(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **3 015 091**

(51) Int. CI.:

G06F 3/039 (2013.01)
G06F 21/36 (2013.01)
G06F 3/044 (2006.01)
G06F 21/34 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **04.05.2018 E 18382310 (3)**
(97) Fecha y número de publicación de la concesión europea: **26.02.2025 EP 3564837**

(54) Título: **Sistema, método y programas informáticos para la autenticación y/o autorización de usuario**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.04.2025

(73) Titular/es:

TELEFÓNICA CYBERSECURITY & CLOUD TECH, S.L.U. (100.00%)
Ronda de la Comunicación S/N
28050 Madrid, ES

(72) Inventor/es:

TORRES VELASCO, JOSÉ;
BIANZINO, ARUNA PREM;
NÚÑEZ-ROMERO CASADO, ÁLVARO y
DE LOS SANTOS VILCHEZ, SERGIO

DESCRIPCIÓN

Sistema, método y programas informáticos para la autenticación y/o autorización de usuario

Campo de la invención

La presente invención se refiere a sistemas y métodos de autenticación y/o autorización de usuario. En particular, la presente invención propone una tarjeta pasiva con puntos capacitivos en su superficie y un dispositivo informático portátil para usarse en soluciones de autenticación y/o autorización.

Antecedentes de la invención

Los usuarios acceden constantemente a servicios y recursos desde dispositivos informáticos móviles y portátiles. La autenticación de los usuarios que acceden es de vital importancia para proteger el acceso a los propios servicios, recursos y datos sensibles, y para limitar el mismo a solo los usuarios autorizados.

La necesidad de identificar a usuarios que consumen diferentes tipos de servicios está relacionada estrechamente con la prevención del robo de identidad, pero también debe considerarse la seguridad de la privacidad. Por lo tanto, es de un interés extremo determinar si los usuarios son quienes afirman ser, pero es igual de importante mantener la confidencialidad acerca de la información intercambiada en tal proceso.

El proceso de identificación de usuario se basa habitualmente en algunas credenciales, cuya titularidad y verificación garantizan comprobar la identidad de usuario. Las credenciales usadas son emitidas habitualmente por una autoridad de confianza y son teóricamente imposibles (o al menos extremadamente difíciles) de falsificar, lo que permite determinar si los usuarios se corresponden, o no, con quienes afirman ser.

El proceso de identificación de usuario se construye sobre los así denominados mecanismos de validación o autenticación. Estos mecanismos se diseñan para validar cierta información que el usuario aporta para acceder a los servicios (digitales) solicitados. La información portada (que el usuario proporciona al mecanismo de autenticación para su validación) pertenece habitualmente a una de las siguientes categorías: algo que el usuario sabe (por ejemplo, una palabra clave secreta), algo que el usuario posee (por ejemplo, un objeto físico también denominado testigo físico, como una tarjeta inteligente, una tarjeta de SIM, una etiqueta de NFC...), algo que el propietario es (por ejemplo, cualquier característica física medible, que identifica unívocamente al usuario, como huellas dactilares o identificación de iris), algo que el usuario hace (por ejemplo, patrones de movimiento, firma, etc.), o algún lugar en el que el usuario está (por ejemplo, estar en una ubicación específica). Esta información es lo que se conoce como identificador o credencial digital. A veces se usa una combinación de información perteneciente a categorías diferentes de estas, para mejorar la seguridad.

La eficacia de cualquier solución de autenticación no puede medirse solo en términos de seguridad - debido a que muchas de las mismas son equivalentes en ese aspecto - sino más bien dando cuenta también de la utilizabilidad, la facilidad de implementación y el coste y consumo de energía. Solo teniendo en cuenta todos estos aspectos al mismo tiempo es posible conseguir una adopción generalizada de la solución de autenticación por los usuarios.

Uno de los defectos principales de las soluciones de autenticación actuales se representa por el hecho de que las credenciales de usuario (contraseña, testigo o huella dactilar de evento, etc.) son objeto de copia, husmeo por encima del hombro o robo por parte de observadores externos malintencionados, que pueden acceder entonces al servicio/activo objetivo falsificando su identidad como la de un usuario autorizado.

Tam Vu y col., "*Capacitive Touch Communication: A Technique to Input Data through Devices' Touchscreen*", describe un método para identificar y autenticar usuarios en dispositivos de pantalla táctil, basándose en artefactos ponibles que generan activamente una entrada, que será detectada por la pantalla capacitiva y se descodificará como una secuencia binaria. La solución descrita usa un dispositivo - anillo, reloj, etc. - activo como un transmisor continuo de baja potencia, para proporcionar a los usuarios autenticación (continua). Por el contrario, la presente invención usa un dispositivo (tarjeta) pasivo para autenticar al usuario final.

Mohamed Azard Rilvan y col., "*User authentication and identification on smartphones by incorporating capacitive touchscreen*", aprovecha una instantánea tomada por una pantalla capacitiva, de cuatro dedos o una oreja o un pulgar y la usa como clave para una autenticación de un solo uso para acceder a servicios o recursos específicos en el propio dispositivo. La solución descrita se basa en mediciones de características del cuerpo humano, no fiables al 100 % por naturaleza (y por afirmación de los autores). Además, la solución descrita no permite una división en múltiples sectores del área legible para proporcionar autenticación de múltiples servicios y/o solicitud aleatoria de un sector específico para la autenticación, y/o codificación de otros datos y metadatos.

