación o proveedor de aplicación al usuario y para capturar la aprobación del usuario de si generar un valor de seguridad dinámico para esa aplicación o proveedor de aplicación y generar el valor de seguridad dinámico en la condición de que el usuario aprobó hacer eso.

Dirección de destino

En algunas realizaciones el mensaje de iniciación de autenticación puede incluir una dirección de destino. En algunas realizaciones la dirección de destino puede comprender una dirección de red de un servidor a la que el dispositivo de autenticación puede enviar datos o uno o más mensajes. En algunas realizaciones esta puede ser la dirección de red de un servidor de aplicación. En algunas realizaciones esta puede ser la dirección de red de un servidor de autenticación. En algunas realizaciones la dirección de destino puede comprender una dirección de IP. En algunas realizaciones la dirección de destino puede comprender un nombre de dominio. En algunas realizaciones la dirección de destino puede comprender un URL (Localizador de Recurso Uniforme) o URI (Identificador de Recurso Uniforme). En algunas realizaciones la dirección de destino puede comprender una dirección de destino de un servidor donde el dispositivo de autenticación puede enviar un valor de seguridad dinámico generado.

Mensaje de respuesta

En algunas realizaciones el dispositivo de autenticación está adaptado para generar un mensaje de respuesta después de que se ha generado un valor de seguridad dinámico. En algunas realizaciones el mensaje de respuesta puede comprender el valor de seguridad dinámico. En algunas realizaciones el mensaje de respuesta puede comprender un elemento de datos que identifica la aplicación o el proveedor de aplicación para los que se ha generado el valor de seguridad dinámico. Este elemento de datos que identifica la aplicación o el proveedor de aplicación puede comprender, por ejemplo, el identificador de aplicación comprendido en el mensaje de iniciación de autenticación recibido por el dispositivo de autenticación. En algunas realizaciones el mensaje de respuesta puede comprender un elemento de datos que identifica el dispositivo de autenticación (p. ej. un número de serie). En algunas realizaciones el mensaje de respuesta puede comprender un elemento de datos que identifica al usuario, p. ej., un nombre de usuario o un ID de usuario (identificador de usuario). En algunas realizaciones el mensaje de respuesta puede comprender un elemento de datos que identifica la sesión para la que se genera el valor de seguridad dinámico. Esto puede comprender, por ejemplo, un id de sesión comprendido en el mensaje de iniciación de autenticación recibido por el dispositivo de autenticación.

En algunas realizaciones el dispositivo de autenticación puede adaptarse para enviar el mensaje de respuesta a un servidor a través de una red informática. En algunas realizaciones el dispositivo de autenticación puede adaptarse para enviar el mensaje de respuesta a un servidor a través de la Internet. En algunas realizaciones el dispositivo de autenticación puede adaptarse para enviar el mensaje de respuesta a un servidor en un mensaje de IP. En algunas realizaciones el dispositivo de autenticación puede adaptarse para enviar el mensaje de respuesta a un servidor en un mensaje de HTTP, por ejemplo un mensaje POST de HTTP, en algunas realizaciones el dispositivo de autenticación puede enviar el mensaje de respuesta al servidor de aplicación. En algunas realizaciones el dispositivo de autenticación puede enviar el mensaje de respuesta a un servidor de autenticación. En algunas realizaciones la dirección de destino del servidor al que el dispositivo de autenticación necesita enviar el mensaje de respuesta puede almacenarse en el dispositivo de autenticación. En algunas realizaciones el dispositivo de autenticación usa una aplicación que identifica el elemento de datos (tal como por ejemplo un identificador de aplicación comprendido en el mensaje de iniciación de autenticación recibido por el dispositivo de autenticación) para recuperar la dirección de destino para el mensaje de respuesta. En algunas realizaciones el dispositivo de autenticación usa una dirección de destino comprendida en el mensaje de iniciación de autenticación recibido por el dispositivo de autenticación para recuperar la dirección de destino para el mensaje de respuesta. En algunas realizaciones ese dispositivo de autenticación aplica un filtro cuando recupera la dirección de destino. En algunas realizaciones el dispositivo de autenticación mantiene una lista blanca de direcciones de destino permitidas y compara la dirección de destino recuperada con esa lista blanca y declina enviar el mensaje de respuesta si la dirección de destino recuperada no coincide con la de esa lista blanca. Por ejemplo en algunas realizaciones el mensaje de iniciación de autenticación comprende el nombre de dominio del servidor para enviar el mensaje de respuesta y el dispositivo de autenticación compara ese nombre de dominio a una lista de nombres de dominio permitidos.

Servidor de autenticación.

En algunas realizaciones las claves secretas de los dispositivos de autenticación se comparten con un servidor de autenticación. En algunas realizaciones el servidor de autenticación puede comprender uno o más ordenadores de servidor que ejecutan una o más aplicaciones de software. En algunas realizaciones el servidor de autenticación comprende una base de datos que almacena los valores de las claves secretas (o valores equivalentes) de los dispositivos de autenticación. En algunas realizaciones el servidor de autenticación almacena uno o más secretos que, en algunas realizaciones, un valor secreto que se almacena en la base de datos se enlaza a un valor de identificación (tal como un número de serie) del dispositivo de autenticación correspondiente o está enlazado a un valor de identificación (tal como un nombre de usuario) de un usuario asociado con el correspondiente dispositivo de autenticación. En algunas realizaciones el servidor de autenticación almacena un secreto maestro y está adaptado para regenerar o derivar el valor secreto de un dispositivo de autenticación usando el secreto maestro y un valor de

identificación del dispositivo de autenticación o un usuario asociado con el dispositivo de autenticación. En algunas realizaciones el servidor de autenticación está adaptado para verificar valores de seguridad dinámicos generados por los dispositivos de autenticación. En algunas realizaciones el servidor de autenticación usa un valor secreto (que puede recuperar desde almacenamiento o regeneración como se ha explicado anteriormente) asociado con el dispositivo de autenticación para verificar un valor de seguridad dinámico que se supone que se ha generado con ese dispositivo de autenticación.

En algunas realizaciones el servidor de autenticación puede comprender una o más bases de datos para almacenar datos. En algunas realizaciones el servidor de autenticación puede usar y/o almacenar datos relacionados con el usuario. En algunas realizaciones el servidor de autenticación puede usar y/o almacenar datos relacionados con el dispositivo de autenticación. En algunas realizaciones los datos relacionados con el usuario o el dispositivo de autenticación comprenden una o más claves secretas. En algunas realizaciones una o más de estas claves secretas puede compartirse con el dispositivo de autenticación del usuario.

Otro aspecto más de la invención comprende un método para asegurar una aplicación basada en servidor remoto que se accede por un usuario a través de un dispositivo de acceso, que comprende un dispositivo informático tal como el PC o portátil del usuario, que comunica con el servidor de aplicación a través de una red informática p. ej. la Internet. El método puede comprender las siguientes etapas.

- Hacer disponible a un usuario un dispositivo de autenticación como se ha analizado anteriormente. En algunas realizaciones esto comprende distribuir dispositivos de autenticación que comprenden un testigo de autenticación de hardware especializado. En algunas realizaciones esto comprende hacer disponible una aplicación de software de autenticación para descarga e instalación en un dispositivo de cliente electrónico móvil portátil, tal como por ejemplo un teléfono inteligente o un asistente digital personal (PDA). En algunas realizaciones esto comprende adicionalmente personalizar el dispositivo de autenticación con datos de personalización. En algunas realizaciones los datos de personalización pueden comprender un valor secreto. En algunas realizaciones los datos de personalización pueden comprender un valor de dispositivo de autenticación tal como, por ejemplo, un número de serie. En algunas realizaciones la personalización comprende carga de datos de personalización en un testigo de autenticación fuerte de hardware antes de que el testigo se distribuya a un usuario. En algunas realizaciones la personalización comprende intercambiar el dispositivo de autenticación mensajes de personalización con un servidor de personalización.

- Registrar un dispositivo de autenticación y/o usuario con un servidor de autenticación.

- Activar una aplicación para uno o más usuarios.

- Ensamblar un mensaje de iniciación de autenticación a transmitirse a dicho dispositivo de autenticación.

En algunas realizaciones el mensaje de iniciación de autenticación se ensambla por el servidor de autenticación. En algunas realizaciones el mensaje de iniciación de autenticación se ensambla por el servidor de aplicación. En algunas realizaciones el mensaje de iniciación de autenticación se ensambla parcialmente por el servidor de autenticación y parcialmente por el servidor de aplicación. El mensaje de iniciación de autenticación puede comprender por ejemplo un identificador de sesión, y/o un desafío, y/o datos relacionados con transacción, y/o datos relacionados con contexto de transacción y/o un identificador de aplicación. En algunas realizaciones el mensaje de iniciación de autenticación puede comprender una credencial de servidor. Para obtener la credencial del servidor un servidor puede generar en primer lugar opcionalmente una credencial de servidor. En algunas realizaciones este servidor puede ser el servidor de aplicación. En algunas realizaciones este servidor puede ser el servidor de autenticación. El servidor puede generar la credencial del servidor usando una clave secreta y un algoritmo criptográfico. El algoritmo criptográfico puede ser un algoritmo criptográfico simétrico. En algunas realizaciones la clave secreta para generar la credencial del servidor puede compartirse con el testigo de autenticación del usuario.

- Transmitir el mensaje de iniciación de autenticación al dispositivo de autenticación del usuario.

En algunas realizaciones esto comprende enviar el mensaje de iniciación de autenticación en primer lugar al dispositivo de acceso del usuario. El dispositivo de acceso del usuario puede ejecutarse en una aplicación de ordenador tal como un explorador web. El mensaje de iniciación de autenticación puede embeberse en una o más páginas web que la aplicación basada en servidor sirve al explorador del dispositivo informático. A continuación el dispositivo de autenticación puede obtener el mensaje de iniciación de autenticación desde el dispositivo de acceso del usuario. En algunas realizaciones la pantalla del dispositivo de acceso del usuario emite una señal óptica que codifica el mensaje de iniciación de autenticación que se recibe y decodifica por el dispositivo de autenticación.

En algunas realizaciones el dispositivo de acceso del usuario visualiza un código de QR que codifica el mensaje de iniciación de autenticación (que puede ser en forma de un URL) y el dispositivo de autenticación del usuario lee y decodifica este código de QR. Por ejemplo el dispositivo de autenticación del usuario puede comprender un teléfono inteligente con una aplicación de autenticación adecuada. El usuario inicia la aplicación de autenticación que usa la cámara del teléfono inteligente para leer el código de QR y a continuación decodifica el código de QR.

En algunas realizaciones el dispositivo de autenticación recibe el mensaje de iniciación de autenticación en un

proceso de múltiples etapas. Por ejemplo, el dispositivo de autenticación puede recibir un primer mensaje que contiene información (tal como un URL) que permite que el dispositivo de autenticación contacte con un servidor y solicite el mensaje de iniciación de autenticación real. Por ejemplo, la página web del servidor de aplicación visualizada en el dispositivo de acceso del usuario puede visualizar un código de QR que codifica un URL que apunta al mensaje de iniciación de autenticación real que puede localizarse, por ejemplo, en el servidor de autenticación.

- Obtener aprobación del usuario.

En algunas realizaciones el dispositivo de autenticación puede adaptarse para buscar aprobación del usuario antes de generar un valor de seguridad dinámico y/o antes de enviar un mensaje de respuesta que comprende un valor de seguridad dinámico generado. En algunas realizaciones esta búsqueda de la aprobación del usuario comprende presentar el dispositivo de autenticación al usuario una representación de la aplicación o el proveedor de aplicación. Esta representación puede obtenerse y presentarse como se ha explicado anteriormente. En algunas realizaciones esta búsqueda de la aprobación del usuario comprende presentar el dispositivo de autenticación al usuario datos comprendidos en el mensaje de iniciación de autenticación. En algunas realizaciones esto puede comprender presentar datos relacionados con transacción al usuario. En algunas realizaciones el usuario puede indicar su aprobación usando un botón de OK. En algunas realizaciones el usuario puede indicar su aprobación introduciendo un PIN o contraseña válidos. En algunas realizaciones el dispositivo de autenticación no genera un valor de seguridad dinámico si el usuario no ha indicado su aprobación. En algunas realizaciones el dispositivo de autenticación no envía un mensaje de respuesta que comprende un valor de seguridad dinámico a un servidor si el usuario no ha indicado su aprobación.

- Generar un valor de seguridad dinámico.

El dispositivo de autenticación puede generar el valor de seguridad dinámico como se ha descrito en los párrafos anteriores. En algunas realizaciones el testigo de autenticación procesa el mensaje de iniciación de autenticación para generar un valor de seguridad dinámico. En algunas realizaciones el valor de seguridad dinámico se genera combinando criptográficamente una variable dinámica con una clave secreta. En algunas realizaciones la combinación criptográfica comprende usar un algoritmo criptográfico simétrico. En algunas realizaciones la variable dinámica comprende un desafío. En algunas realizaciones la variable dinámica comprende datos relacionados con transacción. En algunas realizaciones la variable dinámica comprende un valor relacionado con el tiempo. En algunas realizaciones la variable dinámica comprende un contador. En algunas realizaciones la variable dinámica comprende un elemento de datos comprendido en el mensaje de iniciación de autenticación recibido desde la aplicación basada en servidor. En algunas realizaciones el valor de seguridad dinámico se genera usando una clave que se comparte con la aplicación basada en servidor. En algunas realizaciones los datos de entrada comprenden una credencial de servidor y el dispositivo de autenticación verifica la credencial del servidor antes de generar el valor de seguridad dinámico. En algunas realizaciones el dispositivo de autenticación usa un algoritmo criptográfico simétrico con una clave secreta que se comparte con el servidor de aplicación para verificar la credencial del servidor. En algunas realizaciones el dispositivo de autenticación genera el valor de seguridad dinámico en la condición de que la verificación de la credencial del servidor fue satisfactoria.

En algunas realizaciones el dispositivo de autenticación puede generar el valor de seguridad dinámico usando un algoritmo criptográfico que también usa como entrada un elemento de datos que identifica la aplicación o el proveedor de aplicación. En algunas realizaciones este elemento de datos puede comprender el identificador de aplicación comprendido en el mensaje de iniciación de autenticación.

- transmitir el valor de seguridad dinámico generado al servidor de autenticación.

En algunas realizaciones el testigo de autenticación comprende una interfaz de salida de usuario segura y usa esa interfaz de salida de usuario segura para emitir el valor de seguridad dinámico al usuario. En algunas realizaciones el usuario recibe el valor de seguridad dinámico e introduce el valor de seguridad dinámico en una aplicación web relacionada con la aplicación basada en servidor.

En algunas realizaciones el dispositivo de autenticación ensambla un mensaje de respuesta que comprende el valor de seguridad dinámico y lo envía al servidor de autenticación. En algunas realizaciones el dispositivo de autenticación ensambla un mensaje de respuesta que comprende el valor de seguridad dinámico y lo envía al servidor de aplicación y el servidor de aplicación reenvía el mensaje de respuesta, o alguna parte de él, al servidor de autenticación. En algunas realizaciones el mensaje de respuesta puede comprender otros elementos de datos tales como un identificador de sesión, un identificador de aplicación, un identificador de dispositivo de autenticación, un usuario que identifica el elemento de datos y/u otros datos que pueden haberse aprobado por el usuario y/o pueden haberse usado en la generación del valor de seguridad dinámico tal como un desafío o datos de transacción o tiempo o datos de sincronización de contador.

- Verificar el valor de seguridad dinámico recibido. En algunas realizaciones el servidor de autenticación puede verificar la validez del valor de seguridad dinámico recibido. El servidor de autenticación puede verificar el valor de seguridad dinámico recibido usando un algoritmo criptográfico. En algunas realizaciones el servidor de autenticación

combina criptográficamente una variable dinámica de referencia con una clave secreta de referencia para verificar el valor de seguridad dinámico recibido. En algunas realizaciones el servidor de autenticación genera un valor de seguridad de referencia y compara el valor de seguridad de referencia con el valor de seguridad dinámico recibido. En algunas realizaciones el servidor de autenticación calcula el valor de seguridad de referencia combinando criptográficamente una variable dinámica de referencia con una clave secreta de referencia. En algunas realizaciones la combinación criptográfica comprende realizar un algoritmo criptográfico simétrico. En algunas realizaciones la clave secreta comprende una clave secreta que el servidor de autenticación comparte con el dispositivo de autenticación o con un segundo dispositivo de seguridad extraíble con el que ha cooperado el dispositivo de autenticación del usuario para generar el valor de seguridad dinámico.

- verificación del proveedor de aplicación

En algunas realizaciones el dispositivo de autenticación presenta al usuario un identificador de aplicación. En algunas realizaciones el servidor de autenticación verifica si el servidor de aplicación que solicitó verificación del valor de seguridad dinámico coincide con el identificador de aplicación que se presentó al usuario. En algunas realizaciones el dispositivo de autenticación incluye el identificador de aplicación que se presentó al usuario en el mensaje de respuesta y el servidor de autenticación verifica si el identificador de aplicación en el mensaje de respuesta que recibió coincide con el servidor de aplicación que solicitó verificación del valor de seguridad dinámico.

En algunas realizaciones el dispositivo de autenticación presenta al usuario un identificador de aplicación y usa ese identificador de aplicación en la generación del valor de seguridad dinámico. En algunas realizaciones el servidor usa un identificador de referencia proveedor de aplicación en la verificación del valor de seguridad dinámico de manera que esta verificación fallará si el identificador de aplicación usado por el dispositivo de autenticación en la generación del valor de seguridad dinámico no coincide con el identificador de proveedor de aplicación de referencia usado por el servidor de autenticación. En algunas realizaciones el servidor de autenticación extrae el identificador de proveedor de aplicación de referencia desde el mensaje de respuesta que también contiene el valor de seguridad dinámico a verificarse. En algunas realizaciones el servidor de autenticación deduce el valor de identificador de proveedor de aplicación de referencia desde la identidad del servidor de aplicación en nombre de la cual el servidor verifica el valor de seguridad dinámico.

- Informar al servidor de aplicación acerca del resultado de verificación.

En algunas realizaciones, tras verificar la validez del valor de seguridad dinámico, el servidor de autenticación puede informar al servidor de aplicación acerca del resultado de la verificación. Esta información puede comprender informar si la verificación fue satisfactoria. Esta información puede comprender, en caso de que la verificación fallara, un código de error (p. ej. "verificación criptográfica fallida", "dispositivo de autenticación desconocido", "id de sesión desconocido", "cuenta de usuario expirada", "cuenta de proveedor de aplicación expirada",...).

- informar al servidor de aplicación acerca de la identidad de usuario.

En algunas realizaciones el servidor de autenticación puede pasar también al servidor de aplicación una indicación de la identidad del usuario. En algunas realizaciones el servidor de autenticación puede pasar al servidor de aplicación un nombre de usuario general que es independiente de la aplicación o el proveedor de aplicación. En algunas realizaciones el servidor de autenticación puede pasar al servidor de aplicación un nombre de usuario específico que es una función del usuario y de la aplicación o el proveedor de aplicación. En algunas realizaciones el servidor de autenticación mantiene una base de datos que contiene para cada par de usuarios registrados y aplicaciones activadas un id de usuario para pasar al servidor de aplicación en cada sesión de autenticación.

- Informar al usuario acerca del resultado de verificación.

En algunas realizaciones el servidor que recibe el mensaje de respuesta devuelve un mensaje de acuse de recibo al dispositivo de autenticación que comprende el resultado de la verificación del valor de seguridad dinámico. Este mensaje puede contener, en caso de fallo, un código de error (p. ej. "verificación criptográfica fallida", "dispositivo de autenticación desconocido", "id de sesión desconocida", "cuenta de usuario expirada", "cuenta de proveedor de aplicación expirada",...).

- Tomar acción apropiada dependiendo del resultado de la verificación del valor de seguridad dinámico. En algunas realizaciones esto puede comprender que se conceda acceso al usuario a la aplicación del servidor de aplicación en caso de que la verificación fuera satisfactoria y se rechace el acceso en caso de que la verificación no fuera satisfactoria. En algunas realizaciones esto puede comprender que una solicitud de transacción emitida por el usuario se realice si la verificación fue satisfactoria y no se realice si la verificación no fue satisfactoria.

En algunas realizaciones el servidor de aplicación puede comprender uno o más ordenadores de servidor que ejecutan una o más aplicaciones de software. En algunas realizaciones el servidor de aplicación puede alojar una o más aplicaciones para accederse remotamente por uno o más usuarios. En algunas realizaciones el servidor de aplicación puede comprender uno o más servidores web. En algunas realizaciones una o más aplicaciones alojadas por el servidor de aplicación pueden estar basadas en web.