El documento de Sun, Jingchao, y col., "*Touchin: Sightless two-factor authentication on multi-touch mobile devices*"

describe una solución para identificar usuarios en dispositivos móviles en función de un gesto ejecutado en la interfaz táctil del propio dispositivo móvil. La detección de gestos es independiente de la zona de pantalla en la que se ejecuta esta, lo que impide ataques por análisis de suciedad y hace más difícil el husmeo por encima del hombro. La solución descrita se basa en un factor de autenticación (es decir, el gesto de toque) que no puede traducirse de forma natural en una clave de cifrado, ni dividirse en diferentes sectores/áreas para implementar ni una autenticación multifuncional ni una autenticación basándose en una selección de sectores aleatoria. Además, la solución descrita presenta un conjunto no nulo de elementos visibles, es decir, la firma, que está sujeta por naturaleza a husmeo por encima del hombro.

El documento US 9.652.066 describe un método para la lectura de huellas dactilares a lo largo de toda una pantalla capacitiva, también posible mientras se realizan otras acciones (toque, etc.). La lectura de huellas dactilares se usa entonces como factor de autenticación para el usuario, a la larga, de forma continua. La solución requiere hardware específico en el dispositivo de extremo (es decir, una capa de detección biométrica dactilar). Además, la solución descrita se basa en mediciones de características del cuerpo humano. En este sentido, la solución no es fiable al 100 % por naturaleza y no permite una división en múltiples sectores del área legible para proporcionar autenticación de múltiples servicios y/o solicitud aleatoria de un sector específico para la autenticación.

El documento EP-A1-2527955 se basa en la detección de objetos específicos por dispositivos móviles, mediante detección óptica o capacitiva, para activar un estado predeterminado del dispositivo (por ejemplo, en espera). A la larga, este puede usarse también para fines de autenticación, como se indica en la patente. La identificación de objetos propuesta en esta solicitud de patente tiene por objeto asociar un objeto común a un estado deseado (por ejemplo, cargador con en espera), pero no diferenciar múltiples instancias del mismo objeto, ni codificar un código singular específico en el objeto con fines de autenticación y/o cifrado.

El documento WO-A1-2017143193 describe un método para identificar y autenticar usuarios en dispositivos de pantalla táctil, basándose en artefactos ponibles que generan activamente una entrada, que será detectada por la pantalla capacitiva y se descodificará como una secuencia binaria. Esta solución se refiere a la descrita también en el artículo de Tam Vu y col., "*Capacitive Touch Communication: A Technique to Input Data through Devices' Touchscreen*". El método usa un dispositivo - anillo, reloj, etc. - activo como un transmisor continuo de baja potencia, para proporcionar a los usuarios autenticación (continua). Por el contrario, la presente invención usa un dispositivo (tarjeta) pasivo para autenticar al usuario final.

El documento US-A1-2016004407 se refiere a un sistema de autenticación de usuario basándose en una tarjeta con un toque de superficie multitáctil. También se ha divulgado una superficie capacitiva multitáctil que identifica el objeto y autentica al usuario en función de un movimiento ejecutado por el usuario usando la tarjeta.
El sistema descrito tiene por objeto la autenticación de un conjunto de usuario que portan diferentes instancias de la misma tarjeta de autenticación. La solución descrita puede incluir un movimiento que el usuario debe ejecutar con la tarjeta sobre la superficie capacitiva, introduciendo restricciones limitantes sobre el tamaño de pantalla. De hecho, la solución descrita se diseña para la autenticación en pantallas capacitivas fijas más que en dispositivos móviles con una superficie capacitiva limitada, aunque también se describe una solución variante en el caso de uso de la superficie capacitiva de un teléfono móvil. Por último, no se da ninguna posibilidad de implementar una autenticación de múltiples servicios, ni una autenticación de múltiples sectores seleccionando un sector/área aleatorio en diferentes instancias de autenticación. Además, en esta solicitud de patente no se incluye ninguna posibilidad de usar el patrón de contacto como una parte de un código de cifrado.

El documento KR-A-2016036133A divulga un sistema de autenticación de usuario y autorización de operaciones basándose en un sello de caucho que se aplica sobre una pantalla capacitiva de un dispositivo móvil y presenta un patrón capacitivo específico, permitiendo que el usuario se autentique para un servicio y/o autorice operaciones específicas. Esta solución no descodifica la secuencia de puntos capacitivos para dar un código, como tal, ni incluye el dispositivo en el proceso de autenticación y autorización. En la presente invención, además, el código descodificado a partir de la serie de puntos capacitivos se concatena con un código en el dispositivo para formar una clave singular, que se usa con fines de autenticación y autorización, pero también puede usarse para cifrar la comunicación con el servidor de servicios. Por último, esta solución no incluye múltiples zonas capacitivas para usarse con fines de aleatorización o para autenticar y autorizar diferentes servicios y operaciones.

El documento WO-A1-2017024011 divulga un método que comprende recibir una indicación para iniciar una aplicación en un dispositivo móvil, mostrar una interfaz de usuario, por la aplicación, una solicitud para una captura de un patrón en un artículo, recibir, por la aplicación, una capturar patrones del artículo, determinar si la captura de patrones está completa y enviar la captura de patrones a un primer sistema remoto para autenticar una transacción. Las realizaciones divulgadas también incluyen una tarjeta que comprende una primera información visible sobre una cuenta asociada con la tarjeta, un elemento legible por máquina que comprende una segunda información (que puede tener información en común con la primera información) y un patrón que comprende al menos una marca que incluye al menos una de tinta invisible o tinta capacitiva, que no incluye la primera información o la segunda información.

El documento US-A1-2016004407 divulga un sistema para la autenticación de usuarios, particularmente adecuado para la autenticación de grupos de usuarios en entornos hospitalarios. El sistema comprende un objeto de autenticación provisto de un patrón geométrico redefinido para autenticar al usuario. El sistema comprende además una superficie multitáctil provista de una capa primaria y una capa secundaria. La superficie multitáctil está configurada para generar, en respuesta al patrón geométrico predefinido que se pone en contacto con la capa primaria, un patrón correspondiente de interacción eléctrica entre las capas primaria y secundaria, lo que permite una autenticación singular basada en dicho patrón de interacción eléctrica.

El documento WO-A1-2009009788 desvela que los testigos de seguridad contienen datos que están cada uno cifrados de manera singular basándose en un identificador biométrico singular de un usuario autorizado de ese testigo. Los descodificadores reciben el testigo y el identificador biométrico del usuario, convierten el identificador biométrico en una clave biométrica y aplican la clave biométrica para desencriptar el testigo. De esta manera, los descodificadores autentican a los usuarios sin realizar una comparación de identificador biométrico. En algunas realizaciones, las piezas o conjuntos de los datos se almacenan en compartimentos de datos designados, que se cifran individualmente basándose en claves de autoridad, y todos los compartimentos de datos cifrados se cifran colectivamente basándose en la clave biométrica para crear el testigo. Los descodificadores almacenan únicamente las claves de autoridad correspondientes a los compartimentos de datos que tienen autorización para abrir. Además, en algunas realizaciones, el testigo y el identificador biométrico se cifran y se envían a un servidor de autenticación remoto para el descifrado del testigo.

Las soluciones conocidas siguen careciendo de una fiabilidad, una disponibilidad y una facilidad de uso altas. Por lo tanto, se necesitan más soluciones para autenticación y/o autorización de usuario.

Descripción de la invención

Realizaciones de la presente invención proporcionan de acuerdo con un primer aspecto un sistema para autenticación y/o autorización de usuario, que comprende una tarjeta pasiva para almacenar una primera porción de un código de autenticación o autorización a través de un conjunto de puntos capacitivos incluidos en su superficie; y un dispositivo informático portátil que tiene una pantalla capacitiva y está configurado para almacenar una segunda porción de dicho código de autenticación o autorización.

En el sistema propuesto, una vez que el usuario ha solicitado acceso a un servicio específico o a una operación específica y cuando la tarjeta pasiva está en contacto con la pantalla capacitiva, el dispositivo informático portátil está configurado para leer al menos parte del conjunto de puntos capacitivos, descodificando la primera porción del código de autenticación o autorización, y para firmar criptográficamente la primera porción descodificada usando dicha segunda porción almacenada del código de autenticación o autorización, proporcionando el código de autenticación o autorización, que se usa como clave criptográfica para conceder acceso a dicho servicio específico solicitado u operación específica solicitada al usuario. Por lo tanto, el sistema propuesto representa una solución de autorización y/o autenticación altamente fiable, al tiempo que es utilizable, fácil de implementar, sencilla, barata y con un consumo de energía mínimo.

Preferiblemente, el conjunto de puntos capacitivos es invisible a la inspección humana.

De acuerdo con el sistema propuesto, algunos de los puntos capacitivos pueden incluir información acerca del usuario o metadatos acerca del distribuidor de tarjetas. La información o los metadatos se codifican preferiblemente con un sistema de codificación diferente del sistema de codificación usado para codificar la primera porción del código de autenticación o autorización. El conjunto de puntos capacitivos incluye al menos dos puntos capacitivos ubicados en partes predefinidas de la tarjeta pasiva.

En una realización, la superficie de la tarjeta pasiva se divide en diferentes áreas/sectores lógicos, comprendiendo cada área/sector un conjunto de puntos capacitivos que codifican una primera porción diferente del código de autenticación o autorización de tal modo que cada primera porción diferente puede usarse para autenticar un servicio diferente o para autorizar una operación diferente.

El dispositivo informático portátil puede incluir un teléfono móvil, un ordenador portátil o una tableta, entre otros. En una realización, la segunda porción del código de autenticación o autorización se almacena en un módulo de identificación de abonado (SIM) del dispositivo informático portátil. Como alternativa, en otra realización, la segunda porción se almacena en una memoria del dispositivo informático portátil con acceso restringido.

Las realizaciones de la presente invención también proporcionan, de acuerdo con un segundo aspecto, un método de autenticación y/o autorización de usuario. El método comprende almacenar una primera porción de un código de autenticación o autorización a través de un conjunto de puntos capacitivos incluido en una superficie de una tarjeta pasiva; almacenar una segunda porción del código de autenticación o autorización, en un dispositivo informático portátil que tiene una pantalla capacitiva; una vez que el usuario ha solicitado acceso a un servicio específico o a una

operación específica y cuando la tarjeta pasiva está en contacto con la pantalla capacitiva, leer, por el dispositivo informático portátil, al menos algunos del conjunto de puntos capacitivos, descodificar la primera porción del código de autenticación o autorización; y firmar criptográficamente, por el dispositivo informático portátil, la primera porción descodificada usando la segunda porción almacenada del código de autenticación o autorización, proporcionando el código de autenticación o autorización, que se usa como clave criptográfica para conceder acceso a dicho servicio específico o dicha operación específica al usuario.

De acuerdo con la invención propuesta, la primera porción del código de autenticación o autorización depende de la forma, el tamaño y/o la posición del conjunto de puntos capacitivos sobre la tarjeta pasiva.