En algunas realizaciones el dispositivo de acceso del usuario para acceder a la aplicación alojada por el servidor de aplicación puede comprender un dispositivo informático. En algunas realizaciones este dispositivo informático puede comprender un PC o un portátil. En algunas realizaciones este dispositivo informático puede comprender un dispositivo de acceso a Internet, por ejemplo en un punto de acceso a Internet público. En algunas realizaciones el dispositivo de acceso puede estar en red. En algunas realizaciones el dispositivo de acceso puede estar adaptado para comunicar con un servidor de aplicación a través de una red informática. En algunas realizaciones esta red informática puede comprender una red de telecomunicaciones pública. En algunas realizaciones esta red informática puede comprender la Internet.

Breve descripción de los dibujos

Las anteriores y otras características y ventajas de la invención serán evidentes a partir de la siguiente descripción más particular de las realizaciones de la invención, como se ilustra en los dibujos adjuntos.

La **Figura 1** ilustra esquemáticamente una implementación ejemplar de la invención.

La **Figura 2** ilustra esquemáticamente un ejemplo de un sistema según un aspecto de la invención.

Las **Figuras 3a y 3b** ilustra esquemáticamente ejemplos de un dispositivo de autenticación de usuario según un aspecto de la invención.

Las **Figuras 4a y 4b** ilustran esquemáticamente un método para asegurar una aplicación remotamente accesible según un aspecto de la invención.

Descripción detallada

Algunas implementaciones de la presente invención se analizan a continuación. Aunque se analizan implementaciones específicas, debería entenderse que esto se hace para fines de ilustración únicamente. Un experto en la técnica reconocerá que pueden usarse otros componentes y configuraciones sin alejarse del espíritu y alcance de la invención.

La **Figura 1** ilustra una implementación ejemplar de la invención.

Un usuario trata una aplicación remota (indicada como 'MDP' en la figura) usando un dispositivo de acceso (indicado como 'Explorador Web de PC' en la figura). El dispositivo de acceso puede ser, por ejemplo, un PC o un portátil. La aplicación remota puede alojarse por un servidor de aplicación. El dispositivo de acceso del usuario puede comunicar con el servidor de aplicación a través de una red informática tal como por ejemplo la Internet. La aplicación puede estar basada en web y el usuario puede acceder a la aplicación basada en web usando un explorador web que se ejecuta en el dispositivo de acceso del usuario.

En algún punto, el usuario puede solicitar explícita o implícitamente acceso a una parte de acceso protegido de la aplicación (indicado por la flecha que se etiqueta como 'https://mydigipass.com' en la figura).

La aplicación puede obtener un mensaje de iniciación de autenticación. La aplicación puede obtener el mensaje de iniciación de autenticación enviando una solicitud (indicado por la flecha etiquetada como 'Solicitar Código de QR' en la figura) a un servidor de autenticación (indicado como 'DPS' en la figura). El servidor de autenticación puede responder a esta solicitud devolviendo a la aplicación parte o todos los contenidos del mensaje de iniciación de autenticación. Por ejemplo el servidor de autenticación puede enviar a la aplicación un mensaje que contiene un nombre de dominio. El mensaje puede comprender también un ID de sesión. El mensaje puede comprender también un desafío. La aplicación puede enviar una página web al explorador web en el dispositivo de acceso que contiene una representación del mensaje de iniciación de autenticación. Por ejemplo la página web puede comprender un código de QR. El código de QR puede codificar un URL o URI. Ese URL/URI puede comprender los datos comprendidos en el mensaje de iniciación de autenticación tal como un nombre de dominio y/o un ID de sesión y/o un desafío. La página web puede sugerir que el usuario lea el código de QR con su dispositivo de autenticación.

El dispositivo de autenticación del usuario (indicado por 'Aplicación móvil' en la figura) puede ser, por ejemplo, un teléfono inteligente que comprende una cámara de fotos y que está equipado con una aplicación de autenticación. En otras realizaciones puede comprender un testigo de hardware especializado. El usuario puede iniciar la miniaplicación de autenticación o aplicación en el dispositivo de autenticación y ordenar a la miniaplicación de autenticación o aplicación que obtenga la representación del mensaje de iniciación de autenticación presentada por el dispositivo de acceso. Por ejemplo el usuario puede hacer que el dispositivo de autenticación lea el código de QR en la pantalla del dispositivo de acceso del usuario. Tras obtener la representación del mensaje de iniciación de autenticación presentado por el dispositivo de acceso, p. ej. leyendo el código de QR (indicado por la flechas etiquetadas 'Explorar Código de QR' y 'Código de QR (Sesión)' en la figura), la miniaplicación de autenticación decodifica el código de QR para obtener los contenidos del mensaje de iniciación de autenticación. Estos contenidos pueden comprender, por ejemplo, un nombre de dominio, y/o un ID de sesión, y/o un desafío.

En algunas realizaciones la miniaplicación de autenticación puede a continuación generar un valor de seguridad

dinámico sin interacción adicional del usuario. En otras realizaciones la miniaplicación de autenticación puede solicitar al usuario aprobación explícita antes de continuar. La miniaplicación de autenticación puede generar una contraseña de un solo uso (indicada en la figura como 'Usar Sesión como Desafío') combinando criptográficamente el secreto que almacena con una o más variables dinámicas. La una o más variables dinámicas pueden comprender el valor del desafío extraído desde el mensaje de iniciación de autenticación, y/o el valor del tiempo mantenido por un reloj en el dispositivo de autenticación, y/o el valor de un contador mantenido por la miniaplicación de autenticación (mediante el cual la miniaplicación de autenticación puede incrementar, por ejemplo, el contador cada vez que genera una OTP). La miniaplicación de autenticación puede generar, por ejemplo, un troceo criptográfico de una combinación de la una o más variables dinámicas y el secreto usando un algoritmo de troceo criptográfico tal como SHA-1. La miniaplicación de autenticación puede encriptar, por ejemplo, una combinación de las variables dinámicas usando un algoritmo de encriptación parametrizado para el secreto.

El dispositivo de autenticación puede ensamblar un mensaje de respuesta. Este mensaje de respuesta puede comprender la OTP generada. Puede comprender también el ID de sesión extraído desde el mensaje de iniciación de autenticación. Puede comprender también un identificador del dispositivo de autenticación tal como por ejemplo un número de serie único almacenado por la miniaplicación de autenticación. El dispositivo de autenticación puede enviar este mensaje de respuesta a un servidor indicado por el nombre de dominio extraído desde el mensaje de iniciación de autenticación. El nombre de dominio puede indicar, por ejemplo, el servidor de autenticación. Antes de enviar el mensaje de respuesta la miniaplicación de autenticación puede verificar si el nombre de dominio indica un destino permitido para el mensaje de respuesta. El dispositivo de autenticación puede comparar, por ejemplo, el nombre de dominio a una lista de nombres de dominio permitidos o a una lista de patrones de nombre de dominio permitidos.

El dispositivo de autenticación puede enviar el mensaje de respuesta, p. ej., al servidor de autenticación (indicado por la flecha etiquetada como 'Solicitud de Autenticación (SN, OTP)'). El mensaje de respuesta puede comprender, por ejemplo, un mensaje de POST de HTTP. Este mensaje de POST de HTTP puede enviarse al servidor indicado en el URL que se codificó por el código de QR.

Tras recibir el mensaje de respuesta el servidor de autenticación puede validar la OTP comprendida en el mensaje de respuesta. Para verificar la OTP el servidor de autenticación puede usar un secreto de verificación. El servidor de autenticación puede obtener el secreto de verificación usando un identificador de dispositivo de autenticación (p. ej. un número de serie) comprendido en el mensaje de respuesta. Por ejemplo el servidor de autenticación puede usar el identificador de dispositivo de autenticación para buscar el secreto de verificación en una base de datos, o el servidor de autenticación puede derivar el secreto de verificación desde el identificador de dispositivo de autenticación y un secreto maestro.

Después de validar la OTP el servidor de autenticación puede informar al dispositivo de autenticación del resultado (indicado por la flecha etiquetada como 'ACK' en la Figura).

Después de validar la OTP el servidor de autenticación puede informar al servidor de aplicación del resultado de la verificación. Por ejemplo el servidor de aplicación puede estar interrogando al servidor de autenticación para el resultado de la validación de la OTP asociada con el ID de sesión comprendido en el mensaje de iniciación de autenticación.

El servidor de autenticación puede también pasar un identificador de usuario (tal como un nombre de usuario) al servidor de aplicación. Para obtener el identificador de usuario el servidor de autenticación puede buscar una base de datos usando el identificador de dispositivo de autenticación que puede estar comprendido en el mensaje de respuesta. En algunas realizaciones la base de datos puede comprender más de un identificador de usuario para el mismo usuario asociado con un dispositivo de autenticación dado. Por ejemplo el servidor de autenticación puede almacenar un identificador de usuario diferente para diferentes servidores de aplicación y pasar el correspondiente identificador de usuario al servidor de aplicación. En algunas realizaciones el servidor de autenticación puede almacenar más de un identificador de usuario para el mismo usuario y la misma aplicación y el servidor de autenticación pueden participar en un diálogo con el dispositivo de autenticación para permitir al usuario elegir el identificador de usuario correcto para pasar al servidor de aplicación.

Un sistema para asegurar aplicaciones remotas.

La **Figura 2** ilustra esquemáticamente un ejemplo de un sistema según un aspecto de la invención.

El sistema (200) comprende los siguientes componentes: un servidor (210) de aplicación, un servidor (220) de autenticación, una pluralidad de dispositivos (230) de acceso, y una pluralidad de dispositivos (240) de autenticación de usuario. En algunas realizaciones puede haber más de un servidor de aplicación.

El servidor (210) de aplicación puede estar adaptado para alojar una o más aplicaciones remotamente accesibles. Puede alojar, por ejemplo, un servidor web. El servidor de aplicación puede comprender un ordenador de servidor. El servidor de aplicación puede comprender un componente de procesamiento de datos tal como, por ejemplo, uno o más microprocesadores. Puede comprender componentes de almacenamiento para almacenar datos y/o software. Estos componentes de almacenamiento pueden comprender memoria volátil y/o no volátil tal como RAM y/o discos

duros. El servidor de aplicación puede comprender una interfaz de comunicación de datos (tal como por ejemplo una tarjeta de Ethernet) para conectar el servidor de aplicación a una red (250) informática (tal como por ejemplo la Internet) de modo que el servidor de aplicación puede comunicar e intercambiar datos y mensajes con, por ejemplo, el servidor de autenticación y/o un dispositivo de acceso y/o un dispositivo de autenticación de usuario.

Ejemplos de aplicaciones remotamente accesibles que pueden alojarse por un servidor de aplicación pueden incluir: aplicaciones de banca de Internet, sitios de comercio electrónico, aplicaciones de correo web (tales como Gmail), sitios de redes sociales (tales como Facebook), y otras aplicaciones basadas en web, basadas en Internet o basadas en la nube.

El servidor (220) de autenticación puede alojar una aplicación de servidor de autenticación que puede estar adaptada para verificar valores de seguridad dinámicos tales como, por ejemplo, contraseñas de un solo uso o firmas de transacción que pueden haberse generado por un dispositivo de autenticación de usuario. En algunas realizaciones el servidor de autenticación puede actuar como una parte confiable que verifica valores de seguridad dinámicos en nombre de posiblemente más de un servidor de aplicación que puede estar bajo control de diferentes proveedores de aplicación no relacionados. El servidor de autenticación puede estar adaptado para llevar a cabo cálculos criptográficos que en algunas realizaciones puede implicar algoritmos criptográficos simétricos y/o asimétricos. El servidor de autenticación puede comprender hardware seguro tal como por ejemplo un HSM (módulo de seguridad de hardware) para realizar de manera segura ciertas operaciones o cálculos sensibles de seguridad que pueden implicar claves secretas. El servidor de autenticación puede comprender un ordenador de servidor. El servidor de autenticación puede comprender un componente de procesamiento de datos tal como, por ejemplo, uno o más microprocesadores. Puede comprender componentes de almacenamiento para almacenar datos y/o software. Estos componentes de almacenamiento pueden comprender memoria volátil y/o no volátil tal como RAM (Memoria de Acceso Aleatorio) y/o discos duros.

En algunas realizaciones los componentes de almacenamiento pueden comprender una base de datos. En algunas realizaciones los componentes de almacenamiento pueden usarse para almacenar datos relacionados con el usuario para cada una de una pluralidad de usuarios. En algunas realizaciones estos datos relacionados con el usuario pueden comprender, por ejemplo, una o más claves secretas relacionadas con el usuario o datos de perfil de usuario que en algunas realizaciones pueden ser específicos de la aplicación. En algunas realizaciones estos datos relacionados con el usuario pueden comprender datos de identificación de dispositivo de autenticación de usuario (tales como un número de serie) de uno o más dispositivos de autenticación de usuario que, por ejemplo, pueden estar asociados con el usuario.

En algunas realizaciones los componentes de almacenamiento pueden usarse para almacenar datos relacionados con el dispositivo de autenticación de usuario para cada uno de una pluralidad de dispositivos de autenticación de usuario. En algunas realizaciones estos datos relacionados con el dispositivo de autenticación de usuario pueden comprender, por ejemplo, una o más claves secretas relacionadas con dispositivos de autenticación de usuario o datos de configuración de dispositivo de autenticación de usuario que en algunas realizaciones pueden ser específicos de aplicación y/o de usuario. En algunas realizaciones estos datos relacionados con el dispositivo de autenticación de usuario pueden comprender datos de identificación de usuario (tales como un nombre de usuario o ID de usuario) de uno o más usuarios que, por ejemplo, pueden asociarse con el dispositivo de autenticación de usuario.

El servidor de autenticación puede comprender una interfaz de comunicación (tal como por ejemplo una tarjeta de Ethernet) para conectar el servidor de autenticación a una red informática (tal como por ejemplo la Internet) de modo que el servidor de autenticación puede comunicar con, por ejemplo, un servidor de aplicación y/o un dispositivo de autenticación de usuario y/o un dispositivo de acceso.

En algunas realizaciones un único servidor puede actuar tanto como un servidor de aplicación como un servidor de autenticación. En otras realizaciones los servidores de aplicación y el servidor de autenticación son servidores distintos que interactúan remotamente intercambiando mensajes a través de una red informática (tal como por ejemplo la Internet).

El dispositivo (230) de acceso puede ser un dispositivo electrónico adaptado para conectarse a un servidor de aplicación y para permitir que un usuario interactúe remotamente a través de una red informática con un servidor de aplicación. El dispositivo de acceso puede comprender un componente de procesamiento de datos tal como, por ejemplo, uno o más microprocesadores. Puede comprender componentes de almacenamiento para almacenar datos y/o software. Estos componentes de almacenamiento pueden comprender memoria volátil y/o no volátil tal como RAM y/o discos duros y/o unidades de estado sólido (SSD). El dispositivo de acceso puede comprender una interfaz de comunicación (tal como por ejemplo una tarjeta de Ethernet) para conectar el dispositivo de acceso a una red informática (tal como por ejemplo la Internet) de modo que el dispositivo de acceso puede comunicar con, por ejemplo, un servidor de aplicación y/o un servidor de autenticación. El dispositivo de acceso puede comprender una interfaz de usuario con una interfaz de entrada de usuario y una interfaz de salida de usuario para interactuar con un usuario (290). El dispositivo de acceso puede comprender, por ejemplo, una pantalla y/o altavoces para presentar la salida al usuario y puede comprender, por ejemplo, un teclado y/o una pantalla táctil y/o un ratón para recibir entrada desde un usuario.

El dispositivo de acceso puede comprender, por ejemplo, un dispositivo informático tal como un ordenador personal (PC), o un portátil, o un ordenador de tableta. El dispositivo de acceso puede proporcionarse con un programa informático para permitir que el usuario interactúe con una aplicación remota a través de una red informática tal como Internet. Este programa informático puede comprender, por ejemplo, un explorador web (tal como, por ejemplo, Internet Explorer o Mozilla Firefox) y la aplicación remota puede comprender, por ejemplo, una aplicación de servidor basada en web. El dispositivo de acceso puede interactuar con una aplicación alojada por un servidor de aplicación intercambiando datos y mensajes. El dispositivo de acceso puede interactuar con una aplicación alojada por un servidor de aplicación usando un protocolo de comunicación tal como por ejemplo IP (Protocolo de Internet) y/o SSL/TLS (Capa de Conexiones Segura / Seguridad de Capa de Transporte) para intercambiar mensajes tales como mensajes de HTTP (Protocolo de Transferencia de Hipertexto).

En algunas realizaciones el dispositivo de acceso puede estar adaptado para recibir desde un servidor de aplicación datos relacionados con un mensaje de iniciación de autenticación que posibilitan que el dispositivo de acceso obtenga o genere una representación del mensaje de iniciación de autenticación. Por ejemplo, en algunas realizaciones el dispositivo de acceso está adaptado para recibir desde un servidor de aplicación una representación del mensaje de iniciación de autenticación. Por ejemplo el dispositivo de acceso puede estar adaptado para recibir una página web que contiene una imagen (por ejemplo un código de barras bidimensional tal como un código de QR) o un fichero de audio que codifica el mensaje de iniciación de autenticación. En algunas realizaciones el dispositivo de acceso está adaptado para recibir desde un servidor de aplicación uno o más elementos de datos (tales como, por ejemplo, un desafío y/o datos de transacción y/o un identificador de aplicación) que están comprendidos en el mensaje de iniciación de autenticación y que el dispositivo de acceso usa para generar una representación del mensaje de iniciación de autenticación. Por ejemplo el dispositivo de acceso puede estar adaptado para recibir una página web que contiene elementos de datos para estar comprendidos en el mensaje de iniciación de autenticación y el dispositivo de acceso puede ejecutar una aplicación tal como, por ejemplo, un módulo de extensión de explorador o una miniaplicación (que puede estar también contenida en la página web recibida) para generar una representación (tal como, por ejemplo, un código de barras bidimensional) del mensaje de iniciación de autenticación. En algunas realizaciones el dispositivo de acceso está adaptado para recibir desde el servidor de aplicación un elemento de datos que el dispositivo de acceso usa para recuperar desde otro servidor (tal como, por ejemplo, un servidor de autenticación) uno o más elementos de datos que están comprendidos en el mensaje de iniciación de autenticación y que el dispositivo de acceso usa para generar una representación del mensaje de iniciación de autenticación. Por ejemplo el dispositivo de acceso puede estar adaptado para recibir una página web que contiene un URL (Localizador de Recurso Uniforme) o URI (Identificador de Recurso Uniforme) que apunta a un elemento de datos en algún servidor (tal como por ejemplo un servidor de autenticación) que el dispositivo de acceso puede usar para generar una representación del mensaje de iniciación de autenticación. Este elemento de datos puede comprender, por ejemplo, uno o más elementos de datos (tal como un desafío) que están comprendidos en los contenidos del mensaje de iniciación de autenticación, o puede comprender una representación del mensaje de iniciación de autenticación entero, o puede comprender una credencial de servidor que autentica el origen del mensaje de iniciación de autenticación tal como una firma o MAC (Código de Autenticación de Mensaje) a través de los contenidos del mensaje de iniciación de autenticación o una representación encriptada del mensaje de iniciación de autenticación.

El dispositivo de acceso puede estar adaptado para emitir una señal que codifica una representación del mensaje de iniciación de autenticación. En algunas realizaciones el dispositivo de acceso está adaptado para usar su interfaz de salida de usuario (p. ej. sus altavoces de audio o su pantalla) para emitir la señal que codifica una representación del mensaje de iniciación de autenticación. Por ejemplo en algunas realizaciones el dispositivo de acceso puede estar adaptado para reproducir a través de sus altavoces un fichero de audio que contiene una señal de audio que codifica una representación del mensaje de iniciación de autenticación. En algunas realizaciones el dispositivo de acceso puede estar adaptado para emitir una señal óptica visualizando un patrón óptico variable en el tiempo que codifica una representación del mensaje de iniciación de autenticación. En algunas realizaciones el dispositivo de acceso puede estar adaptado para visualizar una o más imágenes (tal como códigos de barras bidimensionales) que codifican una representación del mensaje de iniciación de autenticación.

El dispositivo (240) de autenticación de usuario se analizará en más detalle en relación a las Figuras 3a y 3b.

En algunas realizaciones el dispositivo de acceso y el dispositivo de autenticación de usuario son físicamente dispositivos distintos. En algunas realizaciones el dispositivo de autenticación de usuario es una entidad confiable mientras que el dispositivo de acceso no es una entidad confiable.

El sistema está adaptado para autenticar usuarios que acceden a una aplicación alojada por uno de los servidores de aplicación y/o para autenticar transacciones emitidas por usuarios a una aplicación alojada por uno de los servidores de aplicación y puede usarse, por ejemplo, con el método analizado en relación a la figura 4.

Las **Figuras 3a y 3b** ilustran esquemáticamente un ejemplo y una variante de ese ejemplo de un aparato según un aspecto de la invención. El aparato comprende un ejemplo de un dispositivo (240) de autenticación de usuario del sistema analizado en relación a la Figura 2.

El dispositivo (240) de autenticación de usuario comprende un dispositivo electrónico adaptado para generar un

mensaje de respuesta que comprende un valor de seguridad dinámico en respuesta a un mensaje de iniciación de autenticación, por ejemplo, para autenticar un usuario o una transacción. El dispositivo de autenticación de usuario puede comprender un componente (310) de procesamiento de datos, componentes (320) de almacenamiento para almacenar datos y/o software, una interfaz (330) de comunicación de datos para conectar el dispositivo de autenticación de usuario a una red informática, una interfaz (340, 350) de usuario para interactuar con un usuario, una interfaz (360, 370) de entrada para capturar una señal que representa un mensaje de iniciación de autenticación que se está emitiendo por un dispositivo de acceso (p. ej. por medio de la interfaz de salida de usuario del dispositivo de acceso), y un reloj (380) en tiempo real para proporcionar valores relacionados con el tiempo.

El componente (310) de procesamiento de datos puede comprender por ejemplo uno o más microprocesadores. El componente de procesamiento de datos puede estar adaptado para realizar un algoritmo para generar valores de seguridad dinámicos. El componente de procesamiento de datos puede estar adaptado para realizar operaciones criptográficas que pueden comprender realizar algoritmos criptográficos simétricos o asimétricos. En algunas realizaciones el componente de procesamiento de datos puede comprender un microprocesador y/o un controlador y/o un ASIC (Circuito Integrado Específico de la Aplicación).

El dispositivo de autenticación de usuario puede comprender componentes (320) de almacenamiento para almacenar datos y/o software. Estos componentes de almacenamiento pueden comprender memoria volátil y/o no volátil tal como RAM y/o ROM (Memoria de Solo Lectura) y/o Flash y/o discos duros y/o unidades de estado sólido (SSD).

El dispositivo de autenticación de usuario puede comprender una interfaz (330) de comunicación de datos para conectar el dispositivo de autenticación de usuario a una red informática (tal como por ejemplo la Internet) de modo que el dispositivo de autenticación de usuario puede comunicar con, por ejemplo, un servidor de aplicación y/o un servidor de autenticación. La interfaz de comunicación de datos puede comprender, por ejemplo, una interfaz de comunicación de datos inalámbrica (330) para conectar a una red de comunicación inalámbrica tal como, por ejemplo, una red de telefonía móvil tal como, por ejemplo, una red de GSM (Sistema Global para Comunicaciones Móviles) o de UMTS (Sistema Universal de Telecomunicaciones Móviles). En algunas realizaciones la interfaz de comunicación de datos puede comprender una interfaz de radio móvil y/o una interfaz de red de GSM. En algunas realizaciones la interfaz de comunicación de datos puede comprender una antena. En algunas realizaciones la interfaz de comunicación de datos inalámbrica puede adaptarse para enviar datos desde el dispositivo de autenticación de usuario a un servidor de destino usando una red de comunicación de datos inalámbrica pública. En algunas realizaciones la interfaz de comunicación de datos inalámbrica puede estar adaptada también para recuperar datos desde un servidor remoto (tal como el servidor de aplicación o el servidor de autenticación) usando una red de comunicación de datos inalámbrica pública.

El dispositivo de autenticación de usuario puede comprender una interfaz (340, 350) de usuario con una interfaz (350) de entrada de usuario y una interfaz (340) de salida de usuario para interactuar con un usuario. El dispositivo de autenticación de usuario puede comprender una interfaz de salida de usuario para proporcionar salida a un usuario. La interfaz de salida de usuario puede comprender, por ejemplo, una pantalla (340) y/o altavoces para presentar salida al usuario. El dispositivo de autenticación de usuario puede comprender una interfaz de entrada de usuario para recibir entrada desde un usuario. La interfaz de entrada de usuario puede comprender, por ejemplo, un teclado (350) y/o una pantalla táctil y/o un micrófono para recibir entrada desde un usuario. La pantalla puede comprender una pantalla gráfica. La pantalla puede comprender una pantalla a color. La pantalla puede comprender, por ejemplo, una pantalla de LCD (Pantalla de Cristal Líquido) o una pantalla de TFT (Transistor de Película Delgada) o una pantalla de OLED (Diodo de Emisión de Luz Orgánico).

El dispositivo de autenticación de usuario puede comprender una interfaz (360, 370) de entrada para capturar una señal que representa un mensaje de iniciación de autenticación que se está emitiendo por un dispositivo de acceso (por ejemplo, por la interfaz de salida de usuario del dispositivo de acceso). Por ejemplo, en algunas realizaciones el dispositivo de autenticación de usuario puede comprender un micrófono (370) para capturar una señal de audio emitida por, por ejemplo, los altavoces de un dispositivo de acceso y codificada con un mensaje de iniciación de autenticación. En algunas realizaciones el dispositivo de autenticación de usuario puede comprender sensores ópticos para capturar señales ópticas emitidas por, por ejemplo, la pantalla de un dispositivo de acceso y codificadas con un mensaje de iniciación de autenticación. En algunas realizaciones el dispositivo de autenticación de usuario puede comprender una cámara (360) para capturar una o más imágenes visualizadas en la pantalla de un dispositivo de acceso y codificar un mensaje de iniciación de autenticación. En algunas realizaciones estas imágenes pueden comprender un código de barras bidimensional tal como un código de QR.

El dispositivo de autenticación de usuario puede comprender un mecanismo de temporización tal como el reloj (380) en tiempo real para proporcionar valores relacionados con el tiempo que el dispositivo de autenticación de usuario puede usar como entrada para un algoritmo criptográfico para generar un valor de seguridad dinámico.

El dispositivo de autenticación de usuario puede estar adaptado para obtener el mensaje de iniciación de autenticación decodificando la señal capturada. Por ejemplo puede estar adaptado para decodificar una señal de audio modulada que codifica un mensaje de iniciación de autenticación o puede estar adaptado para decodificar una o más imágenes (tal como códigos de QR) que codifican un mensaje de iniciación de autenticación.

Verificación de credencial de servidor.

En algunas realizaciones el mensaje de iniciación de autenticación comprende una credencial de servidor y el dispositivo de autenticación de usuario puede estar adaptado para verificar esta credencial. En algunas realizaciones el dispositivo de autenticación de usuario está adaptado para verificar la credencial del servidor usando un algoritmo criptográfico parametrizado con una clave de verificación de credencial de servidor que puede almacenarse en el dispositivo de autenticación de usuario o que el dispositivo de autenticación de usuario puede obtener usando una clave almacenada en el dispositivo de autenticación de usuario.

En algunas realizaciones el dispositivo de autenticación de usuario puede usar un algoritmo criptográfico asimétrico para verificar la credencial del servidor. En algunas realizaciones la credencial del servidor comprende una firma digital a través de al menos algunos elementos de datos del mensaje de iniciación de autenticación y la verificación de la credencial del servidor puede comprender la verificación de esta firma. En algunas realizaciones la firma de la credencial del servidor se ha generado por la clave privada de un par de clave pública-privada asociado con un servidor confiable tal como el servidor de autenticación y el dispositivo de autenticación de usuario verifica la firma usando la correspondiente clave pública que puede almacenarse en el dispositivo de autenticación de usuario.

En algunas realizaciones el dispositivo de autenticación de usuario puede usar un algoritmo criptográfico simétrico para verificar la credencial del servidor. En algunas realizaciones el algoritmo criptográfico simétrico está parametrizado con una clave de credencial de servidor secreta simétrica. En algunas realizaciones la credencial del servidor comprende una porción encriptada del mensaje de iniciación de autenticación y el dispositivo de autenticación de usuario verifica la credencial del servidor desencriptando esta porción encriptada y certificando que en la porción desencriptada están presentes ciertos elementos estructurales esperados, tales como, por ejemplo, ciertos valores fijos para ciertos elementos de datos (p. ej. etiquetas) en la porción desencriptada o ciertas redundancias tales como, por ejemplo el valor de un código de CRC o ciertas consistencias obligatorias entre los valores de ciertos elementos de datos tales como las longitudes de ciertos campos de datos (como se indica por los campos de longitud) o restricciones en el intervalo permisible de los valores de ciertos campos de datos. En algunas realizaciones la credencial del servidor comprende un MAC (código de autenticación de mensaje) o un troceo con clave a través de una porción del mensaje de iniciación de autenticación y el dispositivo de autenticación de usuario puede calcular un valor de referencia para el MAC o el troceo con clave y comparar el valor de referencia con la credencial de servidor recibido.

En algunas realizaciones el dispositivo de autenticación de usuario puede rechazar el mensaje de iniciación de autenticación si la verificación de la credencial del servidor falla.

En algunas realizaciones el mensaje de iniciación de autenticación decodificado puede encriptarse y el dispositivo de autenticación de usuario puede estar adaptado para desencriptar el mensaje de iniciación de autenticación encriptado.

Extraer datos del mensaje de iniciación de autenticación.

El dispositivo de autenticación de usuario puede estar adaptado para extraer algunos elementos de datos que están comprendidos en el mensaje de iniciación de autenticación. En algunas realizaciones los elementos de datos que están comprendidos en el mensaje de iniciación de autenticación y que pueden extraerse por el dispositivo de autenticación de usuario pueden incluir uno o más de: un desafío, fecha relacionada con la transacción, un elemento de datos relacionado con identidad de aplicación, un id de sesión, un número aleatorio utilizado solo una vez, un valor de seguridad dinámico generado de servidor.

Indicación y aprobación de identidad de aplicación.

En algunas realizaciones el dispositivo de autenticación de usuario puede estar adaptado para extraer un elemento de datos relacionado con identidad de aplicación desde el mensaje de iniciación de autenticación. El dispositivo de autenticación de usuario puede estar adaptado para usar este elemento de datos relacionado con identidad de aplicación para obtener o generar una representación de la identidad de aplicación. Esta representación de la identidad de aplicación puede ser interpretable y reconocible por el usuario. En algunas realizaciones el elemento de datos relacionado con identidad de aplicación es la representación de la identidad de aplicación, por ejemplo el elemento de datos relacionado con identidad de aplicación (y la representación de la identidad de aplicación) puede simplemente ser un nombre de aplicación alfanumérico. En algunas realizaciones el elemento de datos relacionado con identidad de aplicación puede comprender un índice que el dispositivo de autenticación de usuario puede usar para recuperar la representación de la identidad de aplicación desde una base de datos interna. En algunas realizaciones el dispositivo de autenticación de usuario puede estar adaptado para determinar la representación de la identidad de aplicación desde el elemento de datos relacionado con identidad de aplicación en el mensaje de iniciación de autenticación sin usar ningún dato específico del elemento de la aplicación (permanentemente) almacenado en el dispositivo de autenticación de usuario. En algunas realizaciones el dispositivo de autenticación de usuario puede estar adaptado para determinar la representación de la identidad de aplicación desde el elemento de datos relacionado con identidad de aplicación en el mensaje de iniciación de autenticación y datos que el dispositivo de autenticación de usuario recupera desde una fuente externa. En algunas realizaciones el dispositivo de

autenticación de usuario puede usar el elemento de datos relacionado con identidad de aplicación para recuperar datos específicos de la aplicación desde una fuente externa y usar los datos recuperados para obtener la representación de la identidad de aplicación. En algunas realizaciones el elemento de datos relacionado con identidad de aplicación puede comprender una referencia, tal como por ejemplo un URL o URI, que el dispositivo de autenticación de usuario puede usar para recuperar la representación de la identidad de aplicación desde una fuente externa tal como un servidor remoto tal como, por ejemplo, el servidor de autenticación o un servidor de aplicación. En algunas realizaciones la representación de la identidad de aplicación puede comprender un nombre de aplicación. En algunas realizaciones la representación de la identidad de aplicación puede comprender una imagen gráfica tal como un logo de aplicación. En algunas realizaciones la representación de la identidad de aplicación puede comprender una secuencia de sonido característica. En algunas realizaciones la representación de la identidad de aplicación puede comprender una representación de voz sintética de un nombre de aplicación.

En algunas realizaciones la representación de la identidad de aplicación puede ser interpretable y reconocible por el usuario y el dispositivo de autenticación de usuario puede estar adaptado para presentar la representación de la identidad de aplicación al usuario del dispositivo de autenticación de usuario como parte del proceso para generar un mensaje de respuesta en respuesta al mensaje de iniciación de autenticación. Por ejemplo en algunas realizaciones el dispositivo de autenticación de usuario puede visualizar en su pantalla un nombre de aplicación. En algunas realizaciones el dispositivo de autenticación de usuario puede visualizar en su pantalla una imagen representativa de la aplicación tal como un logo de aplicación. En algunas realizaciones el dispositivo de autenticación de usuario puede emitir a través de sus altavoces una secuencia de sonido que es representativa de la aplicación tal como una secuencia de sonido característica o una representación de voz sintética del nombre de la aplicación.

En algunas realizaciones el dispositivo de autenticación de usuario está adaptado para obtener la confirmación de la representación implícita o explícita del usuario de la identidad de aplicación que el dispositivo de autenticación de usuario presenta al usuario. En algunas realizaciones el usuario confirma de manera explícita la representación de la identidad de aplicación, p. ej., haciendo clic un botón de OK. En algunas realizaciones la confirmación de la representación de la identidad de aplicación está integrada en una confirmación global en donde el usuario aprueba, p. ej., la generación del mensaje de respuesta y de esta manera señaliza su confirmación o aprobación de todos los datos o mensajes (que además de la representación de la identidad de aplicación pueden incluir ciertos datos comprendidos en el mensaje de iniciación de autenticación que deben confirmarse por el usuario) que el dispositivo de autenticación de usuario presentó al usuario hasta el momento en el curso del proceso para generar un mensaje de respuesta. En algunas realizaciones se considera que el usuario que introduce un PIN o contraseña por el dispositivo de autenticación de usuario como una aprobación implícita o confirmación.

En algunas realizaciones el dispositivo de autenticación de usuario está adaptado para abortar la generación del mensaje de respuesta si el usuario no confirma la representación de la identidad de aplicación. En algunas realizaciones, si el usuario no confirma, el dispositivo de autenticación de usuario puede, sin embargo, continuar la generación del mensaje de respuesta pero en su lugar no hacer que el mensaje de respuesta esté disponible para el usuario o un servidor de destino.

Aprobación de datos relacionados con transacción.

En algunas realizaciones el dispositivo de autenticación de usuario puede estar adaptado para extraer datos relacionados con transacción desde el mensaje de iniciación de autenticación. En algunas realizaciones los datos relacionados con transacción pueden estar comprendidos en una porción encriptada del mensaje de iniciación de autenticación o pueden estar criptográficamente enlazados (por ejemplo por una credencial de servidor) a otros datos en el mensaje de iniciación de autenticación tal como un valor de seguridad dinámico generado de servidor. Estos datos relacionados con la transacción pueden incluir valores para elementos de una transacción que el usuario ha emitido a la aplicación remota. Por ejemplo, en el caso de una transacción de transferencia monetaria estos datos relacionados con transacción pueden comprender la cantidad de dinero a transferirse, el código de divisa y el número de cuenta de destino. En el caso de una transacción bursátil los datos relacionados con transacción pueden comprender, por ejemplo, el símbolo de la acción a negociar, si comprar o vender, el precio por participación y la cantidad de participaciones a negociar.

En algunas realizaciones el dispositivo de autenticación de usuario está adaptado para presentar estos datos relacionados con transacción al usuario y obtener la confirmación implícita o explícita del usuario de los datos relacionados con transacción que el dispositivo de autenticación de usuario presenta al usuario. En algunas realizaciones el usuario confirma de manera explícita la representación de los datos relacionados con transacción, p. ej., haciendo clic un botón de OK. En algunas realizaciones la confirmación de los datos relacionados con transacción está integrada en una confirmación global en donde el usuario aprueba, p. ej., la generación del mensaje de respuesta y señaliza de esta manera su confirmación o aprobación de todos los datos o mensajes (que además de los datos relacionados con transacción pueden incluir, por ejemplo, una representación de la identidad de aplicación que debe confirmarse por el usuario) que el dispositivo de autenticación de usuario presentó al usuario hasta ahora en el curso del proceso para generar un mensaje de respuesta. En algunas realizaciones se considera que el usuario que introduce un PIN o contraseña por el dispositivo de autenticación de usuario como una aprobación implícita o confirmación.

En algunas realizaciones el dispositivo de autenticación de usuario está adaptado para abortar la generación del mensaje de respuesta si el usuario no confirma los datos relacionados con transacción. En algunas realizaciones, si el usuario no confirma, el dispositivo de autenticación de usuario puede, sin embargo, continuar la generación del mensaje de respuesta pero en su lugar no hacer que el mensaje de respuesta esté disponible para el usuario o un servidor de destino.

Entrada de datos proporcionados por el usuario.

En algunas realizaciones el dispositivo de autenticación de usuario puede estar adaptado para pedir al usuario que introduzca los valores para ciertos elementos de datos. En algunas realizaciones el dispositivo de autenticación de usuario puede usar estos valores en la generación del valor de seguridad dinámico y/o en la generación del mensaje de respuesta.

Entrada de PIN y uso de PIN.

En algunas realizaciones el dispositivo de autenticación de usuario está adaptado para obtener un PIN o valor de contraseña del usuario. En algunas realizaciones el usuario puede proporcionar el PIN o valor de contraseña usando el teclado o pantalla táctil del dispositivo de autenticación de usuario. En algunas realizaciones el dispositivo de autenticación de usuario está adaptado para almacenar un PIN o valor de referencia de contraseña y para verificar el PIN o valor de contraseña proporcionado por el usuario comparándolo con el valor de referencia almacenado. El dispositivo de autenticación de usuario puede considerar la verificación de PIN o contraseña satisfactoria si el PIN o valor de contraseña proporcionado por el usuario coincide con el valor de referencia almacenado. En algunas realizaciones el dispositivo de autenticación de usuario está adaptado para abortar la generación del mensaje de respuesta si el PIN o la verificación de contraseña fallan. En algunas realizaciones, si el PIN o la verificación de contraseña fallan, el dispositivo de autenticación de usuario, sin embargo, puede continuar la generación del mensaje de respuesta pero en su lugar no hacer que el mensaje de respuesta esté disponible para el usuario o un servidor de destino.

En algunas realizaciones el dispositivo de autenticación de usuario puede usar el PIN o valor de contraseña introducido para obtener o generar el valor de una clave secreta. Por ejemplo, el dispositivo de autenticación de usuario puede combinar criptográficamente el PIN o valor de contraseña con una clave maestra para derivar otra clave, o puede usar el PIN o valor de contraseña como una clave para desencriptar un valor de clave encriptado.

En algunas realizaciones el dispositivo de autenticación de usuario está adaptado para añadir un valor representativo del PIN o valor de contraseña introducido al mensaje de respuesta. En algunas realizaciones el dispositivo de autenticación de usuario está adaptado para encriptar una porción del mensaje de respuesta que comprende el valor representativo del PIN o valor de contraseña introducido.

Generar u obtener criptográficamente un valor de seguridad dinámico.

El dispositivo de autenticación de usuario puede estar adaptado para generar u obtener un valor de seguridad dinámico usando un algoritmo criptográfico parametrizado con al menos una clave secreta.

En algunas realizaciones la al menos una clave secreta que el dispositivo de autenticación de usuario usa para generar el valor de seguridad dinámico (o clave de generación de valor de seguridad dinámico) está matemáticamente relacionada con un secreto de base que está almacenado en un componente de almacenamiento del dispositivo de autenticación de usuario. En algunas realizaciones el secreto de base puede comprender un elemento de datos personalizado. En el contexto de esta aplicación la terminología 'elemento de datos personalizado' de un dispositivo de autenticación de usuario hace referencia a un elemento de datos que está presente en una pluralidad de dispositivos de autenticación de usuario que tienen la misma función en cada dispositivo de esa pluralidad de dispositivos de autenticación de usuario, pero que tiene un valor individual particular en cada dispositivo individual particular de la pluralidad de dispositivos de autenticación de usuario. En otras realizaciones el secreto de base puede comprender un secreto maestro que se comparte entre múltiples dispositivos de autenticación de usuario. En algunas realizaciones el dispositivo de autenticación de usuario está adaptado para derivar la al menos una clave de generación de valor de seguridad dinámico desde el secreto de base que está almacenado en un componente de almacenamiento del dispositivo de autenticación de usuario. En algunas realizaciones el dispositivo de autenticación de usuario está adaptado para derivar la al menos una clave de generación de valor de seguridad dinámico usando un PIN o contraseña u otro valor secreto proporcionado por el usuario. En algunas realizaciones la al menos una clave de generación de valor de seguridad dinámico es el secreto de base. En algunas realizaciones los valores de la al menos una clave de generación de valor de seguridad dinámico y/o el secreto de base personalizado están asociados con un usuario particular o con un dispositivo de autenticación de usuario particular. En algunas realizaciones la clave de generación de valor de seguridad dinámico puede comprender una clave simétrica, tal como, por ejemplo, una clave de encriptación o desencriptación simétrica, el valor de la cual se comparte con o está disponible para un servidor de autenticación. En algunas realizaciones la clave de generación de valor de seguridad dinámico puede comprender la clave privada de un par de clave pública/privada a usarse con un algoritmo criptográfico asimétrico.