En una realización, la lectura se realiza mientras la tarjeta pasiva está en contacto con la pantalla capacitiva en una posición específica, por ejemplo, una posición horizontal o una posición vertical de la tarjeta pasiva. Como alternativa, la lectura se realiza mientras la tarjeta pasiva ha experimentado un movimiento específico, por ejemplo, una rotación o un deslizamiento de la tarjeta pasiva. La posición específica o el movimiento específico pueden ser característicos de un servicio u operación particular solicitado por el usuario.

En otra realización más, el almacenamiento de la segunda porción del código de autenticación o autorización en el dispositivo informático portátil se realiza después de darse la tarjeta pasiva al usuario. En este caso, la segunda porción puede almacenarse en el SIM del dispositivo informático portátil o en una memoria del mismo con acceso restringido. En caso de pérdida o robo de la tarjeta pasiva, esta última puede bloquearse (temporal o permanentemente) o puede reemplazarse a través de un canal seguro.

Otras realizaciones de la invención que se desvelan en el presente documento incluyen programas de software para realizar las etapas de realización del método y operaciones anteriormente resumidas y desveladas en detalle a continuación. Más particularmente, un producto de programa informático es una realización que tiene un medio legible por ordenador que incluye instrucciones de programa informático codificadas en el mismo que cuando se ejecutan en al menos un procesador en un sistema informático provoca que el procesador realice las operaciones indicadas en el presente documento como realizaciones de la invención.

La presente invención presenta las siguientes ventajas singulares:

- No requiere un hardware específico para funcionar, sino que se basa en hardware disponible en cualquier dispositivo informático portátil actual (es decir, un área de entrada capacitiva).
- No requiere precisión por parte del usuario en términos de gesto ejecutado, ya que la tarjeta pasiva presenta puntos de referencia para el lector, haciendo que el proceso sea más fácil de usar.
- Garantiza, de hecho, un factor doble de autenticación, debido a que el sistema está compuesto por dos componentes singulares, es decir, la tarjeta pasiva y el dispositivo informático portátil, cada uno de los cuales solo puede funcionar en correspondencia con el otro correspondiente.
- No requiere un dispositivo activo, sino solo una tarjeta pasiva del tamaño de una "tarjeta de crédito" común, fácil de portar y barata de producir. Además, el sistema es robusto frente a daño parcial de la tarjeta, gracias a la división de superficie multisector.
- Es robusto frente a ataques, debido a que el código no es visible sobre la tarjeta (husmeo por encima del hombro, copia, fotografías distantes), se necesita un contacto físico para leer (y, a la larga, copiar la tarjeta) - a diferencia de NFC, la clave de autenticación se almacena parcialmente en la tarjeta pasiva y se almacena parcialmente en el dispositivo informático, haciendo que sea ineficaz usar la tarjeta en un dispositivo informático diferente (robo), la clave se codifica en una porción específica de la tarjeta, desconocida para el atacante, y el proceso de autenticación puede basarse cada vez en un código diferente, impredecible y generado aleatoriamente (virus troyanos, ataques de piratas informáticos o servicios de suplantación de identidad). Por lo tanto, es resistente a ataques de fuerza bruta al menos en 1/n de las veces, siendo "n" el número de códigos posibles.
- Es fácil y rápido de usar, debido a que el usuario solo tiene que colocar la tarjeta en la superficie capacitiva del dispositivo informático, sin requerir centrado de tarjeta o una colocación de tarjeta específica.
- Puede usarse para autenticar para diferentes servicios o para autorizar una clase diferente de operaciones, gracias a la división de superficie en múltiples sectores.
- Puede usarse no solo como un testigo para identificación y autenticación, sino que una porción específica de los puntos capacitivos puede usarse para codificar información acerca del usuario (como un OpenID), o metadatos acerca del sistema y el distribuidor de tarjetas, entre otras posibilidades. Esta información se codificará usando un sistema de codificación - abierto - diferente para que su descodificación esté disponible para cualquier uso.

Breve descripción de los dibujos

Las ventajas y características previas, así como otras, se entenderán más completamente a partir de la siguiente descripción detallada de realizaciones, con referencia a los dibujos adjuntos, que deben considerarse de una forma ilustrativa y no limitante, en los que:

La figura 1 ilustra un ejemplo de los puntos capacitivos incluidos en la tarjeta pasiva y una división en áreas/sectores posible.

La figura 2 es un diagrama de flujo de un proceso de autenticación de ejemplo.

Descripción detallada de realizaciones preferidas

La presente invención propone un sistema y método de autenticación y/o autorización de usuario. La solución propuesta aprovecha la presencia de un área de entrada capacitiva en dispositivos informáticos portátiles 20 como un lector de una tarjeta pasiva 10 especial que incluye sobre su superficie un conjunto de puntos capacitivos 11 (véase la figura 1). Los puntos capacitivos 11 dan como resultado una presión sobre el área capacitiva, generando una entrada específica y singular.

Los puntos capacitivos 11 son fáciles y baratos de implementar en una tarjeta de plástico común (un dispositivo pasivo), al tiempo que son invisibles a la inspección humana, haciendo que la solución sea robusta frente a husmeo por encima del hombro, fotografías distantes o escaneado, y la superficie de la tarjeta se mantiene disponible para cualquier impresión (marca, publicidad, etc.). Por otro lado, la lectura de tarjeta se ejecuta mediante una superficie capacitiva que está presente actualmente en cualquier dispositivo informático portátil 20 (por ejemplo, teléfono inteligente, tableta, portátil, etc. que tenga una pantalla táctil o panel táctil), no requiriendo ningún hardware adicional o específico, a diferencia de otras soluciones basándose en tecnología de NFC o lectura de huellas dactilares.