En algunas realizaciones el dispositivo de autenticación de usuario puede estar adaptado para generar el valor de

seguridad dinámico combinando criptográficamente un número de valores de entrada y la al menos una clave de generación de valor de seguridad dinámico emitiendo los valores de entrada a un algoritmo criptográfico que está parametrizado con la al menos una clave de generación de valor de seguridad dinámico. Estos valores de entrada pueden comprender por ejemplo: una variable dinámica (tal como un valor relacionado con el tiempo proporcionado por el dispositivo de autenticación de usuario, y/o un valor relacionado con el contador proporcionado por el dispositivo de autenticación de usuario, y/o un desafío que el dispositivo de autenticación de usuario extrae desde el mensaje de iniciación de autenticación), y/o datos relacionados con la transacción que el dispositivo de autenticación de usuario extrae desde el mensaje de iniciación de autenticación y que pueden confirmarse por el usuario, y/o un identificador de sesión que el dispositivo de autenticación de usuario extrae desde el mensaje de iniciación de autenticación, y/o un elemento de datos que está relacionado con un identificador de aplicación que el dispositivo de autenticación de usuario extrae desde el mensaje de iniciación de autenticación o que está relacionado con una representación del identificador de aplicación que se ha de presentar al usuario y que puede confirmarse por el usuario. En algunas realizaciones los valores de entrada pueden comprender también datos proporcionados al dispositivo de autenticación de usuario por el usuario.

En algunas realizaciones el dispositivo de autenticación de usuario puede estar adaptado para generar el valor de seguridad dinámico usando un elemento de datos personalizado. En alguna realización este elemento de datos personalizado puede comprender una clave criptográfica personalizada. En algunas realizaciones este elemento de datos personalizado puede comprender un elemento de datos relacionado con el identificador de dispositivo de autenticación del usuario (tal como un número de serie). En algunas realizaciones el dispositivo de autenticación de usuario deriva la clave de generación de valor de seguridad dinámico desde un secreto maestro y un elemento de datos personalizado que en algunas realizaciones puede comprender un elemento de datos relacionado con el identificador de dispositivo de autenticación de usuario (tal como un número de serie).

En algunas realizaciones el algoritmo criptográfico usado por el dispositivo de autenticación de usuario para generar u obtener el valor de seguridad dinámico puede comprender un algoritmo criptográfico simétrico. Ejemplos de algoritmos criptográficos simétricos pueden incluir algoritmos de encriptación/desencriptación simétricos tales como DES (Norma de Encriptación de Datos) o AES (Norma de Encriptación Avanzada), algoritmos de MAC (Código de Autenticación de Mensaje) simétricos, algoritmos de troceo con clave tales como HMAC (código de autenticación de mensaje de troceo con clave) o SHA-1 o MD5 (mediante el cual la al menos una clave de generación de valor de seguridad dinámico trocea el algoritmo). Por ejemplo, en algunas realizaciones el dispositivo de autenticación de usuario puede encriptar una concatenación de los valores de entrada usando un cifrado de bloque simétrico tal como DES o AES en modo de CBC (Encadenamiento de Bloque de Cifrado) y usar una parte del criptograma resultante (preferiblemente una parte del último bloque del criptograma).

En algunas realizaciones el algoritmo criptográfico usado por el dispositivo de autenticación de usuario para generar u obtener el valor de seguridad dinámico puede comprender un algoritmo criptográfico asimétrico. Ejemplos de algoritmos criptográficos simétricos pueden incluir por ejemplo RSA (Rivest-Shamir-Adleman) o DSA (Algoritmo de Firma Digital). En algunas realizaciones el dispositivo de autenticación de usuario puede generar, por ejemplo, una firma digital a través de los valores de entrada usando un algoritmo criptográfico asimétrico parametrizado con la clave privada de un par de clave pública-privada.

En algunas realizaciones un valor de seguridad dinámico generado de servidor puede estar comprendido en una porción encriptada del mensaje de iniciación de autenticación y el dispositivo de autenticación de usuario puede estar adaptado para obtener este valor de seguridad dinámico desencriptando la porción encriptada y extrayendo el valor de seguridad dinámico generado de servidor desde la porción desencriptada.

Dispositivo de seguridad extraíble

En algunas realizaciones, como se ilustra en la **figura 3b,** el dispositivo (240) de autenticación de usuario puede comprender un dispositivo (395) de seguridad extraíble y una interfaz (390) de comunicación para intercambiar datos y/o mensajes y/o comandos y respuestas con este dispositivo de seguridad extraíble. En algunas realizaciones el dispositivo de seguridad extraíble puede estar adaptado para almacenar y/o manejar de manera segura claves secretas y/o puede estar adaptado para realizar ciertos cálculos criptográficos. En algunas realizaciones el dispositivo de autenticación de usuario puede basarse en el dispositivo de seguridad extraíble para almacenar y/o gestionar de manera segura algunos secretos (tal como claves criptográficas y/o valores de PIN o contraseñas de usuario). En algunas realizaciones el dispositivo de autenticación de usuario puede delegar algunos cálculos criptográficos al dispositivo de seguridad extraíble. En algunas realizaciones el dispositivo de autenticación de usuario usa elementos de datos proporcionados por el dispositivo de seguridad extraíble para obtener el valor de la clave de generación del valor de seguridad dinámico. En algunas realizaciones el dispositivo de autenticación de usuario delega algunos de los cálculos criptográficos para derivar el valor de la clave de generación de valor de seguridad dinámico al dispositivo de seguridad extraíble. En algunas realizaciones el dispositivo de autenticación de usuario delega algunos de los cálculos criptográficos para generar el valor de seguridad dinámico al dispositivo de seguridad extraíble. En algunas realizaciones el dispositivo de seguridad extraíble comprende datos de referencia relacionados con autenticación de usuario (tales como, por ejemplo, valores de referencia para un PIN o contraseña de usuario o una plantilla de referencia para una biométrica del usuario) y el dispositivo de autenticación de usuario usa el dispositivo de seguridad extraíble para autenticar el usuario (p. ej. teniendo el dispositivo de seguridad

extraíble que verificar un PIN o contraseña de usuario o una biométrica relacionada con el usuario).

Por ejemplo en algunas realizaciones el dispositivo (240) de autenticación de usuario puede comprender una interfaz (390) de comunicación que comprende un lector (391) de tarjeta inteligente y el dispositivo de seguridad extraíble puede comprender una tarjeta (395) de tarjeta inteligente o SIM (Módulo de Identidad de Abonado). En algunas realizaciones algunos aspectos de la comunicación entre la tarjeta inteligente y el dispositivo de autenticación de usuario pueden especificarse por la norma ISO/IEC 7816. En algunas realizaciones la tarjeta inteligente puede comprender una tarjeta expedida por una institución financiera. En algunas realizaciones la tarjeta inteligente puede comprender una tarjeta EMV (Europay-Mastercard-Visa). En algunas realizaciones el dispositivo de autenticación de usuario puede cumplir parcial o completamente con la norma CAP (Programa de Autenticación de Chip).

Generar un mensaje de respuesta.

El dispositivo de autenticación de usuario puede estar adaptado para generar un mensaje de respuesta que comprende al menos el valor de seguridad dinámico generado u obtenido. En algunas realizaciones el mensaje de respuesta puede comprender también elementos de datos adicionales tales como, por ejemplo, un identificador de sesión que el dispositivo de autenticación de usuario ha extraído del mensaje de iniciación de autenticación, y/o un identificador de dispositivo de autenticación de usuario (tal como un número de serie del dispositivo de autenticación de usuario) y/o un identificador de usuario (tal como un ID de usuario o un nombre de usuario) y/o un identificador de aplicación y/o un número aleatorio utilizado solo una vez. En algunas realizaciones el dispositivo de autenticación de usuario puede estar adaptado para encriptar el mensaje de respuesta completa o parcialmente.

Hacer que el mensaje de respuesta esté disponible para el usuario o servidor de autenticación.

En algunas realizaciones el dispositivo de autenticación de usuario puede estar adaptado para que el mensaje de respuesta esté disponible para el usuario, de modo que el usuario pueda reenviar el mensaje de respuesta al servidor de autenticación (por ejemplo copiando el mensaje de respuesta al dispositivo de acceso que puede reenviar el mensaje de respuesta directamente al servidor de autenticación o al servidor de aplicación que puede reenviarlo a su vez al servidor de autenticación). En algunas realizaciones el dispositivo de autenticación de usuario puede estar adaptado, por ejemplo, para visualizar el mensaje de respuesta como una cadena de dígitos o caracteres numéricos o hexadecimales o alfanuméricos que el usuario puede leer y copiar al dispositivo de acceso. En algunas realizaciones el dispositivo de autenticación de usuario puede estar adaptado, por ejemplo, para emitir una secuencia de fragmentos de voz sintetizados que representan una cadena de dígitos o caracteres numéricos o hexadecimales o alfanuméricos que el usuario puede escuchar y copiar al dispositivo de acceso.

En algunas realizaciones el dispositivo de autenticación de usuario puede adaptarse para enviar el mensaje de respuesta a un servidor de destino. En algunas realizaciones el dispositivo de autenticación de usuario puede adaptarse para enviar el mensaje de respuesta a un servidor de destino a través de una red de comunicación inalámbrica (tal como por ejemplo una red de telefonía móvil) usando su interfaz de comunicación de datos inalámbrica. En algunas realizaciones el dispositivo de autenticación puede estar adaptado, por ejemplo, para enviar el mensaje de respuesta mediante un SMS (Servicio de Mensajes Cortos) o puede estar adaptado para enviar el mensaje de respuesta a través de una conexión de IP inalámbrica, por ejemplo, en forma de un mensaje de POST de HTTP.

Tipos de dispositivos de autenticación de usuario.

En algunas realizaciones el dispositivo de autenticación de usuario puede ser un dispositivo de seguridad de hardware especializado. Un dispositivo de seguridad de hardware especializado en este contexto significa que su función primaria es recibir y procesar un mensaje de iniciación de autenticación y generar un valor de seguridad dinámico en respuesta. Significa adicionalmente que el dispositivo comprende un componente de almacenamiento adaptado para almacenar de manera segura secretos tales como claves criptográficas y/o valores de PIN y que su firmware de aplicación no puede cambiarse o actualizarse, o que puede cambiarse o actualizarse únicamente usando protocolos de actualización de firmware que usan mecanismos criptográficos para probar al dispositivo la autenticidad de la actualización de firmware.

En otras realizaciones el dispositivo de autenticación de usuario puede comprender un dispositivo la función primaria del cual no es recibir y procesar un mensaje de iniciación de autenticación y generar un valor de seguridad dinámico en respuesta y que puede permitir la adición o actualización libre de aplicaciones de software por el usuario. Por ejemplo el dispositivo de autenticación de usuario puede comprender un teléfono inteligente.

Método para asegurar una aplicación.

Las **Figuras 4a y 4b** ilustran un método (400) para asegurar una aplicación remotamente accesible que se accede por un usuario usando, por ejemplo, un sistema tal como el sistema analizado en relación a la Figura 2.

El método comprende las siguientes etapas.

Interacción inicial del usuario con la aplicación

En una primera etapa una aplicación remotamente accesible alojada por un servidor de aplicación interactúa con un usuario intercambiando (410) datos y mensajes con un dispositivo de acceso que se usa por el usuario para acceder e interactuar con la aplicación. Por ejemplo la aplicación puede recibir una solicitud de acceso desde el dispositivo de acceso, o la aplicación puede recibir desde el dispositivo de acceso (p. ej. en un mensaje de solicitud de transacción) datos de transacción emitidos por el usuario. En algunas realizaciones la aplicación es una aplicación basada en web y la aplicación interactúa con un explorador web en el dispositivo de acceso, p. ej., intercambiando mensajes de HTTP. En algún punto la aplicación puede requerir que el usuario o los datos emitidos por el usuario se autentiquen. En algunas realizaciones el usuario puede haber comunicado su (reivindicada o supuesta) identidad a la aplicación antes del comienzo del proceso de autenticación. En otras realizaciones la aplicación inicia el proceso de autenticación antes de que el usuario se haya identificado. Por ejemplo, en algunas realizaciones el usuario puede emitir una solicitud de acceso que comprende el nombre de usuario o nombre de inicio de sesión o número de cuenta del usuario. En otras realizaciones ese usuario puede emitir una solicitud de acceso anónima que no comprende una indicación de la identidad de usuario.

Obtener o generar un mensaje (420) de iniciación de autenticación.

En una siguiente etapa la aplicación puede recopilar (421) un número de elementos de datos y ensamblar estos elementos de datos en un mensaje de iniciación de autenticación. La aplicación puede recopilar, por ejemplo, un desafío, y/o datos de transacción a autenticarse (y que pueden tener que presentarse por el dispositivo de autenticación de usuario al usuario para aprobación), y/o un identificador de sesión, y/o un identificador de aplicación (que puede usarse por el usuario para identificar la aplicación y que puede presentarse por el dispositivo de autenticación de usuario al usuario para aprobación), y/o una credencial de servidor (que puede verificarse por el dispositivo de autenticación de usuario para autenticar el origen y/o los contenidos del mensaje de iniciación de autenticación), y/o una respuesta o dirección de destino (que puede usarse por el dispositivo de autenticación de usuario cuando envía un mensaje de respuesta), y/o un número aleatorio utilizado solo una vez (que puede usarse por el dispositivo de autenticación de usuario para derivar claves criptográficas secretas tales como, por ejemplo, una clave de verificación de credencial de servidor o una clave de generación de valor de seguridad dinámico), y/o un identificador de usuario (por ejemplo un nombre de usuario que el usuario proporcionó en una solicitud de acceso o de inicio de sesión). Algunos o todos estos elementos de datos pueden haberse generado por la aplicación. Algunos o todos estos elementos de datos pueden haberse generado por otra entidad y pueden haberse obtenido por la aplicación desde esta entidad. Esta entidad puede ser, por ejemplo, un servidor de autenticación confiable por la aplicación. Ejemplos de elementos de datos que pueden haberse generado y proporcionado a la aplicación por otra entidad tal como un servidor de autenticación confiable pueden comprender: un desafío, y/o un identificador de sesión, y/o una credencial de servidor, y/o un número aleatorio utilizado solo una vez, en algunas realizaciones el mismo elemento de datos puede tener más de una función. Por ejemplo, en algunas realizaciones un único elemento de datos puede combinar la función de desafío, identificador de sesión y número aleatorio utilizado solo una vez.

En algunas realizaciones recopilar los elementos de datos y/o usarlos para generar un mensaje de iniciación de autenticación puede hacerse completamente por la aplicación en el servidor de aplicación. En algunas realizaciones la recopilación de los elementos de datos y/o usarlos para generar un mensaje de iniciación de autenticación puede hacerse parcialmente por la aplicación en el servidor de aplicación y puede hacerse parcialmente bajo el control de la aplicación en el dispositivo de acceso (p. ej. por una miniaplicación tal como una miniaplicación de java o un módulo de extensión de explorador asociado con la aplicación). En algunas realizaciones la recopilación de los elementos de datos y/o usarlos para generar un mensaje de iniciación de autenticación puede hacerse completamente bajo el control de la aplicación en el dispositivo de acceso (p. ej. por una miniaplicación tal como una miniaplicación de java o un módulo de extensión de explorador asociado con la aplicación). En algunas realizaciones el mensaje de iniciación de autenticación completo puede generarse por otra entidad tal como un servidor de autenticación confiable y proporcionarse a la aplicación (por ejemplo enviando el mensaje de iniciación de autenticación generado al servidor de aplicación que aloja la aplicación o enviándolo al dispositivo de acceso con el que está interactuando el servidor de aplicación). Por ejemplo en algunas realizaciones el servidor de aplicación puede recopilar todos los elementos de datos y generar un mensaje de iniciación de autenticación y enviarlo al dispositivo de acceso. En algunas realizaciones el servidor de aplicación puede recopilar todos los elementos de datos y enviarlos al dispositivo de acceso donde el mensaje de iniciación de autenticación se genera usando estos elementos de datos (p. ej. por una miniaplicación tal como una miniaplicación java o un módulo de extensión de explorador asociado con la aplicación). En algunas realizaciones el servidor de aplicación puede recopilar algunos elementos de datos y enviarlos al dispositivo de acceso y el dispositivo de acceso puede recopilar algunos otros elementos de datos y el mensaje de iniciación de autenticación se genera en el dispositivo de acceso usando estos elementos de datos (p. ej. por una miniaplicación tal como una miniaplicación de java o un módulo de extensión de explorador asociado con la aplicación). En algunas realizaciones otra entidad tal como un servidor de autenticación puede recopilar todos los elementos de datos y generar el mensaje de iniciación de autenticación y enviarlo al servidor de aplicación (que puede reenviarlo al dispositivo de acceso) o enviarlo directamente al dispositivo de acceso.

Generar una credencial (422) de servidor

En algunas realizaciones el mensaje de iniciación de autenticación comprende una credencial de servidor. En algunas realizaciones el mensaje de iniciación de autenticación puede generarse usando un algoritmo criptográfico

parametrizado por una clave secreta. En algunas realizaciones la credencial del servidor se genera por el servidor de autenticación. La credencial del servidor puede usarse para unir y/o autenticar criptográficamente al menos algunos de los elementos de datos comprendidos en el mensaje de iniciación de autenticación. Por ejemplo en algunas realizaciones la credencial del servidor puede usarse para autenticar un identificador de aplicación y/o datos relacionados con transacción comprendidos en el mensaje de iniciación de autenticación. En algunas realizaciones la credencial del servidor puede usarse, por ejemplo, para unir criptográficamente, por ejemplo, un valor de seguridad dinámico generado de servidor comprendido en el mensaje de iniciación de autenticación a un identificador de aplicación y/o datos relacionados con transacción también comprendidos en el mensaje de iniciación de autenticación. En algunas realizaciones la credencial del servidor comprende una porción encriptada del mensaje de iniciación de autenticación. En las realizaciones la credencial del servidor comprende todo el mensaje de iniciación de autenticación encriptado completo. En algunas realizaciones la credencial del servidor comprende una porción encriptada del mensaje de iniciación de autenticación que comprende al menos un valor de seguridad dinámico generado de servidor.

Emitir (430) en el dispositivo de acceso una señal que codifica la representación de un mensaje de iniciación de autenticación.

El dispositivo de acceso puede obtener el mensaje de iniciación de autenticación o una representación de él como se describe en más detalle a continuación. Después de haber obtenido el mensaje de iniciación de autenticación o una representación de él, el dispositivo de acceso emite una señal que codifica el mensaje de iniciación de autenticación. El dispositivo de acceso puede emitir esta señal usando su interfaz de salida de usuario como se describe en más detalle a continuación.

Capturar en el dispositivo de autenticación de usuario la señal emitida y decodificar para obtener el mensaje (435) de iniciación de autenticación.

Cuando la señal que codifica el mensaje de iniciación de autenticación se está emitiendo por el dispositivo de acceso, puede capturarse por el dispositivo de autenticación de usuario como se describe en más detalle a continuación. El mensaje de iniciación de autenticación puede a continuación decodificarse por el dispositivo de autenticación de usuario desde la señal capturada como se describe en más detalle a continuación.

Procesar el mensaje de iniciación de autenticación y generar (440) un mensaje de respuesta

Una vez que se ha obtenido el mensaje de iniciación de autenticación por el dispositivo de autenticación de usuario, puede procesarse y puede generarse un mensaje de respuesta que comprende un valor de seguridad dinámico por el dispositivo de autenticación de usuario.

El mensaje de iniciación de autenticación puede procesarse para obtener sus contenidos y, si fuera aplicable (p. ej. si el mensaje de iniciación de autenticación comprende una credencial de servidor), autenticarlo o sus contenidos como se describe en más detalle a continuación.