La tarjeta puede incluir un par de (o más) puntos capacitivos específicos ubicados en puntos preestablecidos de la tarjeta, por ejemplo, situados en dos esquinas opuestas, en tres esquinas diferentes como en los códigos OR en el caso de incluir tres puntos capacitivos, etc., para hacer sencilla la eliminación de cualquier desplazamiento de medición de la lectura de entrada y hacer más sencilla la lectura de tarjeta (es decir, no tener que centrar la misma con respecto a ninguna marca, ni colocar la misma en una posición específica). En caso de que la tarjeta solo incluya dos puntos capacitivos, estos tendrán una forma no simétrica y serán singulares en el patrón.

Preferiblemente, el tamaño, la forma o la posición de los puntos capacitivos 11, o una combinación de al menos dos de estas características (dependiendo de la calidad o cantidad de la información que se va a codificar) se usa para codificar una secuencia singular (o primera porción de un código de autenticación o autorización). El número de secuencias posibles es lo bastante alto como para garantizar la singularidad entre diferentes tarjetas creadas. Entonces, la secuencia singular se firma criptográficamente usando como una clave otra secuencia singular (o segunda porción del código de autenticación o autorización) almacenada en el dispositivo informático portátil 20 y obtenida preferiblemente en el momento de la instalación de una aplicación de software específica que se usará para realizar la lectura de la tarjeta pasiva 10, representando un emparejamiento singular con la secuencia singular (o primera porción) codificada en la tarjeta pasiva 10. La secuencia obtenida a partir de la concatenación representa el código de autenticación o autorización que puede usarse como una clave criptográfica para acceder al servicio requerido y/o autorizar la operación requerida. La porción del código almacenada en el dispositivo informático portátil 20 puede ubicarse en la tarjeta de SIM o en otras porciones de memoria con acceso restringido, como los elementos de seguridad (SE) que tienen algunos teléfonos inteligentes.

La presencia de dos porciones de código diferentes (primera porción y segunda porción o porción de código de tarjeta y porción de código de dispositivo, como también puede denominarse), ubicadas en dos dispositivos físicos diferentes (es decir, el dispositivo informático portátil 20 y la tarjeta pasiva 10) hacen que el sistema sea robusto frente a robo, debido a que el robo de solamente uno de los dos elementos no permite ningún acceso/autorización, mientras que la ausencia de los dispositivos se percibirá fácilmente, y los dispositivos de acceso pueden ser bloqueados de forma remota por el propio usuario a través de un procedimiento de software apropiado.

Como puede verse en la realización de la figura 1, la superficie de la tarjeta pasiva 10 puede dividirse en diferentes áreas lógicas o sectores 12, comprendiendo cada uno un conjunto de puntos capacitivos que codifican una secuencia singular (o una primera porción diferente de un código de autenticación o autorización).

La presencia de diferentes áreas 12 en la tarjeta pasiva 10, correspondientes a diferentes secuencias codificadas, permiten las siguientes funcionalidades adicionales para el sistema:

- Usar diferentes áreas 12 para acceder a diferentes servicios (por ejemplo, un banco n.º 1, un banco n.º 2, otro servicio, etc.) o para autorizar una clase diferente de operaciones.
- Garantizar la redundancia en caso de daño parcial de la tarjeta pasiva 10.
- Permitir requerir el código correspondiente a un sector (o secuencia de sectores) aleatorio para diferentes instancias de la autenticación a un mismo servicio o de la autorización de una operación. Esto es funcionalmente equivalente a las tarjetas de código actuales distribuidas a clientes de bancos para el acceso a banca electrónica. Esto da como resultado coordenadas de acceso impredecibles, designadas aleatoriamente y, por lo tanto, impide un robo de código a través de sitios web falsos, virus troyanos o ataques de piratas informáticos, haciendo que la

transacción sea segura. Esto permite no solo autenticar sino autorizar, únicamente en la misma tarjeta.

La posición de la tarjeta pasiva 10 con respecto a la superficie de lectura (por ejemplo, horizontal/vertical, etc.) o un movimiento específico que hay que ejecutar con la tarjeta pasiva 10 sobre la superficie de lectura (por ejemplo, rotación, deslizamiento, etc.) puede usarse, o no, como un elemento de autenticación adicional para el sistema, basándose en algo que el usuario sabe. Por ejemplo, el sistema puede configurarse de una forma tal que una posición horizontal de la tarjeta pasiva 10 sobre la superficie de lectura es para acceder a un servicio dado, mientras que un deslizamiento de la tarjeta pasiva 10 sobre la superficie de lectura es para acceder a otro servicio dado diferente.

Con referencia a continuación a la figura 2, en la misma se ilustra una realización de un método de autenticación y/o autorización de usuario que usa el sistema propuesto. En primer lugar, se produce la tarjeta pasiva 10, codificando un código específico (la primera porción del código de autenticación o autorización) a través de la secuencia de puntos capacitivos 11 impresos sobre su superficie. Entonces, se le da al usuario 1 la tarjeta pasiva 10, y un código secreto específico (la segunda porción del código de autenticación o autorización), asociado con la tarjeta pasiva 10 como un par singular, se almacena en un área de memoria de confianza en su dispositivo informático portátil 20 (en este caso particular, un teléfono inteligente), preferiblemente cuando se instala la aplicación de software para realizar la lectura de la tarjeta pasiva 10.

El usuario 1 se conecta de forma remota a un servidor 30 que requiere acceso a un servicio específico (por ejemplo, banca electrónica, acceso a información restringida, etc.) o autorizar una operación específica (por ejemplo, transferencia de dinero, publicación de contenido, etc.). Este acceso puede ejecutarse o bien en el dispositivo informático portátil 20 o bien en cualquier otro dispositivo informático, incluyendo dispositivos fijos tales como un PC.

El servidor 30 requiere una autenticación de usuario específica para proceder con la operación requerida. El servidor 30 puede incluir en esta solicitud la identificación de un área de tarjeta 12 o secuencia de áreas de tarjeta específica, dependiendo de la implementación.

Si el usuario 1 está accediendo al servicio desde un dispositivo informático diferente del dispositivo informático portátil 20, el dispositivo informático empleado se conecta al dispositivo informático portátil 20 usando una conexión segura y le requiere que proceda con el procedimiento de autorización. De lo contrario, el dispositivo informático portátil 20 procede directamente con el procedimiento de autenticación. El usuario 1 ubica la tarjeta pasiva 10 sobre la superficie capacitiva del dispositivo informático portátil 20, a la larga en una posición específica o con un movimiento específico; dependiendo de la implementación. La entrada de tarjeta (secuencia de puntos capacitivos en su superficie) es leída por el dispositivo informático portátil 20. Toda la superficie o una(s) área(s) específica(s) (o una secuencia específica de las mismas) es descodificada por la aplicación de software instalada en el dispositivo informático portátil 20. El código resultante se firma criptográficamente entonces usando como una clave el código singular (segunda porción del código de autenticación o autorización) almacenado en el dispositivo informático portátil 20 para obtener una clave criptográfica para ser usada por el dispositivo informático portátil 20 para confirmar la autenticación al servidor 30.

Por último, en función de la comunicación recibida, el servidor 30 autentica al usuario 1/autoriza la operación, o no.

En el caso de pérdida/robo de uno de los dos componentes 10, 20 del sistema descrito, el usuario 1 puede requerir al distribuidor, detrás de una autenticación requerida específicamente:

- El bloque (temporal) de las operaciones ejecutadas con su usuario (por ejemplo, pérdida de ambos elementos).
- La cancelación de la tarjeta pasiva 10 poseída previamente y el reemparejamiento de su dispositivo informático portátil 20 con una nueva tarjeta pasiva 10, que se proporcionará a través de un canal seguro (por ejemplo, pérdida de la tarjeta pasiva 10).
- La cancelación del código poseído previamente para el dispositivo informático portátil 20 y el reemparejamiento de su tarjeta pasiva 10 con un nuevo dispositivo informático portátil 20 (por ejemplo, pérdida del dispositivo informático portátil 20).

En una realización, como una característica adicional, una porción específica de los puntos capacitivos 11 puede usarse para codificar algún otra clase de información, incluyendo metadatos acerca del distribuidor o el propio sistema, o alguna información abierta acerca del usuario 1, sirviendo como un OpenID o como un nivel adicional de validación. Esta información se codificaría usando un sistema de codificación diferente, debido a que puede estar disponible para una descodificación abierta.

Los métodos y sistemas analizados anteriormente son ejemplos. Diversas configuraciones pueden omitir, sustituir o añadir diversas etapas de método o procedimientos, o componentes de sistema según sea apropiado. Por ejemplo, en configuraciones alternativas, los métodos pueden realizarse en un orden diferente del descrito, y/o pueden añadirse, omitirse y/o combinarse diversas fases o etapas o módulos. Asimismo, características descritas con respecto a ciertas configuraciones pueden combinarse en diversas otras configuraciones. Diferentes aspectos y elementos de las configuraciones pueden combinarse de una forma similar. Asimismo, la tecnología evoluciona y, por lo tanto,

muchos de los elementos son ejemplos y no limitan el alcance de la divulgación o las reivindicaciones.

En la descripción se dan detalles específicos para proporcionar un entendimiento exhaustivo de configuraciones de ejemplo (incluyendo implementaciones). Sin embargo, las configuraciones pueden ponerse en práctica sin estos detalles específicos. Por ejemplo, se han mostrado circuitos, procesos, algoritmos, estructuras y técnicas bien conocidos sin ningún detalle innecesario para evitar complicar las configuraciones. Esta descripción solo proporciona configuraciones de ejemplo, y no limita el alcance, la aplicabilidad o las configuraciones de las reivindicaciones. Más bien, la descripción precedente de las configuraciones proporcionará a los expertos una descripción habilitante para implementar técnicas descritas. Pueden hacerse diversos cambios en la función y disposición de elementos sin apartarse del espíritu de la divulgación.

Además, pueden implementarse ejemplos de los métodos por hardware, software, firmware, soporte intermedio, microcódigo, lenguajes de descripción de hardware, o cualquier combinación de los mismos. Cuando se implementan en software, firmware, soporte intermedio o microcódigo, el código de programa o segmentos de código para realizar las tareas necesarias puede(n) almacenarse en un medio legible por ordenador no transitorio tal como un medio de almacenamiento. Unos procesadores pueden realizar las tareas descritas.

Además, los ejemplos de ejemplo descritos en el presente documento pueden implementarse como operaciones lógicas en un dispositivo informático en un entorno de sistema informático en red. Las operaciones lógicas pueden implementarse como: (i) una secuencia de instrucciones, etapas o módulos de programa implementados por ordenador en ejecución en un dispositivo informático; y (ii) módulos de lógica o hardware interconectados en ejecución dentro de un dispositivo informático.