Verificación (441) de credencial de servidor

Si fuera aplicable (p. ej. si el mensaje de iniciación de autenticación comprende una credencial de servidor), puede procesarse para autenticar su o sus contenidos como se describe en más detalle a continuación. En algunas realizaciones el mensaje de iniciación de autenticación puede comprender una credencial de servidor y este credencial de servidor puede verificarse por el dispositivo de autenticación de usuario como se describe en más detalle a continuación p. ej. para autenticar el origen del mensaje de iniciación de autenticación o alguno de sus contenidos. Si la verificación de credencial de servidor falla, el dispositivo de autenticación de usuario puede abortar etapas adicionales del proceso de autenticación. En un caso de este tipo el dispositivo de autenticación de usuario puede informar al usuario del fallo.

Presentación (442) de identidad de aplicación

En algunas realizaciones el mensaje de iniciación de autenticación comprende un identificador de aplicación que el dispositivo de autenticación de usuario usa para obtener una representación de la identidad de aplicación. La representación de la identidad de aplicación puede presentarse al usuario por medio de su interfaz de salida de usuario y la aprobación del usuario de la representación presentada de la identidad de aplicación puede capturarse por el dispositivo de autenticación de usuario. La aprobación puede usarse en etapas adicionales del proceso de autenticación.

En algunas realizaciones el mensaje de iniciación de autenticación puede comprender un identificador de aplicación así como una credencial de servidor que autentica al menos el identificador de aplicación comprendido en el mensaje de iniciación de autenticación, mediante el cual la credencial del servidor ha sido generada por el servidor de autenticación y mediante el cual el servidor de autenticación puede haber verificado que el identificador de aplicación coincide con la identidad de la aplicación para la que ha generado la credencial del servidor de modo que el usuario puede estar seguro de que el mensaje de iniciación de autenticación de hecho se origina desde la aplicación asociada con el identificador de aplicación.

Presentación (443) de datos de transacción

En algunas realizaciones el mensaje de iniciación de autenticación puede comprender uno o más elementos de datos relacionados con transacción que pueden presentarse al usuario por el dispositivo de autenticación de usuario por medio de su interfaz de salida de usuario para revisarse y/o aprobarse por el usuario. La aprobación del usuario de los datos relacionados con transacción presentados puede capturarse por el dispositivo de autenticación de usuario. La aprobación puede usarse en etapas adicionales del proceso de autenticación.

Entrada (444) de PIN

En algunas realizaciones puede solicitarse al usuario por el dispositivo de autenticación de usuario que proporcione un PIN o contraseña y el dispositivo de autenticación de usuario puede capturar el PIN o contraseña que el usuario proporciona y usarla como se ha descrito anteriormente. En algunas realizaciones la entrada del usuario de un PIN o contraseña actúa como una aprobación implícita. Puede considerarse por ejemplo por el dispositivo de autenticación de usuario como una aprobación de elementos de datos o mensajes (p. ej. representando la identidad de aplicación o datos relacionados con transacción) que se han presentado por el dispositivo de autenticación de usuario al usuario hasta este punto en el proceso de autenticación, o puede considerarse una aprobación del usuario para el dispositivo de autenticación de usuario para que siga adelante con la generación de un valor de seguridad dinámico y/o generación del mensaje de respuesta y/o envío del mensaje de respuesta a un servidor de destino.

Obtener (445) aprobación del usuario.

Puede requerirse una o más aprobaciones de usuario implícitas o explícitas por el dispositivo de autenticación de usuario (p. ej. una aprobación para seguir adelante con el proceso de autenticación, o una aprobación de la identidad de aplicación o una aprobación de la fecha relacionada con la transacción). En algunas realizaciones el dispositivo de autenticación de usuario solicita explícitamente que el usuario proporcione una aprobación (p. ej. visualizar un mensaje tal como "¿aprueba los siguientes datos de transacción?" u "¿obtiene acceso ahora a la siguiente aplicación?") y presenta explícitamente al usuario con una elección de si aprobar u observar (por ejemplo: "sí/no" o "continuar/cancelar") y el usuario puede proporcionar explícitamente la aprobación haciendo una elección e indicando explícitamente la elección apropiada al dispositivo de autenticación de usuario. En algunas realizaciones el usuario indica la aprobación de una manera implícita. Por ejemplo simplemente continuando (en lugar de abortar) la interacción de usuario normal cuando se está presentando con ciertos datos o mensajes a revisarse o, por ejemplo, introduciendo un PIN o contraseña cuando ciertos datos o mensajes se han presentado al usuario.

Uso y verificación de aprobaciones de usuario en el proceso de autenticación.

La continuación del proceso de autenticación puede depender de una o más de estas aprobaciones del usuario y el proceso de autenticación puede abortarse en algún punto si una o más de las aprobaciones no se proporcionan por el usuario o si el usuario las desaprueba. Por ejemplo en algunas realizaciones la generación de un valor de seguridad dinámico y/o la generación del mensaje de respuesta que comprende el valor de seguridad dinámico puede abortarse si la aprobación del usuario ha fallado. En algunas realizaciones, si no se han obtenido las aprobaciones del usuario requeridas, el dispositivo de autenticación de usuario puede no enviar el mensaje de respuesta generado a un servidor de destino o puede no presentar el mensaje de respuesta al usuario.

En algunas realizaciones las aprobaciones del usuario pueden estar implícitas en el mensaje de respuesta ya que son una condición necesaria para que el dispositivo de autenticación de usuario genere el valor de seguridad dinámico y/o el mensaje de respuesta o para que el dispositivo de autenticación de usuario presente el mensaje de respuesta al usuario o para enviar el mensaje de respuesta a un servidor de destino. En tales realizaciones el servidor de autenticación que verifica el valor de seguridad dinámico puede verificar implícitamente las aprobaciones del usuario verificando el valor de seguridad dinámico puesto que el servidor de autenticación no recibiría nunca un mensaje de respuesta con un valor de seguridad dinámico válido si el usuario no hubiera proporcionado las aprobaciones requeridas.

En algunas realizaciones el dispositivo de autenticación de usuario incluye elementos de datos que indican las aprobaciones del usuario (o la ausencia de las mismas) en el cálculo criptográfico del valor de seguridad dinámico y puede o puede no incluir estos elementos de datos en el mensaje de respuesta. Por ejemplo el dispositivo de autenticación de usuario puede usar un elemento de datos que comprende banderas de bits que indican si se solicitó al usuario proporcionar una cierta aprobación y/o si el usuario de hecho proporcionó esta aprobación. En algunas realizaciones el dispositivo de autenticación de usuario puede incluir estos elementos de datos que son indicativos de las aprobaciones del usuario como entradas para que el algoritmo criptográfico genere el valor de seguridad dinámico y puede incluir estos elementos de datos también en los contenidos del mensaje de respuesta. Un servidor de verificación que recibe el mensaje de respuesta puede a continuación verificar si estos elementos de datos indican un estado satisfactorio con respecto a las aprobaciones por el usuario y puede verificar criptográficamente si el valor de seguridad dinámico comprendido en el mismo mensaje de respuesta es coherente con los valores de estos elementos de datos. En otras realizaciones el dispositivo de autenticación de usuario puede incluir los elementos de datos que son indicativos de las aprobaciones del usuario como entradas para que el algoritmo criptográfico genere el valor de seguridad dinámico pero puede no incluir estos elementos de datos también en los

contenidos del mensaje de respuesta. Un servidor de verificación que recibe el mensaje de respuesta puede a continuación asumir ciertos valores para estos elementos de datos que son obligatorios para que el mensaje de respuesta se acepte (p. ej. valores que indican que el usuario proporcionó todas las aprobaciones requeridas) y puede verificar criptográficamente si el valor de seguridad dinámico comprendido en el mismo mensaje de respuesta es coherente con estos valores supuestos para estos elementos de datos.

Generar un valor (449) de seguridad dinámico

Después de que el dispositivo de autenticación de usuario haya obtenido todos los elementos de datos que se requieren para generar un valor de seguridad dinámico, el valor de seguridad dinámico puede generarse como se ha descrito anteriormente.

La generación del valor de seguridad dinámico por el dispositivo de autenticación de usuario puede estar condicionada a ciertas verificaciones y/o eventos. Por ejemplo, puede estar condicionada a la verificación satisfactoria de una credencial de servidor comprendida en el mensaje de iniciación de autenticación, o puede estar condicionada a que el usuario proporcione ciertas aprobaciones requeridas, o puede estar condicionada a la verificación satisfactoria de un PIN o contraseña introducido por el usuario.

Generar (450) un mensaje de respuesta

Como se ha descrito anteriormente, un mensaje de respuesta puede generarse por el dispositivo de autenticación de usuario que comprende el valor de seguridad dinámico. El mensaje de respuesta puede comprender también otros elementos de datos tales como por ejemplo un elemento de datos relacionado con la identidad de aplicación, y/o un identificador de sesión, y/o un identificador de usuario (que puede almacenarse en el dispositivo de autenticación de usuario, o puede haberse extraído desde el mensaje de iniciación de autenticación, o puede haberse proporcionado al dispositivo de autenticación de usuario por el usuario), y/o un identificador de dispositivo de autenticación de usuario (que puede almacenarse en el dispositivo de autenticación de usuario tal como un número de serie), y/o banderas que indican aprobaciones de usuario.

La generación del mensaje de respuesta por el dispositivo de autenticación de usuario puede estar condicionada a ciertas verificaciones y/o eventos. Por ejemplo, puede estar condicionada a la verificación satisfactoria de una credencial de servidor comprendida en el mensaje de iniciación de autenticación, o puede estar condicionada a que el usuario proporcione ciertas aprobaciones requeridas, o puede estar condicionada a la verificación satisfactoria de un PIN o contraseña introducido por el usuario.

Hacer el mensaje de respuesta disponible para un servidor (460) de verificación.

El mensaje de respuesta generado puede a continuación comunicarse a un servidor de verificación tal como el servidor de autenticación.

Presentar el mensaje de respuesta al usuario (461).

En algunas realizaciones el mensaje de respuesta se presenta por el dispositivo de autenticación de usuario al usuario por medio de la interfaz de salida de usuario después de lo que el usuario puede copiar el mensaje de respuesta al dispositivo de acceso que a su vez puede enviar el mensaje de respuesta directamente a un servidor de verificación tal como el servidor de autenticación o puede enviarlo al servidor de aplicación que puede reenviarlo al servidor de verificación.

Presentar el mensaje de respuesta al usuario por el dispositivo de autenticación de usuario puede estar condicionado a ciertas verificaciones y/o eventos. Por ejemplo, puede estar condicionado a la verificación satisfactoria de una credencial de servidor comprendida en el mensaje de iniciación de autenticación, o puede estar condicionado a que el usuario proporcione ciertas aprobaciones requeridas, o puede estar condicionado a la verificación satisfactoria de un PIN o contraseña introducido por el usuario.

Enviar el mensaje de respuesta a un servidor (465) de destino.

En algunas realizaciones el mensaje de respuesta se envía a un servidor de destino (que puede ser, por ejemplo, el servidor de aplicación o el servidor de autenticación) por el dispositivo de autenticación de usuario usando una interfaz de comunicación de datos. En algunas realizaciones esta interfaz de comunicación de datos comprende una interfaz de comunicación de datos inalámbrica. En algunas realizaciones esta interfaz de comunicación de datos inalámbrica comprende una interfaz para enviar mensajes de datos a través de una red de comunicación móvil pública tal como una red de GSM o UMTS.

En algunas realizaciones la dirección de destino del servidor de destino se almacena en el dispositivo de autenticación de usuario. En algunas realizaciones el dispositivo de autenticación de usuario puede determinar la dirección de destino usando un elemento de datos relacionado con la dirección de destino extraído desde el mensaje de iniciación de autenticación. En algunas realizaciones el dispositivo de autenticación de usuario verifica si la dirección de destino determinada es permisible. Puede comparar, por ejemplo, la dirección de destino determinada a

una lista negra de direcciones prohibidas o a una lista blanca de direcciones permitidas o puede verificar si satisface un número de reglas.

Enviar el mensaje de respuesta a un servidor de destino indicado por la dirección de destino determinada por el dispositivo de autenticación de usuario puede estar condicionado a ciertas verificaciones y/o eventos. Por ejemplo, puede estar condicionado a la verificación satisfactoria de una credencial de servidor comprendida en el mensaje de iniciación de autenticación, o puede estar condicionado a que el usuario proporcione ciertas aprobaciones requeridas, o puede estar condicionado a la verificación satisfactoria de un PIN o contraseña introducido por el usuario.

Verificación del mensaje (470) de respuesta.

Después de que se ha recibido el mensaje de respuesta en el servidor de verificación, puede verificarse. La verificación del mensaje de respuesta puede comprender diversas etapas y partes de la verificación pueden hacerse por el servidor de aplicación y partes de la verificación pueden hacerse por el servidor de autenticación.

En algunas realizaciones parte de la verificación del mensaje de respuesta comprende si los valores de ciertos elementos de datos en el mensaje de respuesta tienen valores aceptables. En algunas realizaciones esto puede comprender verificar que algunos de estos valores están dentro de un cierto intervalo. En algunas realizaciones esto puede comprender verificar que algunos de estos valores tienen uno de un número limitado de valores permisibles. Por ejemplo en algunas realizaciones el mensaje de respuesta puede comprender banderas que indican si el usuario ha aprobado o no ciertos elementos de datos y parte de la verificación puede comprender verificar que estas banderas indican que el usuario ha proporcionado de hecho ciertas aprobaciones. En algunas realizaciones el mensaje de respuesta puede comprender un elemento de datos que está relacionado con la representación de un identificador de aplicación que se ha presentado al usuario y la verificación del mensaje de respuesta puede comprender verificar que el valor de este elemento de datos corresponde a la presentación del identificador de aplicación que el usuario se supone que revisó. Por ejemplo, en algunas realizaciones el mensaje de iniciación de autenticación puede comprender un URL que apunta a un logo de aplicación a recuperarse por el dispositivo de autenticación de usuario y presentarse al usuario. En algunas de estas realizaciones el mensaje de iniciación de autenticación y/o el proceso para recuperar el logo no se aseguran criptográficamente de modo que no puede excluirse que un logo incorrecto se presentara al usuario. Para detectar si se presentó un logo incorrecto al usuario, el dispositivo de autenticación de usuario en tales realizaciones puede incluir en el mensaje de respuesta (y posiblemente también en el cálculo del valor de seguridad dinámico) p. ej. un troceo del logo que se presentó de manera efectiva al usuario. La verificación del mensaje de respuesta puede a continuación comprender que este valor de troceo corresponde al logo que se supuso que se presentó al usuario. En algunas realizaciones el dispositivo de autenticación de usuario puede capturar alguna entrada del usuario e incluir esta en el mensaje de respuesta (y posiblemente también en el cálculo del valor de seguridad dinámico), por ejemplo en algunas realizaciones el dispositivo de autenticación de usuario puede solicitar que el usuario introduzca un PIN o contraseña que puede ser conocido para la aplicación o servidor de autenticación e incluir un elemento de datos representativo del PIN o contraseña en el mensaje de respuesta (posiblemente en una porción encriptada del mensaje de respuesta). Parte de la verificación del mensaje de respuesta puede a continuación comprender verificar el servidor apropiado el valor de este elemento de datos relacionado con el PIN o la contraseña.

Verificación del mensaje de respuesta puede comprender también verificación del valor (475) de seguridad dinámico.

En algunas realizaciones el mensaje de iniciación de autenticación puede comprender un valor de seguridad dinámico generado de servidor y la verificación del valor de seguridad dinámico en el mensaje de respuesta puede comprender comparar el valor de seguridad dinámico recibido en el mensaje de respuesta con el valor de seguridad dinámico generado de servidor.

En algunas realizaciones la verificación del valor de seguridad dinámico comprende verificar la validez criptográfica del valor de seguridad dinámico.

En algunas realizaciones esto comprende determinar valores de referencia para los elementos de datos que se supone que se han usado en el cálculo del valor de seguridad dinámico por el dispositivo de autenticación de usuario. En algunas realizaciones: la fuente de los valores de referencia de algunos de estos elementos de datos pueden ser el mensaje de respuesta (por ejemplo banderas de aprobación de usuario y/o datos relacionados con identidad de aplicación). En algunas realizaciones la fuente de los valores de referencia de algunos de estos elementos de datos pueden ser el servidor de aplicación (por ejemplo un desafío que la aplicación incluyó en el mensaje de iniciación de autenticación y que no está comprendido en el mensaje de respuesta sino que se usa como entrada en el cálculo del valor de seguridad dinámico, o por ejemplo datos relacionados con la transacción). En algunas realizaciones la fuente de los valores de referencia de algunos de estos elementos de datos pueden ser el servidor de autenticación (por ejemplo el valor de un desafío originalmente proporcionado por el servidor de autenticación). En algunas realizaciones la determinación de los valores de referencia de ciertos elementos de datos pueden basarse en suposiciones. Por ejemplo en algunas realizaciones el dispositivo de autenticación de usuario puede usar un valor relacionado con contador en el cálculo del valor de seguridad dinámico y el servidor de autenticación puede mantener una copia de este valor relacionado con el contador y usar un algoritmo de

sincronización para determinar el valor que puede suponerse que usará el dispositivo de autenticación de usuario, o el dispositivo de autenticación de usuario usa un valor relacionado con el tiempo en el cálculo del valor de seguridad dinámico y el servidor de autenticación puede estimar el valor de este valor relacionado con el tiempo basándose en el tiempo de recepción del mensaje de respuesta.

En algunas realizaciones la validación criptográfica del valor de seguridad dinámico comprende la recuperación de una clave de verificación criptográfica. En algunas realizaciones esta clave de verificación está asociada con el dispositivo de autenticación de usuario y puede recuperarse usando un identificador de dispositivo de autenticación de usuario comprendido en el mensaje de respuesta. En algunas realizaciones esta clave de verificación está asociada con el usuario y puede recuperarse usando un identificador de usuario comprendido en el mensaje de respuesta. En algunas realizaciones recuperar la clave de verificación puede comprender hacer una búsqueda en la base de datos usando un identificador de usuario o un elemento de datos relacionado con el identificador de dispositivo de autenticación de usuario como un índice de búsqueda. En algunas realizaciones recuperar la clave de verificación puede comprender hacer una derivación de clave o diversificación desde una clave maestra usando un identificador de usuario o un elemento de datos relacionado con el identificador de dispositivo de autenticación de usuario como derivación o semilla de diversificación.

En algunas realizaciones una clave de verificación usada en la verificación criptográfica del valor de seguridad dinámico comprende una clave simétrica secreta que se ha usado también por el dispositivo de autenticación de usuario en el cálculo del valor de seguridad dinámico. En algunas realizaciones una clave de verificación usada en la verificación criptográfica del valor de seguridad dinámico comprende una clave pública de un par de clave pública-privada, la clave privada de la cual se ha usado por el dispositivo de autenticación de usuario en el cálculo del valor de seguridad dinámico. En algunas realizaciones la validación criptográfica del valor de seguridad dinámico recibido comprende ejecutar un algoritmo criptográfico en los valores de referencia anteriormente mencionados usando la clave de verificación criptográfica anteriormente mencionada y comparar el resultado de esta operación criptográfica con el valor de seguridad dinámico recibido. Por ejemplo en algunas realizaciones la validación criptográfica del valor de seguridad dinámico recibido puede comprender calcular un troceo con clave o un MAC a través de los valores de referencia anteriormente mencionados (en donde el troceo con clave o algoritmo de MAC está parametrizado con una clave de verificación simétrica que puede haberse recuperado como se ha descrito anteriormente). En algunas realizaciones la validación criptográfica del valor de seguridad dinámico recibido comprende ejecutar un algoritmo criptográfico en el valor de seguridad dinámico recibido usando la clave de verificación criptográfica anteriormente mencionada y comparar el resultado de esta operación criptográfica con los valores de referencia anteriormente mencionados. Por ejemplo en algunas realizaciones la validación criptográfica del valor de seguridad dinámico recibido comprende desencriptar el valor de seguridad dinámico con un algoritmo de desencriptación asimétrico usando la clave pública que corresponde a la clave privada que se usó por el dispositivo de autenticación de usuario para generar el valor de seguridad dinámico, y posteriormente comparar el valor desencriptado con un troceo de los valores de referencia anteriormente mencionados.

Comunicar un resultado de verificación al servidor (480) de aplicación.

En algunas realizaciones al menos una parte de la verificación del mensaje de respuesta se hace por un servidor de autenticación confiable y el resultado de la verificación hecho por el servidor de autenticación confiable se comunica al servidor de aplicación. En algunas realizaciones además del resultado de verificación también pueden comunicarse otros elementos de datos al servidor de aplicación. Por ejemplo en algunas realizaciones el servidor de autenticación puede comunicar elementos de datos comprendidos en el mensaje de respuesta al servidor de aplicación, tal como, por ejemplo, un identificador de sesión o un identificador de usuario o un elemento de datos relacionado con la representación de la identidad de aplicación que se presentó al usuario u otros elementos de datos que pueden haberse presentado al usuario por el dispositivo de autenticación de usuario (tal como datos relacionados con transacción) o que pueden haberse proporcionado al dispositivo de autenticación de usuario por el usuario. Recibir un identificador de sesión puede permitir que el servidor de aplicación determine para qué sesión de aplicación son aplicables los resultados comunicados. Recibir un identificador de usuario puede permitir al servidor de aplicación determinar la identidad del usuario sin que el usuario tenga que proporcionar manualmente esa identidad a la aplicación aumentando por lo tanto la conveniencia de usuario global. Recibir datos que se han presentado al usuario por el dispositivo de autenticación de usuario permite que el servidor de aplicación verifique los datos correctos que se presentaron al usuario.

En algunas realizaciones puede asegurarse la comunicación entre el servidor de aplicación y el servidor de autenticación. Por ejemplo en algunas realizaciones los mensajes desde el servidor de autenticación al servidor de aplicación pueden autenticarse criptográficamente para demostrar al servidor de aplicación que se originaron desde el servidor de autenticación legítimo. En algunas realizaciones los mensajes desde un servidor de aplicación al servidor de autenticación pueden autenticarse criptográficamente para demostrar que se originaron desde un servidor de aplicación legítimo. En algunas realizaciones algunos mensajes pueden encriptarse para garantizar confidencialidad de los contenidos de los mensajes. En algunas realizaciones algunos mensajes pueden protegerse criptográficamente (p. ej. con sumas de comprobación criptográficas o firmas) para garantizar la integridad de los contenidos de los mensajes.

En algunas realizaciones el servidor de autenticación puede determinar el servidor de aplicación y enviar el resultado

de verificación posiblemente junto con datos adicionales al servidor de aplicación. En algunas realizaciones los datos adicionales pueden comprender datos (tales como un identificador de sesión o un identificador de usuario) que permiten que el servidor de aplicación enlace los resultados de verificación proporcionados por el servidor de autenticación a una sesión de aplicación.

En otras realizaciones el servidor de aplicación puede interrogar al servidor de autenticación para el resultado de verificación. En los mensajes de solicitud de interrogación que el servidor de aplicación envía al servidor de autenticación, el servidor de aplicación puede incluir datos que el servidor de autenticación puede usar para adaptar la solicitud de interrogación al correcto de los mensajes de respuesta que ha recibido. Estos datos pueden incluir, por ejemplo, datos tales como un identificador de sesión o un identificador de usuario que puede adaptar correspondientes elementos de datos en el mensaje de respuesta. En algunas realizaciones el servidor de aplicación también proporciona al servidor de autenticación datos que pueden requerirse para la validación del valor de seguridad dinámico tales como, por ejemplo, los valores de datos relacionados con transacción que se han usado en el cálculo del valor de seguridad dinámico.

Comunicar datos adicionales relacionados con el usuario al servidor (499) de aplicación.

En algunas realizaciones el servidor de autenticación confiable puede almacenar y gestionar datos relacionados con el usuario que no se requieren para la verificación del mensaje de respuesta sino que pueden ser de valor para la aplicación. Tales datos pueden incluir, por ejemplo, el nombre de usuario del usuario para la aplicación dada, información personal (tal como el nombre real del usuario, dirección física y/o número de teléfono), información financiera (tal como el número de tarjeta de crédito), y/o información de perfil de usuario. En algunas realizaciones el servidor de autenticación puede pasar alguna de esta información a la aplicación junto con la comunicación del resultado de verificación. Esto puede depender de la verificación satisfactoria del valor de seguridad dinámico. En algunas realizaciones esto puede ser el objeto de reglas de política y una configuración de perfil de usuario. Por ejemplo en algunas realizaciones un usuario puede tener un perfil con el servidor de autenticación que comprende una pluralidad de datos relacionados con el usuario y el usuario puede configurar ese perfil para indicar qué datos pueden comunicarse a qué aplicación en qué condiciones. En algunas realizaciones el mensaje de iniciación de autenticación puede comprender una solicitud para presentarse al usuario por el dispositivo de autenticación de usuario para aprobar que el servidor de autenticación pase ciertos datos al servidor de aplicación (tal como por ejemplo el número de teléfono o dirección del usuario o número de tarjeta de crédito). El dispositivo de autenticación de usuario puede presentar esta solicitud al usuario e incluir la respuesta del usuario en el mensaje de respuesta y en el cálculo del valor de seguridad dinámico. Tras verificación positiva del mensaje de respuesta el servidor de autenticación puede concluir que el usuario ha aprobado la liberación de los datos solicitados a la aplicación y comunicar los datos solicitados al servidor de aplicación

En algunas realizaciones la aplicación puede incluir en el mensaje de iniciación de autenticación solicitudes para que el usuario proporcione ciertos datos (tales como una contraseña específica de aplicación) o solicitudes para liberar a la aplicación de ciertos datos almacenados por el servidor de autenticación mediante los cuales el servidor de autenticación puede, tras una verificación del mensaje de respuesta con éxito, comunicar los datos solicitados (es decir la información introducida o liberada) al servidor de aplicación. En algunas de estas realizaciones la comunicación de la fecha solicitada al servidor de aplicación por el servidor de autenticación puede depender de la verificación satisfactoria por el servidor de autenticación que el dispositivo de autenticación de usuario presentó una representación de la identidad de aplicación al usuario que el usuario aprobó y que la representación de la identidad de aplicación a la que se ha presentado y se ha aprobado por el usuario de hecho, coincide con la identidad de la aplicación que solicita los datos. En algunas de estas realizaciones el identificador de aplicación en el mensaje de iniciación de autenticación se autentica por una credencial de servidor también comprendida en el mensaje de iniciación de autenticación de manera que el usuario puede estar seguro de que la solicitud para los datos de hecho proviene de la aplicación pretendida.

Reaccionar en el servidor de aplicación como una función del resultado (490) de verificación.

Dependiendo del resultado de la verificación del mensaje de respuesta la aplicación puede tomar la acción apropiada. Por ejemplo en caso de una verificación satisfactoria la aplicación puede conceder acceso al usuario o puede ejecutar la transacción (491) emitida, y en caso de una verificación insatisfactoria la aplicación puede rechazar el acceso al usuario o para ejecutar la transacción (492) emitida.

Enlace criptográfico del identificador de aplicación al valor de seguridad dinámico.

En algunas realizaciones el mensaje de iniciación de autenticación comprende un identificador de aplicación que se usa por el dispositivo de usuario de autenticación para obtener una representación de la identidad de aplicación que presenta al usuario. En algunas realizaciones este identificador de aplicación o la correspondiente representación de la identidad de aplicación pueden enlazarse criptográficamente al valor de seguridad dinámico que el dispositivo de autenticación de usuario puede generar.

En algunas realizaciones el identificador de aplicación o la representación correspondiente de la identidad de aplicación se enlazan criptográficamente de manera directa al valor de seguridad dinámico generado. Por ejemplo

en algunas realizaciones el identificador de aplicación o la correspondiente representación de la aplicación (o un elemento de datos matemáticamente relacionado con el identificador de aplicación o la correspondiente representación de la aplicación) es uno de los elementos de datos de entrada para el algoritmo criptográfico usado por el dispositivo de autenticación de usuario para generar el valor de seguridad dinámico.

En algunas realizaciones el identificador de aplicación o la correspondiente representación de la identidad de aplicación se enlaza criptográficamente de manera indirecta al valor de seguridad dinámico generado. Por ejemplo en algunas realizaciones el identificador de aplicación comprendido en el mensaje de iniciación de autenticación se enlaza criptográficamente a otros elementos de datos en el mensaje de iniciación de autenticación (por ejemplo por medio de una credencial de servidor) que puede usarse por el dispositivo de autenticación de usuario como el elemento de datos de entrada para el algoritmo criptográfico usado por el dispositivo de autenticación de usuario para generar el valor de seguridad dinámico. En algunas realizaciones este enlace criptográfico entre el identificador de aplicación y otros elementos de datos comprendidos en el mensaje de iniciación de autenticación pueden verificarse por el dispositivo de autenticación de usuario. Por ejemplo en algunas realizaciones el identificador de aplicación se enlaza criptográficamente por una credencial de servidor (tal como una firma de servidor o un troceo con clave o un MAC a través de datos del mensaje de iniciación de autenticación) a otros elementos de datos (tales como un desafío o un identificador de sesión) en el mensaje de iniciación de autenticación que el dispositivo de autenticación de usuario (después de la verificación satisfactoria de la credencial del servidor) usa como entrada en el algoritmo criptográfico para la generación del valor de seguridad dinámico.

En algunas realizaciones el mensaje de iniciación de autenticación puede comprender un identificador de aplicación y un valor de seguridad dinámico generado de servidor que se enlazan criptográficamente (p. ej. por una credencial de servidor) mediante la cual el dispositivo de autenticación de usuario puede incluir este valor de seguridad dinámico generado de servidor en el mensaje de respuesta mediante el cual esta inclusión puede ser condicional tras la verificación satisfactoria por el dispositivo de autenticación de usuario del enlace criptográfico entre el identificador de aplicación y el valor de seguridad dinámico generado de servidor en el mensaje de iniciación de autenticación).

Modos para llevar a cabo la invención

Algunas realizaciones de los métodos según la invención.

Una primera clase de realizaciones de los métodos de la presente invención comprende métodos para asegurar la interacción con una aplicación mediante un usuario que accede remotamente a dicha aplicación a través de un dispositivo de acceso que está conectado a un servidor de aplicación que aloja dicha aplicación, comprendiendo los métodos las etapas de:

en un dispositivo de autenticación de usuario capturar una señal emitida por el dispositivo de acceso, dicha señal codificada con un mensaje de iniciación de autenticación, dicho mensaje de iniciación de autenticación que comprende al menos un identificador de aplicación que corresponde a una identidad de la aplicación;

en el dispositivo de autenticación de usuario decodificar dicha señal y obtener el mensaje de iniciación de autenticación;

en el dispositivo de autenticación de usuario recuperar desde el mensaje de iniciación de autenticación el identificador de aplicación;

en el dispositivo de autenticación de usuario usar el identificador de aplicación para obtener una representación interpretable humana de la identidad de aplicación y presentar la representación de identidad de aplicación obtenida al usuario usando una interfaz de salida de usuario del dispositivo de autenticación de usuario;

en el dispositivo de autenticación de usuario obtener desde el usuario, usando una interfaz de entrada de usuario del dispositivo de autenticación de usuario, una aprobación para generar un mensaje de respuesta y hacer el mensaje de respuesta disponible a un servidor de verificación;

en el dispositivo de autenticación de usuario generar un valor de seguridad dinámico usando un primer algoritmo criptográfico parametrizado con una clave de generación criptográfica de valor de seguridad dinámico y usar al menos un elemento de datos personalizado que está asociado con el usuario particular o el dispositivo de autenticación de usuario particular, en donde el valor de seguridad dinámico generado se enlaza criptográficamente a la identidad de aplicación presentada al usuario;

en el dispositivo de autenticación de usuario generar un mensaje de respuesta que comprende al menos el valor de seguridad dinámico generado;

hacer el mensaje de respuesta generado disponible a un servidor de verificación;

en el servidor de verificación recibir el mensaje de respuesta;

verificar el mensaje de respuesta que incluye verificar la validez del valor de seguridad dinámico;

comunicar el resultado de la verificación del mensaje de respuesta a la aplicación.

Una segunda clase de realizaciones de los métodos de la presente invención comprende métodos de la primera clase en donde el mensaje de respuesta comprende adicionalmente un elemento de datos que es indicativo de una identidad del usuario o una identidad del dispositivo de autenticación de usuario y en donde dicho elemento de datos indicativo de la identidad de usuario o la identidad del dispositivo de autenticación de usuario se usa para determinar una identidad de usuario y en donde dicha identidad de usuario también se comunica a la aplicación.

Una tercera clase de realizaciones de los métodos de la presente invención comprende cualquiera de los métodos de la primera y segunda clases en donde la identidad de usuario se determina también como una función de la identidad de aplicación.

Una cuarta clase de realizaciones de los métodos de la presente invención comprende cualquiera de los métodos de la primera a la tercera clases en donde todos los datos dependientes de la aplicación usados para obtener la representación de la identidad de aplicación se obtienen por el dispositivo de autenticación de usuario desde una fuente externa al dispositivo de autenticación de usuario o desde el mensaje de iniciación de autenticación.

Una quinta clase de realizaciones de los métodos de la presente invención comprende cualquiera de los métodos de la primera a cuarta clases que comprende adicionalmente las etapas de generar una credencial de servidor a incluirse en el mensaje de iniciación de autenticación, dicha generación usando un segundo algoritmo criptográfico parametrizado con una clave de generación de credencial de servidor criptográfico; recuperar en el dispositivo de autenticación de usuario desde el mensaje de iniciación de autenticación la credencial de servidor incluida; y verificar en el dispositivo de autenticación de usuario la credencial del servidor usando un tercer algoritmo criptográfico parametrizado con una clave de verificación de credencial de servidor criptográfico.

Una sexta clase de realizaciones de los métodos de la presente invención comprende cualquiera de los métodos de la quinta clase en donde el identificador de aplicación comprendido en el mensaje de iniciación de autenticación está enlazado criptográficamente a la credencial del servidor.

Una séptima clase de realizaciones de los métodos de la presente invención comprende cualquiera de los métodos de la primera a sexta clases en donde la etapa de generar un mensaje de respuesta comprende adicionalmente en el dispositivo de autenticación de usuario que incluye en el mensaje de respuesta generado por el dispositivo de autenticación de usuario un elemento de datos indicativo de la representación de identidad de aplicación presentada al usuario.

Una octava clase de realizaciones de los métodos de la presente invención comprende cualquiera de los métodos de la séptima clase que comprende adicionalmente verificar en el servidor de verificación si el elemento de datos que es indicativo de la representación de identidad de aplicación presentada al usuario es coherente con la identidad de aplicación indicada por el identificador de aplicación comprendido en el mensaje de iniciación de autenticación.

Una novena clase de realizaciones de los métodos de la presente invención comprende cualquiera de los métodos de la primera a octava clases que comprende adicionalmente las etapas de: recuperar en el dispositivo de autenticación de usuario desde el mensaje de iniciación de autenticación datos relacionados con transacción comprendidos en el mensaje de iniciación de autenticación; presentar en el dispositivo de autenticación de usuario los datos relacionados con transacción recuperados usando una interfaz de salida de usuario del dispositivo de autenticación de usuario; en donde el valor de seguridad dinámico generado se enlaza criptográficamente a los datos relacionados con transacción.

Una décima clase de realizaciones de los métodos de la presente invención comprende cualquiera de los métodos de la novena clase que comprende adicionalmente las etapas de generar una credencial de servidor para incluirse en el mensaje de iniciación de autenticación, dicha generación usando un segundo algoritmo criptográfico parametrizado con una clave de generación de credencial de servidor criptográfico; recuperar en el dispositivo de autenticación de usuario desde el mensaje de iniciación de autenticación la credencial de servidor incluida; verificar en el dispositivo de autenticación de usuario la credencial del servidor usando un tercer algoritmo criptográfico parametrizado con una clave de verificación de credencial de servidor criptográfico; en donde la credencial del servidor está enlazada criptográficamente a los datos relacionados con transacción.

Una undécima clase de realizaciones de los métodos de la presente invención comprende cualquiera de los métodos de la novena clase que comprende adicionalmente las etapas de incluir en el dispositivo de autenticación de usuario en el mensaje de respuesta generado por el dispositivo de autenticación de usuario elementos de datos que son indicativos de los datos relacionados con transacción presentados al usuario; y en el servidor de verificación verificar si los elementos de datos que son indicativos de los datos relacionados con transacción presentados al usuario son coherentes con los datos relacionados con transacción comprendidos en el mensaje de iniciación de autenticación.

Una duodécima clase de realizaciones de los métodos de la presente invención comprende cualquiera de los métodos de la primera a undécima clases en donde la clave de generación del valor de seguridad dinámico comprende una clave personalizada secreta; y en donde el dispositivo de autenticación de usuario calcula el valor de seguridad dinámico combinando criptográficamente la clave de generación de valor de seguridad dinámico con al

menos un valor de entrada dinámico; y en donde dicho valor de entrada dinámico comprende al menos uno de un valor relacionado con el tiempo proporcionado por un mecanismo temporal en el dispositivo de autenticación de usuario, un valor relacionado con el contador almacenado y mantenido por el dispositivo de autenticación de usuario, o un desafío comprendido en el mensaje de iniciación de autenticación.

Una decimotercera clase de realizaciones de los métodos de la presente invención comprende cualquiera de los métodos de la duodécima clase en donde el dispositivo de autenticación de usuario calcula el valor de seguridad dinámico combinando criptográficamente la clave de generación de valor de seguridad dinámico también con un elemento de datos que es indicativo de la representación de identidad de aplicación presentada al usuario.

Una decimocuarta clase de realizaciones de los métodos de la presente invención comprende cualquiera de los métodos de la duodécima clase en donde el dispositivo de autenticación de usuario recupera desde el mensaje de iniciación de autenticación datos relacionados con transacción comprendidos en el mensaje de iniciación de autenticación y presenta estos datos relacionados con transacción al usuario; y en donde el dispositivo de autenticación de usuario calcula el valor de seguridad dinámico combinando criptográficamente la clave de generación de valor de seguridad dinámico también con elementos de datos que son indicativos de los datos relacionados con transacción presentados al usuario.

Aparato según la invención

Una primera clase de realizaciones de dispositivos de la presente invención comprende el aparato para generar credenciales de autenticación que comprende un componente de procesamiento adaptado para procesar datos; un componente de almacenamiento para almacenar datos; un componente de interfaz de usuario que comprende una primera interfaz de salida de usuario para presentar salidas a un usuario y una interfaz de usuario de entrada para recibir entrada desde el usuario; y una interfaz de entrada de datos adaptada para capturar una señal emitida por una segunda interfaz de salida de usuario de un dispositivo de acceso que el usuario está usando para acceder remotamente a una aplicación a través de una red informática, dicha señal codificada con un mensaje de iniciación de autenticación, dicho mensaje de iniciación de autenticación que comprende al menos un identificador de aplicación que corresponde a una identidad de dicha aplicación; mediante el cual el aparato está adaptado para decodificar dicha señal y obtener el mensaje de iniciación de autenticación; recuperar desde el mensaje de iniciación de autenticación el identificador de aplicación; usar el identificador de aplicación para obtener una representación interpretable humana de la identidad de aplicación y presentar la representación de identidad de aplicación obtenida al usuario usando la primera interfaz de salida de usuario; obtener desde el usuario, usando la interfaz de entrada de usuario, una aprobación para generar un mensaje de respuesta y hacer el mensaje de respuesta disponible a un servidor de verificación; generar un valor de seguridad dinámico usando un primer algoritmo criptográfico parametrizado con una clave de generación de valor de seguridad dinámico criptográfico y usar al menos un elemento de datos personalizado que está asociado con el usuario o el aparato, en donde el valor de seguridad dinámico generado está enlazado criptográficamente a la identidad de aplicación presentada al usuario; y generar un mensaje de respuesta que comprende al menos el valor de seguridad dinámico generado.

Una segunda clase de realizaciones de dispositivos de la presente invención comprende cualquiera del aparato de la primera clase de aparatos que están adaptados adicionalmente para presentar el mensaje de respuesta generado al usuario usando la primera interfaz de salida de usuario.

Una tercera clase de realizaciones de dispositivos de la presente invención comprende cualquiera del aparato de la primera clase de aparatos que comprende adicionalmente una interfaz de comunicaciones de datos adaptada para comunicar dicho mensaje de respuesta a un servidor de verificación.

Una realización de un sistema de la presente invención comprende un sistema para asegurar la interacción con una aplicación por un usuario que accede de manera remota a dicha aplicación a través de un dispositivo de acceso que está conectado a un servidor de aplicación que aloja dicha aplicación, que comprende una pluralidad de dispositivos de autenticación de usuario como se ha descrito anteriormente y un servidor de verificación adaptado para recibir un mensaje de respuesta generado por cualquiera de la pluralidad de dispositivos de autenticación de usuario, y adaptado para verificar el mensaje de respuesta recibido que incluye verificar la validez del valor de seguridad dinámico comprendido en el mensaje de respuesta, y adaptado para comunicar el resultado de la verificación del mensaje de respuesta a la aplicación.

Efectos ventajosos

Las ventajas de la invención anteriormente descrita incluyen las siguientes.

Soporte de múltiples aplicaciones verdadero.

Modelo de confianza.