Aunque la materia objeto se ha descrito en lenguaje específico de características estructurales y/o actos metodológicos, ha de entenderse que la materia objeto definida en las reivindicaciones adjuntas no está limitada necesariamente a las características o actos específicos descritos anteriormente. Más bien, las características y actos específicos descritos anteriormente se divulgan como formas de ejemplo de implementación de las reivindicaciones.

REIVINDICACIONES

1. Un sistema para autenticación y/o autorización de usuario, que comprende:

una tarjeta pasiva (10) configurada para almacenar una primera porción de un código de autenticación o autorización a través de un conjunto de puntos capacitivos (11) incluidos en su superficie; y
un dispositivo informático portátil (20) de un usuario (1) que tiene una pantalla capacitiva, **caracterizado porque**:

- el dispositivo informático portátil (20) está configurado para almacenar una segunda porción de dicho código de autenticación o autorización; y
- la superficie de la tarjeta pasiva (10) se divide en diferentes áreas lógicas (12), comprendiendo cada área un conjunto de puntos capacitivos que codifican una primera porción diferente, siendo cada primera porción diferente para autenticar un servicio diferente o para autorizar una operación diferente,

de tal modo que, una vez que el usuario (1) ha solicitado acceso a un servicio específico o a una operación específica y cuando la tarjeta pasiva (10) está en contacto con la pantalla capacitiva, el dispositivo informático portátil (20) está configurado adicionalmente para leer al menos parte del conjunto de puntos capacitivos (11), descodificando la primera porción del código de autenticación o autorización, y firmando criptográficamente la primera porción descodificada usando como clave dicha segunda porción almacenada del código de autenticación o autorización, obteniendo el código de autenticación o autorización, que se usa como clave criptográfica para conceder acceso a dicho servicio específico u operación específica al usuario (1).

2. El sistema de la reivindicación 1, en donde el conjunto de puntos capacitivos (11) es invisible a la inspección humana.

3. El sistema de la reivindicación 1 o 2, en donde algunos de los puntos capacitivos del conjunto de puntos capacitivos (11) incluyen información acerca del usuario (1) o metadatos acerca de un distribuidor de tarjetas, codificándose la información o los metadatos con un sistema de codificación diferente del sistema de codificación usado para almacenar la primera porción del código de autenticación o autorización.

4. El sistema de una cualquiera de las reivindicaciones previas, en donde el conjunto de puntos capacitivos (11) incluye al menos dos puntos capacitivos ubicados en partes predefinidas de la tarjeta pasiva (10).

5. El sistema de la reivindicación 1, en donde la primera porción del código de autenticación o autorización depende de la forma, el tamaño y/o la posición del conjunto de puntos capacitivos (11) sobre la tarjeta pasiva (10).

6. El sistema de la reivindicación 1, en donde el dispositivo informático portátil (20) es un teléfono móvil, un portátil o una tableta y en donde la segunda porción del código de autenticación o autorización se almacena en un módulo de identificación de abonado, SIM, del dispositivo informático portátil (20) o en una memoria del mismo con acceso restringido.

7. Un método de autenticación y/o autorización de usuario, que comprende:

almacenar una primera porción de un código de autenticación o autorización a través de un conjunto de puntos capacitivos (11) incluido sobre una superficie de una tarjeta pasiva (10);
almacenar una segunda porción de dicho código de autenticación o autorización en un dispositivo informático portátil (20) de un usuario (1), teniendo el dispositivo informático portátil (20) una pantalla capacitiva;
dividir la superficie de la tarjeta pasiva (10) en diferentes áreas lógicas (12), comprendiendo cada área un conjunto de puntos capacitivos que codifican una primera porción diferente, siendo cada primera porción diferente para autenticar un servicio diferente o para autorizar una clase diferente de operación;
una vez que el usuario (1) ha solicitado acceso a un servicio específico o a una operación específica y cuando la tarjeta pasiva (10) está en contacto con dicha pantalla capacitiva, leer, por el dispositivo informático portátil (20), al menos parte del conjunto de puntos capacitivos (11), descodificar la primera porción del código de autenticación o autorización; y
firmar criptográficamente, por el dispositivo informático portátil (20), la primera porción descodificada usando como clave la segunda porción almacenada del código de autenticación o autorización, obteniendo el código de autenticación o autorización, que se usa como clave criptográfica para conceder acceso a dicho servicio específico u operación específica al usuario (1).

8. El método de la reivindicación 7, en donde algunos de los puntos capacitivos del conjunto de puntos capacitivos (11) incluyen información acerca del usuario (1) o metadatos acerca de un distribuidor de tarjetas, codificándose la información o los metadatos con un sistema de codificación diferente del sistema de codificación usado para almacenar la primera porción del código de autenticación o autorización.

9. El método de una cualquiera de las reivindicaciones previas 7 a 8, en donde el conjunto de puntos capacitivos (11) incluye al menos dos puntos capacitivos ubicados en partes predefinidas de la tarjeta pasiva (10), y en donde el conjunto de puntos capacitivos (11) es invisibles a la inspección humana.

10. El método de la reivindicación 7, en donde la primera porción del código de autenticación o autorización depende de la forma, el tamaño y/o la posición del conjunto de puntos capacitivos (11) sobre la tarjeta pasiva (10).