La invención es adecuada para un entorno de múltiples aplicaciones con el siguiente modelo de confianza. Los usuarios confían en un servidor de autenticación confiable para manejar correctamente sus credenciales de autenticación hacia un número de aplicaciones y para basarse en un dispositivo de autenticación de usuario

proporcionado y/o controlado por el dispositivo de autenticación confiable y, hasta cierto punto, para gestionar de manera correcta ciertos datos que se han proporcionado al servidor de autenticación confiable. Las aplicaciones confían en el servidor de autenticación confiable con respecto a la verificación de credenciales de autenticación (es decir los valores de seguridad dinámicos comprendidos en los mensajes de respuesta). No hay necesidad de que las aplicaciones confíen entre sí. Más en particular no tienen que compartir ningún secreto entre sí. Los usuarios confían en una aplicación particular únicamente en el alcance y contexto de esa aplicación particular. Es decir los usuarios no confían en ninguna aplicación para que actúe de manera responsable en nombre del usuario en el alcance y contexto de cualquier otra aplicación y por lo tanto no desean proporcionar aplicaciones con credenciales que podrían usarse para acceder a otras aplicaciones en nombre del usuario.

En algunas realizaciones de la aplicación el valor de seguridad dinámico se enlaza criptográficamente a un identificador de aplicación al que se presenta, revisa por y aprueba por el usuario. Este enlace criptográfico limita de manera eficaz la validez de un mensaje de respuesta generado a una aplicación particular y asegura que las credenciales (mensajes de respuesta) generados para una aplicación no pueden reciclarse para otra aplicación.

Flexibilidad para soportar aplicaciones adicionales

Puesto que el dispositivo de autenticación de usuario no requiere diferentes claves criptográficas o diferentes datos de configuración para diferentes aplicaciones (más en particular no hay necesidad de que los dispositivos de autenticación de usuario almacenen ninguno de los datos específicos de la aplicación tal como, por ejemplo, identidades de representaciones de la aplicación), pueden soportarse fácilmente aplicaciones adicionales. La única cosa que se requiere para que se soporte una aplicación adicional es que esta aplicación adicional establezca una relación de confianza con el servidor de autenticación confiable.

Alta seguridad.

Los dispositivos de autenticación de usuario se han personalizado con claves criptográficas individuales de manera que pueden generar valores de seguridad dinámicos que son específicos para cualquier dispositivo de autenticación de usuario particular y por lo tanto (mediante la asociación conocida entre un dispositivo de autenticación de usuario particular y su usuario asociado) para el usuario legítimo de ese dispositivo de autenticación. Cualquier credencial que se genera por un dispositivo de autenticación de usuario particular se enlaza criptográficamente por lo tanto a ese dispositivo de autenticación de usuario particular (y su usuario asociado).

El uso de una variable dinámica (tal como un desafío o un contador o un valor de tiempo) en los cálculos de los valores de seguridad dinámicos asegura la imprevisibilidad de los valores de seguridad dinámicos generados y protege contra ataques de reproducción.

La presentación de una representación interpretable humana y reconocible de la identidad de aplicación y el enlace criptográfico de la misma con el valor de seguridad dinámico protege contra recogida de credenciales válidos por aplicaciones fraudulentas (p. ej. ataques de suplantación de identidad en tiempo real) para usarlos para obtener acceso a otras aplicaciones.

La presentación de datos de transacción en el dispositivo de autenticación de usuario confiable y la inclusión de los datos de transacción aprobados en el cálculo del valor de seguridad dinámico protege contra ataques MITM (hombre en el medio) mediante los cuales una parte fraudulenta intercepta y modifica datos de transacción que se emiten a una aplicación por un usuario legítimo.

Alta conveniencia para el usuario.

El usuario no tiene que recordar ningún dato de seguridad específico de aplicación tal como contraseñas específicas de aplicación. La invención incluso permite la identificación de usuario automática a la aplicación por el servidor de autenticación de manera que el usuario ya no tiene que recordar sino que tampoco tiene que introducir más ningún nombre de usuario específico de aplicación o id de usuario. La invención también proporciona la comunicación automática a aplicaciones de otros datos que se han proporcionado comúnmente a una amplia gama de aplicaciones (información de contacto, dirección, o número de tarjeta de crédito) evitando de esta manera entrada de datos manual tediosa.

Puesto que la invención puede funcionar con cualquier dispositivo de acceso convencional normal y no requiere que esté presente ningún hardware o software específico en el dispositivo de acceso (es decir un explorador web convencional para interactuar con la aplicación y una interfaz de salida de usuario normal para emitir el mensaje de iniciación de autenticación son suficientes) la invención asegura un muy alto grado de movilidad y autonomía para los usuarios,

Rentabilidad.

Puesto que el mismo dispositivo de autenticación de usuario puede usarse para un número intrínsecamente ilimitado de aplicaciones, la solución de la invención es muy rentable. También, puesto que la solución plantea requisitos muy pequeños al dispositivo de acceso (distintos a los que debería tener una interfaz de salida de usuario normal para

emitir la señal que codifica el mensaje de iniciación de autenticación) no hay problemas de soporte tediosos y costosos normalmente asociados con la instalación en dispositivos de acceso de hardware y/o software específicos (tales como, por ejemplo, lectores de tarjetas inteligentes y sus controladores asociados).

Algunas realizaciones del dispositivo de autenticación de usuario se basan únicamente en criptografía simétrica y no usan criptografía asimétrica. Estas realizaciones tienen la ventaja de que pueden funcionar con criptogramas más cortos y requieren menos potencia de procesamiento que las realizaciones que se basan en criptografía asimétrica.

Se ha descrito un número de implementaciones. Sin embargo, se entenderá que pueden realizarse diversas modificaciones. Por ejemplo, los elementos de una o más implementaciones pueden combinarse, borrarse, modificarse o complementarse para formar implementaciones adicionales. Por consiguiente, otras implementaciones están dentro del alcance de las reivindicaciones adjuntas. Además, aunque una característica particular de la presente invención puede haberse descrito con respecto a únicamente una de varias implementaciones, tal característica puede combinarse con una o más otras características de las otras implementaciones según pueda desearse y sea ventajoso para cualquier aplicación dada o particular. Aunque se han descrito las diversas realizaciones de la presente invención, debería entenderse que se han presentado a modo de ejemplo únicamente y no para limitación. En particular, por supuesto, no es posible describir cualquier combinación concebible de componentes o metodologías para los fines de describir la materia objeto reivindicada, aunque un experto en la técnica puede reconocer que son posibles muchas combinaciones y permutaciones adicionales de la presente invención. Por lo tanto, el ámbito y alcance de la presente invención no debería estar limitado por ninguna de las realizaciones ejemplares anteriormente descritas sino que debería definirse únicamente según las siguientes reivindicaciones y sus equivalentes.

REIVINDICACIONES

1. Un método (400) para asegurar la interacción con una aplicación por un usuario (290) que accede remotamente a dicha aplicación a través de un dispositivo (230) de acceso que está conectado a un servidor (210) de aplicación que aloja dicha aplicación, que comprende las etapas de:

en un dispositivo (240) de autenticación de usuario capturar (435) una señal emitida por el dispositivo de acceso, dicha señal codificada con un mensaje de iniciación de autenticación, comprendiendo dicho mensaje de iniciación de autenticación al menos un identificador de aplicación que corresponde a una identidad de la aplicación;

en el dispositivo (240) de autenticación de usuario decodificar (435) dicha señal y obtener el mensaje de iniciación de autenticación;

en el dispositivo (240) de autenticación de usuario recuperar (440) desde el mensaje de iniciación de autenticación el identificador de aplicación;

en el dispositivo (240) de autenticación de usuario generar (449) un valor de seguridad dinámico usando un primer algoritmo criptográfico parametrizado con una clave de generación de valor de seguridad dinámico criptográfico y usar al menos un elemento de datos personalizado que está asociado con el usuario particular o el dispositivo de autenticación de usuario particular;

en el dispositivo (240) de autenticación de usuario generar (450) un mensaje de respuesta que comprende al menos el valor de seguridad dinámico generado;

el método (400) **caracterizado por que** comprende adicionalmente las etapas de:

en el dispositivo (240) de autenticación de usuario usar el identificador de aplicación recuperado desde el mensaje de iniciación de autenticación para obtener una representación interpretable humana de la identidad de aplicación y presentar (442) la representación de identidad de aplicación obtenida al usuario (290) usando una interfaz (340) de salida de usuario del dispositivo (240) de autenticación de usuario;

en el dispositivo (240) de autenticación de usuario, generar el valor de seguridad dinámico de manera que esté criptográficamente enlazado a la identidad de aplicación presentada al usuario;

en el dispositivo (240) de autenticación de usuario obtener (445) desde el usuario, usando una interfaz (350) de entrada de usuario del dispositivo (240) de autenticación de usuario, una aprobación para generar un mensaje de respuesta y hacer el mensaje de respuesta generado disponible a dicho servidor (220) de verificación;

hacer (460) el mensaje de respuesta generado disponible a dicho servidor (220) de verificación;

en el servidor (220) de verificación recibir el mensaje de respuesta;

verificar (470) el mensaje de respuesta que incluye verificar (475) la validez del valor de seguridad dinámico;

comunicar (480) el resultado de la verificación del mensaje de respuesta a la aplicación.

2. El método de la reivindicación 1, en donde el mensaje de respuesta comprende adicionalmente un elemento de datos que es indicativo de una identidad del usuario o una identidad del dispositivo de autenticación de usuario y en donde dicho elemento de datos indicativo de la identidad de usuario o la identidad de dispositivo de autenticación de usuario se usa para determinar una identidad de usuario y en donde dicha identidad de usuario también se comunica a la aplicación.

3. El método de la reivindicación 2, en donde la identidad de usuario se determina también como una función de la identidad de aplicación.

4. El método de la reivindicación 1, en donde todos los datos dependientes de la aplicación usados para obtener la representación de identidad de aplicación se obtienen por el dispositivo de autenticación de usuario desde una fuente externa al dispositivo de autenticación de usuario o desde el mensaje de iniciación de autenticación.

5. El método de cualquiera de las reivindicaciones anteriores que comprende adicionalmente las etapas de:

generar (422) una credencial de servidor para que esté incluida en el mensaje de iniciación de autenticación, dicha generación usando un segundo algoritmo criptográfico parametrizado con una clave de generación de credencial de servidor criptográfico;

en el dispositivo de autenticación de usuario recuperar desde el mensaje de iniciación de autenticación la credencial de servidor incluida;

en el dispositivo de autenticación de usuario verificar (441) la credencial del servidor usando un tercer algoritmo criptográfico parametrizado con una clave de verificación de credencial de servidor criptográfico.

6. El método de la reivindicación 5, en donde el identificador de aplicación comprendido en el mensaje de iniciación de autenticación está enlazado criptográficamente a la credencial del servidor.

7. El método de cualquiera de las reivindicaciones anteriores, en donde la etapa de generar un mensaje de respuesta comprende adicionalmente:

en el dispositivo de autenticación de usuario incluir en el mensaje de respuesta generado por el dispositivo de autenticación de usuario un elemento de datos indicativo de la representación de identidad de aplicación presentada al usuario.

8. El método de la reivindicación 7, que comprende adicionalmente:

en el servidor de verificación verificar si el elemento de datos que es indicativo de la representación de identidad de aplicación presentada al usuario es coherente con la identidad de aplicación indicada por el identificador de aplicación comprendido en el mensaje de iniciación de autenticación.

9. El método de cualquiera de las reivindicaciones anteriores que comprende adicionalmente las etapas de:

en el dispositivo de autenticación de usuario recuperar desde el mensaje de iniciación de autenticación datos relacionados con transacción comprendidos en el mensaje de iniciación de autenticación;

en el dispositivo de autenticación de usuario presentar (443) los datos relacionados con transacción recuperados usando una interfaz de salida de usuario del dispositivo de autenticación de usuario; y

en donde el valor de seguridad dinámico generado se enlaza criptográficamente a los datos relacionados con transacción.

10. El método de la reivindicación 9, que comprende adicionalmente las etapas de:

generar (422) una credencial de servidor para que esté incluida en el mensaje de iniciación de autenticación, dicha generación usando un segundo algoritmo criptográfico parametrizado con una clave de generación de credencial de servidor criptográfico;

en el dispositivo de autenticación de usuario recuperar desde el mensaje de iniciación de autenticación la credencial de servidor incluida;

en el dispositivo de autenticación de usuario verificar (441) la credencial del servidor usando un tercer algoritmo criptográfico parametrizado con una clave de verificación de credencial de servidor criptográfico;

en donde la credencial del servidor está enlazada criptográficamente a los datos relacionados con transacción.

11. El método de la reivindicación 9 o 10, que comprende adicionalmente las etapas de:

en el dispositivo de autenticación de usuario incluir en el mensaje de respuesta generado por el dispositivo de autenticación de usuario elementos de datos indicativos de los datos relacionados con transacción presentados al usuario; y

en el servidor de verificación verificar si los elementos de datos que son indicativos de los datos relacionados con transacción presentados al usuario son coherentes con los datos relacionados con transacción comprendidos en el mensaje de iniciación de autenticación.

12. El método de cualquiera de las reivindicaciones anteriores en donde

la clave de generación de valor de seguridad dinámico comprende una clave personalizada secreta; y en donde

el dispositivo de autenticación de usuario calcula el valor de seguridad dinámico combinando criptográficamente la clave de generación de valor de seguridad dinámico con al menos un valor de entrada dinámico; y en donde

dicho valor de entrada dinámico comprende al menos uno de un valor relacionado con el tiempo proporcionado por un mecanismo temporal en el dispositivo de autenticación de usuario, un valor relacionado con el contador almacenado y mantenido por el dispositivo de autenticación de usuario, o un desafío comprendido en el mensaje de iniciación de autenticación.

13. El método de la reivindicación 12, en donde el dispositivo de autenticación de usuario calcula el valor de seguridad dinámico combinando criptográficamente la clave de generación de valor de seguridad dinámico también con un elemento de datos que es indicativo de la representación de identidad de aplicación presentada al usuario.

14. Un aparato (240) para generar credenciales de autenticación que comprende:

un componente (310) de procesamiento adaptado para procesar datos;

un componente (320) de almacenamiento para almacenar datos;

un componente de interfaz (340, 350) de usuario que comprende una primera interfaz (340) de salida de usuario para presentar salidas a un usuario y una interfaz (350) de usuario de entrada para recibir entrada desde el usuario; y

una interfaz (360, 370) de entrada de datos adaptada para capturar una señal emitida por una segunda interfaz de salida de usuario de un dispositivo (230) de acceso que el usuario está usando para acceder remotamente a una aplicación a través de una red informática, dicha señal codificada con un mensaje de iniciación de autenticación, comprendiendo dicho mensaje de iniciación de autenticación al menos un identificador de aplicación que corresponde a una identidad de dicha aplicación; mediante la cual el aparato (240) está adaptado para decodificar dicha señal y obtener el mensaje de iniciación de autenticación;

recuperar desde el mensaje de iniciación de autenticación el identificador de aplicación;

generar un valor de seguridad dinámico usando un primer algoritmo criptográfico parametrizado con una clave de generación de valor de seguridad dinámico criptográfico y usar y al menos un elemento de datos personalizado que está asociado con el usuario o el aparato; y

generar un mensaje de respuesta que comprende al menos el valor de seguridad dinámico generado;

el aparato (240) **caracterizado por que** está adaptado adicionalmente para:

usar el identificador de aplicación recuperado desde el mensaje de iniciación de autenticación para obtener una representación interpretable humana de la identidad de aplicación y presentar la representación de identidad de aplicación obtenida al usuario usando la primera interfaz de salida de usuario;

generar el valor de seguridad dinámico de manera que esté criptográficamente enlazado a la identidad de aplicación presentada al usuario; y

obtener desde el usuario, usando la interfaz de entrada de usuario, una aprobación para generar un mensaje de respuesta y hacer el mensaje de respuesta disponible a un servidor de verificación.

15. El aparato (240) de la reivindicación 14, adaptado adicionalmente para presentar el mensaje de respuesta generado al usuario usando la primera interfaz (340) de salida de usuario.

16. El aparato (240) de la reivindicación 14, que comprende adicionalmente una interfaz (330) de comunicaciones de datos adaptada para comunicar dicho mensaje de respuesta a un servidor (220) de verificación.

17. Un sistema (200) para asegurar la interacción con una aplicación por un usuario que accede remotamente a dicha aplicación a través de un dispositivo (230) de acceso que está conectado a un servidor (210) de aplicación que aloja dicha aplicación, que comprende:

una pluralidad de dispositivos (240) de autenticación de usuario según la reivindicación 14; y

un servidor (220) de verificación adaptado para recibir un mensaje de respuesta generado por cualquiera de la pluralidad de dispositivos (240) de autenticación de usuario, y adaptado para verificar el mensaje de respuesta recibido que incluye verificar la validez del valor de seguridad dinámico comprendido en el mensaje de respuesta, y adaptado para comunicar el resultado de la verificación del mensaje de respuesta a la aplicación.

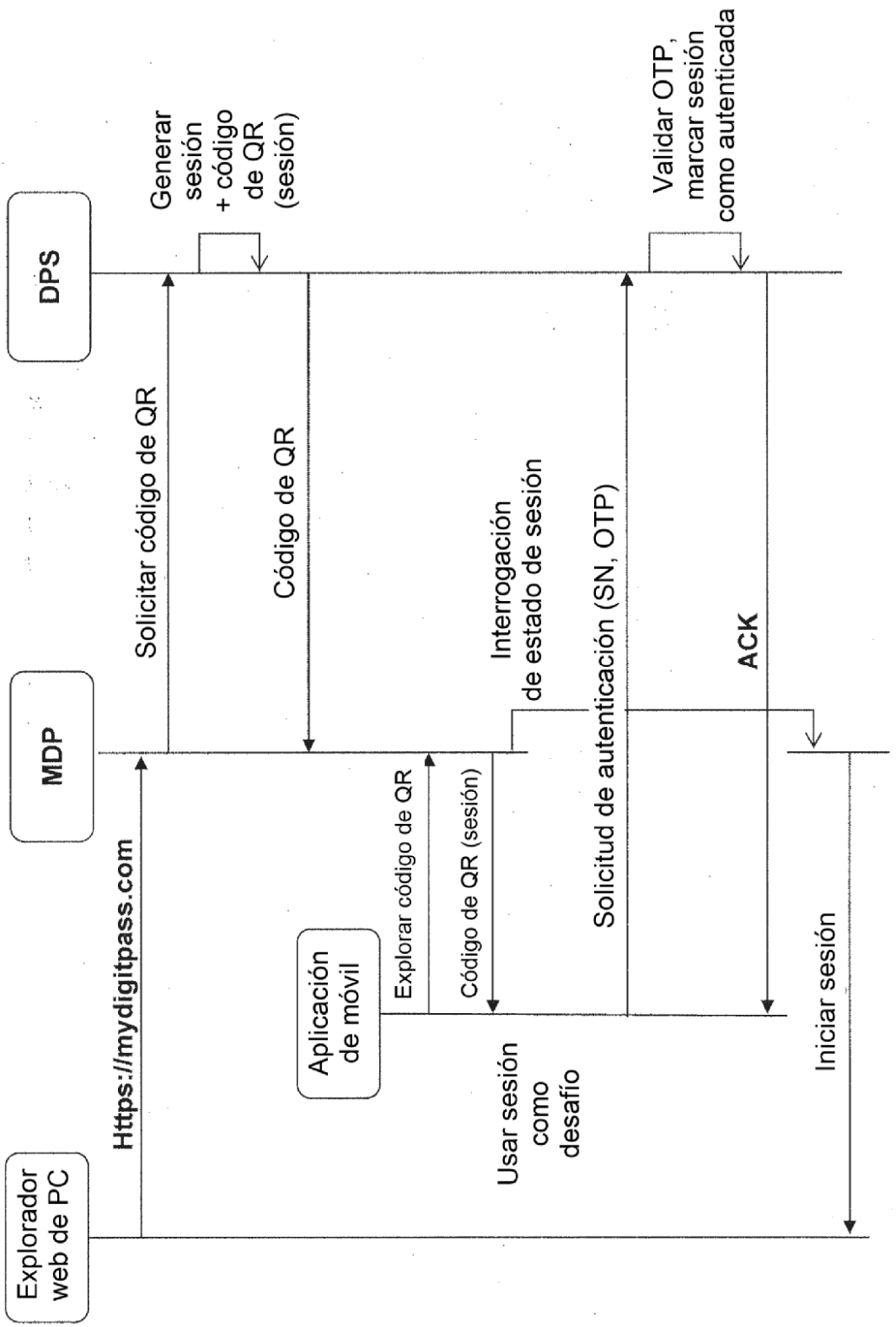
Explorador web de PC
Aplicación de móvil
MDP
DPS
Https://mydigitpass.com
Solicitar código de QR
Generar sesión + código de QR (sesión)
Código de QR
Explorar código de QR
Código de QR (sesión)
Usar sesión como desafío
Interrogación de estado de sesión
Solicitud de autenticación (SN, OTP)
Validar OTP, marcar sesión como autenticada
ACK
Iniciar sesión

Figura 1

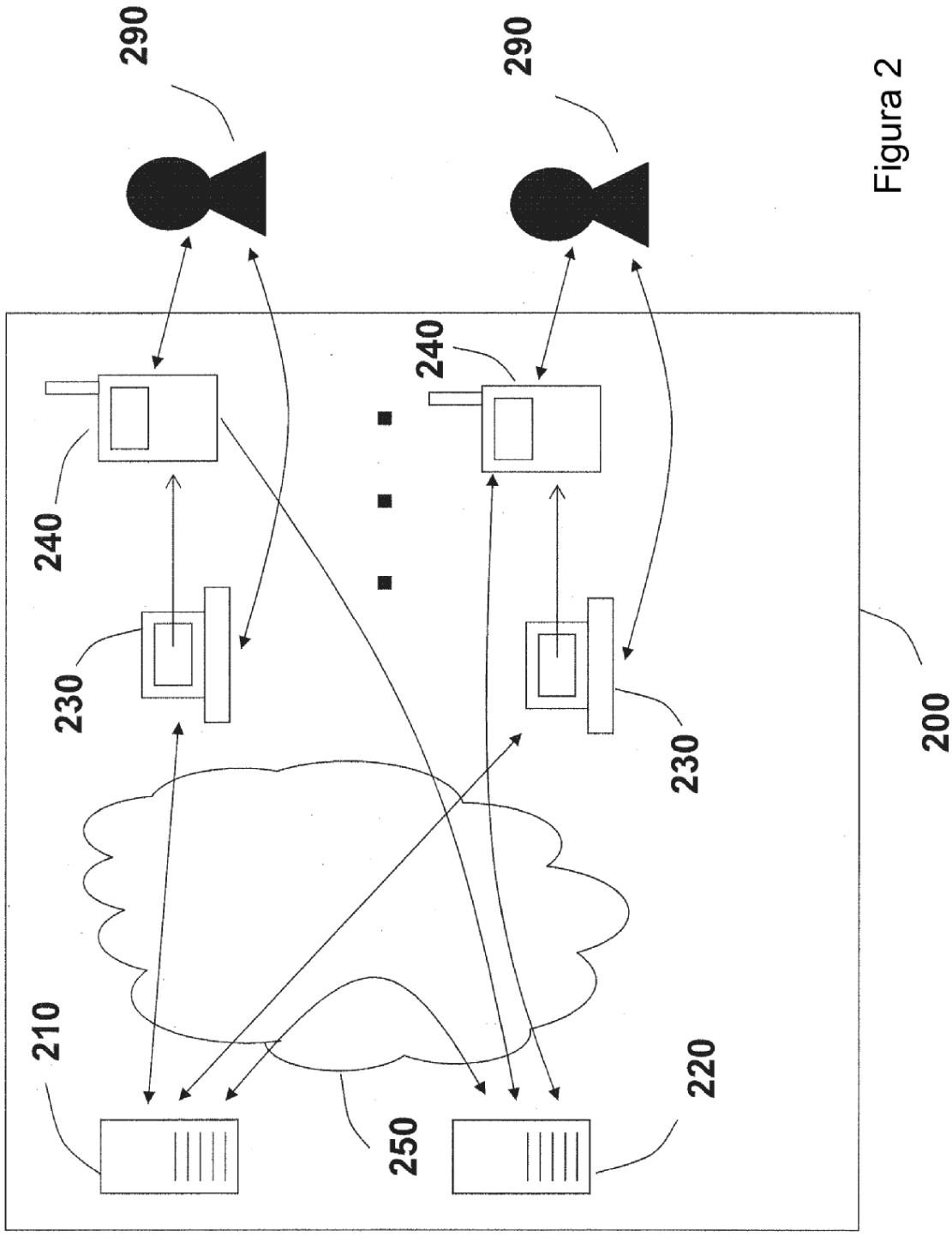

Figura 2

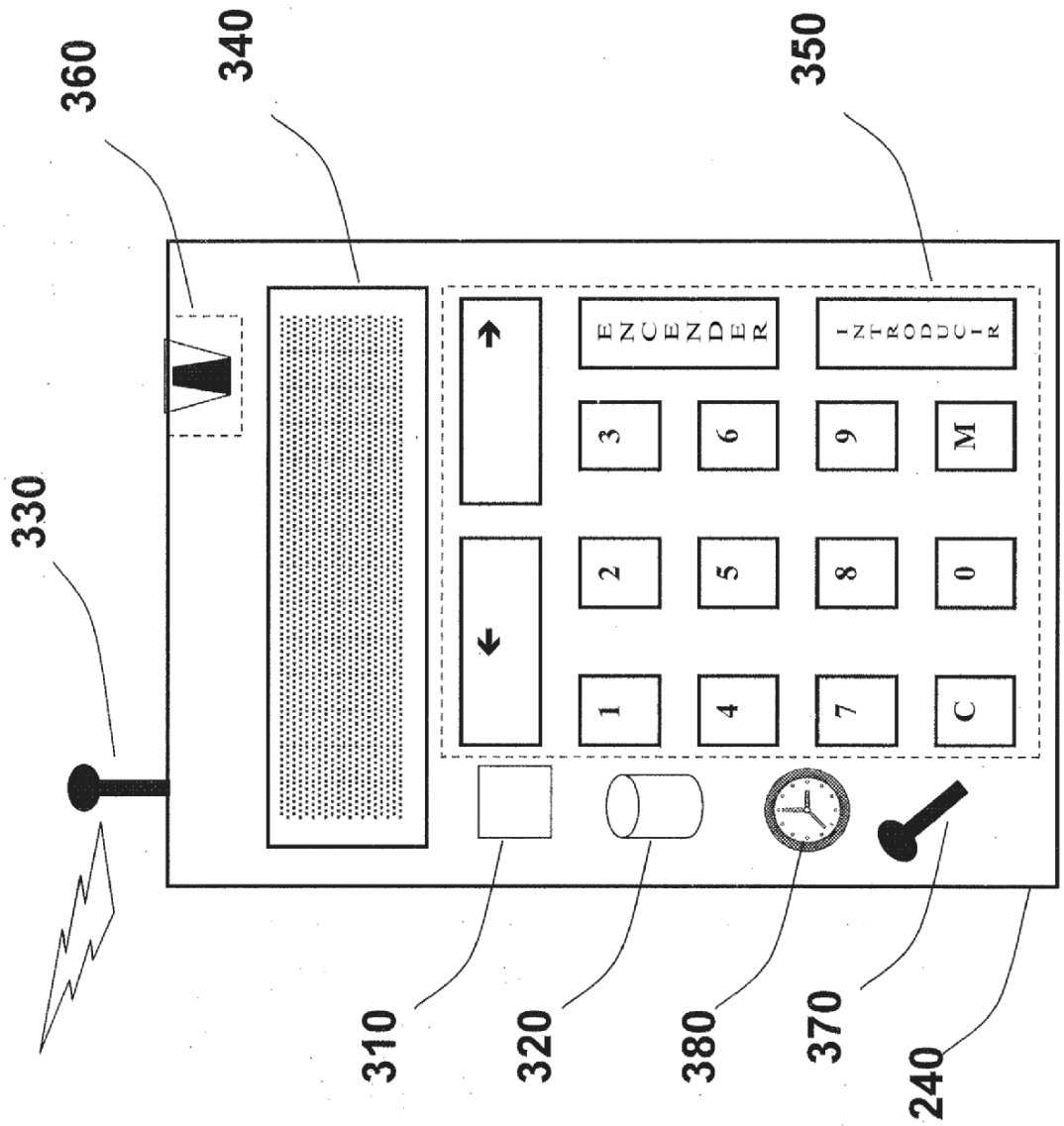
360
340
350
330
ENCENDER
INTRODUCIR
3
6
9
M
2
5
8
0
1
4
7
C
310
320
380
370
240

Figura 3a

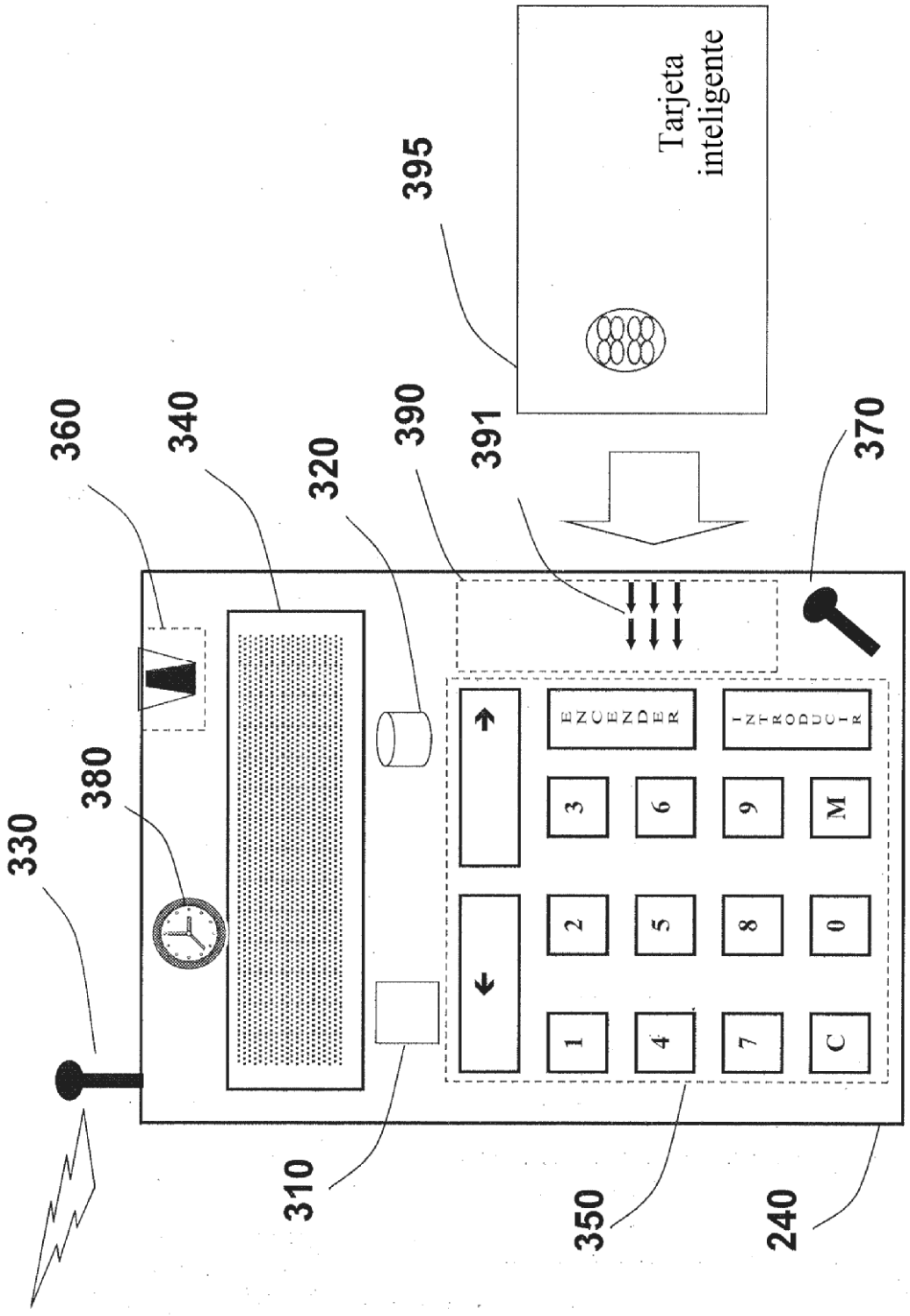
Tarjeta inteligente
395
360
340
320
390
391
370
380
330
310
350
240
ENCENDER
INTRODUCIR
1
2
3
4
5
6
7
8
9
0
C
M

Figura 3b

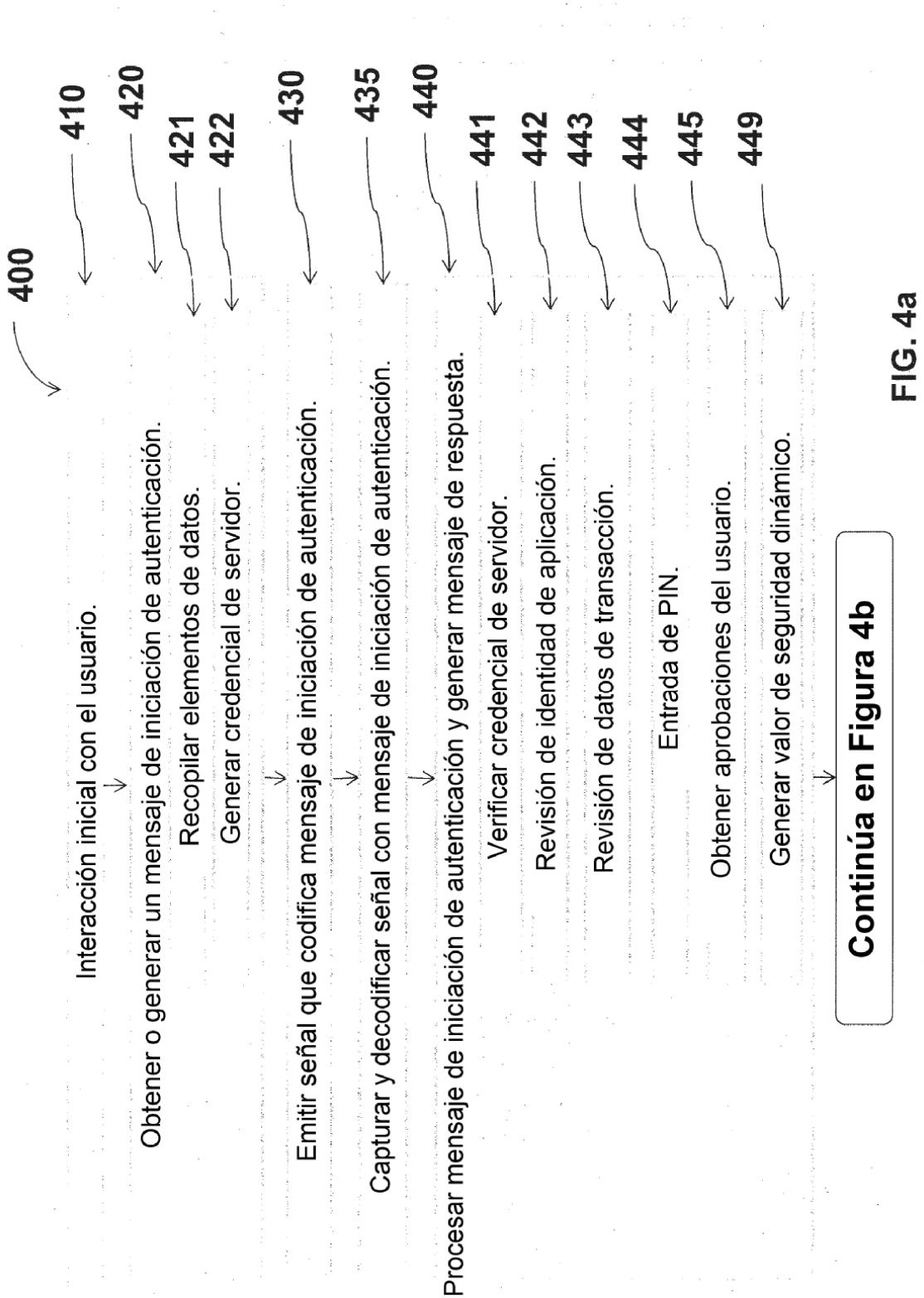
400
410
Interacción inicial con el usuario.
420
Obtener o generar un mensaje de iniciación de autenticación.
421
Recopilar elementos de datos.
422
Generar credencial de servidor.
430
Emitir señal que codifica mensaje de iniciación de autenticación.
435
Capturar y decodificar señal con mensaje de iniciación de autenticación.
440
Procesar mensaje de iniciación de autenticación y generar mensaje de respuesta.
441
Verificar credencial de servidor.
442
Revisión de identidad de aplicación.
443
Revisión de datos de transacción.
444
Entrada de PIN.
445
Obtener aprobaciones del usuario.
449
Generar valor de seguridad dinámico.
Continúa en Figura 4b

FIG. 4a

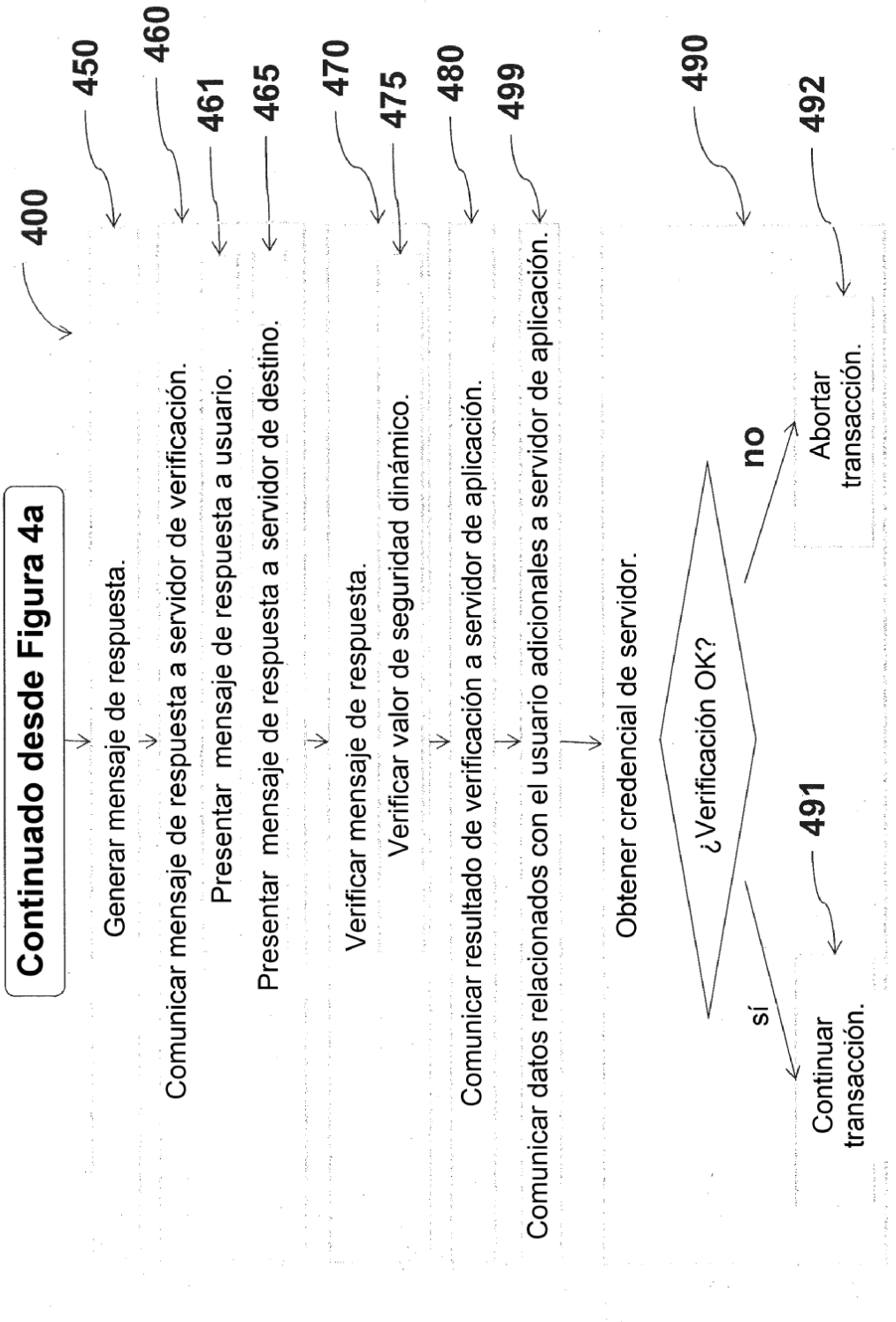
Continuado desde Figura 4a
400
450
Generar mensaje de respuesta.
460
Comunicar mensaje de respuesta a servidor de verificación.
461
Presentar mensaje de respuesta a usuario.
465
Presentar mensaje de respuesta a servidor de destino.
470
Verificar mensaje de respuesta.
475
Verificar valor de seguridad dinámico.
480
Comunicar resultado de verificación a servidor de aplicación.
499
Comunicar datos relacionados con el usuario adicionales a servidor de aplicación.
Obtener credencial de servidor.
490
¿Verificación OK?
no
492
Abortar transacción.
sí
491
Continuar transacción.

FIG. 4b