11. El método de la reivindicación 7, en donde dicha lectura se realiza mientras la tarjeta pasiva (10) está en contacto con dicha pantalla capacitiva en una posición específica, que incluye una posición horizontal o una posición vertical de la tarjeta pasiva (10), o mientras la tarjeta pasiva ha experimentado un movimiento específico, que incluye una rotación o un deslizamiento de la tarjeta pasiva (10), y en donde la posición específica o el movimiento específico son característicos del servicio o la operación solicitados por el usuario (1).

12. El método de la reivindicación 7, en donde el almacenamiento de la segunda porción del código de autenticación o autorización en el dispositivo informático portátil (20) se realiza después darse al usuario la tarjeta pasiva (10), en donde la segunda porción se almacena en un módulo de identificación de abonado, SIM, del dispositivo informático portátil (20) o en una memoria del mismo con acceso restringido, y en donde en caso de pérdida o robo de al menos la tarjeta pasiva (10), esta última se bloquea durante un periodo dado de tiempo o se reemplaza a través de un canal seguro.

13. Un producto de programa informático que comprende instrucciones de código de programa que, cuando se ejecutan por un procesador de un dispositivo informático portátil, implementan un método de autenticación y/o autorización de usuario mediante:

dividir la superficie de una tarjeta pasiva (10) en diferentes áreas lógicas (12), comprendiendo cada área un conjunto de puntos capacitivos (11) que codifican una primera porción diferente de un código de autenticación o autorización, siendo cada primera porción diferente para autenticar un servicio diferente o para autorizar una clase diferente de operación;
leer al menos parte de dicho conjunto de puntos capacitivos (11), realizándose dicha lectura cuando la tarjeta pasiva (10) está en contacto con una pantalla capacitiva del dispositivo informático portátil (20) y una vez que un usuario (1) ha solicitado acceso a un servicio específico o a una operación específica;
como resultado de dicha lectura, descodificar la primera porción; y
firmar criptográficamente la primera porción descodificada usando como clave una segunda porción de dicha autenticación o autorización almacenada en el dispositivo informático portátil (20), obteniendo el código de autenticación o autorización, que se usa como clave criptográfica para conceder acceso a dicho servicio específico u operación específica al usuario (1).

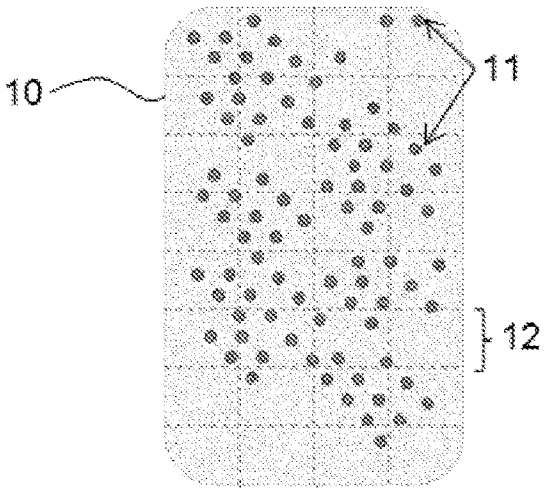
10
11
12

Fig. 1

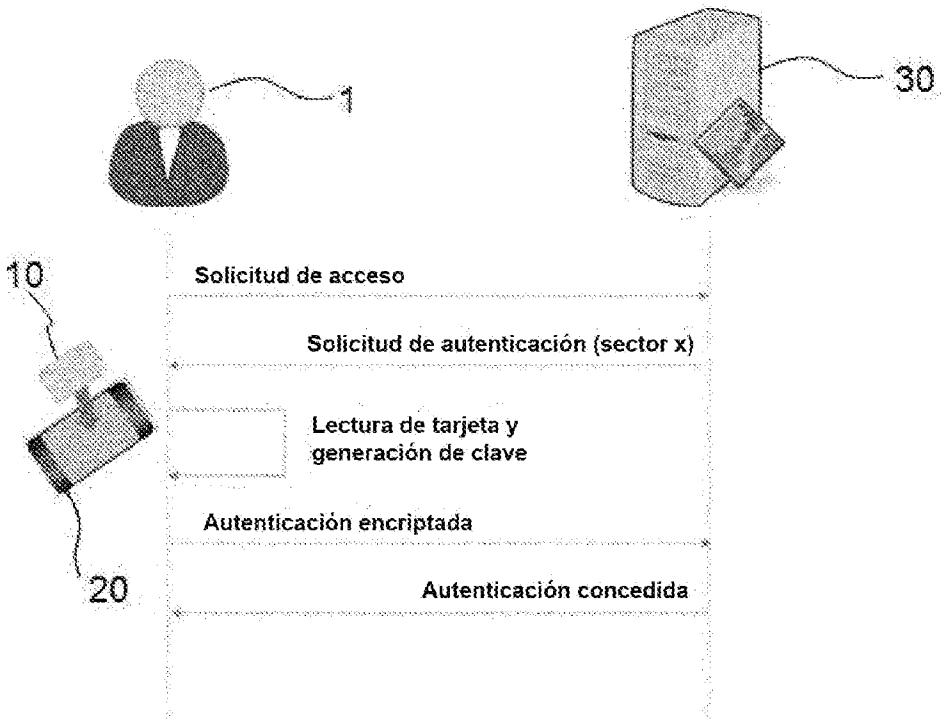
1
30
10
Solicitud de acceso
Solicitud de autenticación (sector x)
Lectura de tarjeta y
generación de clave
Autenticación encriptada
Autenticación concedida
20

Fig. 2