(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 359 788**

(51) Int. Cl.:
G07D 7/04 (2006.01)
G07D 7/06 (2006.01)
G07D 7/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **01949430 .1**
(96) Fecha de presentación : **22.06.2001**
(97) Número de publicación de la solicitud: **1295263**
(97) Fecha de publicación de la solicitud: **26.03.2003**

(54) Título: **Uso de un equipo de comunicación y procedimiento para autenticar un artículo, unidad y sistema para autenticar artículos, y dispositivo de autenticación.**

(30) Prioridad: **28.06.2000 EP 00113670**

(45) Fecha de publicación de la mención BOPI:
26.05.2011

(45) Fecha de la publicación del folleto de la patente:
26.05.2011

(73) Titular/es: **SICPA HOLDING S.A.**
avenue de Florissant 41
1008 Prilly, CH

(72) Inventor/es: **Amon, Maurice;**
Bleikolm, Anton;
Rozumek, Olivier;
Müller, Edgar y
Bremond, Olivier

(74) Agente: **Fàbrega Sabaté, Xavier**

DESCRIPCIÓN

Uso de un equipo de comunicación y procedimiento para autenticar un artículo, unidad y sistema para autenticar artículos, y dispositivo de autenticación

Campo de la invención

La invención es en el campo de la autenticación de artículos, específicamente de documentos, en particular de documentos de seguridad. Se refiere a un uso concreto de un equipo de comunicación, un procedimiento y una unidad para la autenticación de artículos de acuerdo con las reivindicaciones independientes.

Los artículos a autenticar, en particular los documentos de seguridad, se proporcionan con marcados o características de seguridad específicos que son difíciles de obtener o de producir, con el fin de conferir al artículo resistencia contra la falsificación. Dichos marcados o características de seguridad pueden tener propiedades físicas o químicas concretas, como permitir la interrogación con la ayuda de un equipo de detección correspondiente. Tales propiedades incluyen: características de absorción espectral concretas en el alcance óptico (longitud de onda de 200 nm - 2500 nm) del espectro electromagnético; luminiscencia (fluorescencia, fosforescencia) en el campo UV-visible-IR; absorción de IR medio, lejano, y muy lejano (longitud de onda de 2,5 µm - 1 µm); resonancia de radiofrecuencia y microondas; así como propiedades magnéticas y dieléctricas concretas. Dichos marcados de seguridad pueden diseñarse además para llevar información, que puede ser codificada o no. Los expertos en la materia conocen el significado de estos términos.

Dichas características de seguridad o marcados pueden ser parte del propio artículo (p. ej., ingredientes de un papel de seguridad o moldeadas en el plástico de una tarjeta), o estar fijadas al mismo a través de láminas metálicas, tintas, tóneres o recubrimientos. Particularmente interesantes en el contexto de la presente invención son las características de seguridad basadas en tinta, que se aplican al artículo a través de un proceso de impresión, como grabado en dulce, tipografía, impresión offset, serigrafía, huecograbado, flexografía, o impresión por chorro de tinta, o impresión de tinta sólida. La característica de seguridad también puede estar contenida en una composición de tóner electrostático o magnético, y aplicarse al documento por impresión láser. De manera alternativa, la característica de seguridad puede estar contenida en una composición de un recubrimiento superior de protección, aplicada al artículo de seguridad a través de cualquiera de las técnicas de recubrimiento conocidas.

Las características de seguridad en los artículos, en particular en los documentos de seguridad, son realmente aprovechadas por las autoridades de expedición y sus representantes legales. P. ej. la moneda emitida es reciclada y procesada regularmente por los bancos centrales que la ayuda de un equipo de autenticación y clasificación de alta velocidad especializado; pasaportes, documentos de identidad y carnets de conducir son verificados por la policía y las autoridades aduaneras; tarjetas de crédito, tarjetas de acceso y documentos valorados son verificados por los servicios forenses en caso de sospecha de falsificación; y los productos de marca son verificados por los comisarios del propietario de la marca con la ayuda de un equipo de detección especialmente diseñado.

El "hombre de la calle" debe confiar generalmente en sus cinco sentidos para autenticar un artículo, en base a las características de seguridad manifiestas del artículo, como el tacto y el perfecto registro de una impresión de grabado en dulce, la rigidez del billete de papel, el cambio de color de una tinta ópticamente variable, etc. Puede llevarse a cabo un examen más profundo con la ayuda de medios técnicos simples, como una fuente de luz UV portátil.

Hay, sin embargo, en algunos casos una necesidad de una verificación en el lugar de la autenticidad de determinados artículos a un nivel de seguridad como el que estaría normalmente sólo disponible en las instalaciones de una autoridad expedidora o del propietario de la marca. Tal necesidad surge especialmente en los dominios de productos de marca y artículos aduaneros, donde los propietarios de la marca o los comisionados del Estado deben verificar la autenticidad de las etiquetas de marca, marcas de impuestos, timbres etc. No existe ninguna solución técnica simple y versátil para resolver esta tarea.

En el documento EP-A-0 063 036 se sugiere un procedimiento para la autenticación de un billete de autobús, que comprende la instalación de una unidad de verificación de billetes en un autobús, pudiendo dicha unidad leer un código de barras impreso en el billete de autobús.

El documento WO 00/31679 divulga un módulo de seguridad telefónico por imágenes de iris y un procedimiento en el que un aparato de obtención de imágenes en el teléfono móvil toma una imagen del iris del usuario y compara una plantilla de la imagen con las plantillas almacenadas en una base de datos local o remota.

Objeto de la invención

Es un objeto de la presente invención ofrecer un procedimiento y el equipo correspondiente para la autenticación en el lugar de artículos, en particular documentos de seguridad, a niveles de seguridad avanzados con la ayuda de un

medio técnico de comunicación moderno. Dicho procedimiento y equipo son de uso fácil y casi en todas partes, son versátiles, altamente confiables y compatibles con los estándares técnicos comprobados.

De esta manera el objeto se consigue mediante la invención definida en la reivindicación 1, 7 y 11; las formas de realización de la invención se definen en las reivindicaciones dependientes.

Descripción de la invención

La invención, representada esquemáticamente en la Figura 1, se basa en la idea de utilizar el equipo de comunicación móvil ampliamente distribuido para la autenticación y el seguimiento de los productos de seguridad.

El terminal móvil es un componente de un sistema global, interactúa con cualquier tipo de capturador de datos de autenticidad que autentique capturadores de datos y se comunica con un servidor remoto de una manera amigable y segura (p. ej., utilizando un protocolo WAP).

Los capturadores de datos de autenticidad (detectores) se conectan al terminal móvil utilizando ya sea:

- una conexión por cable a un puerto,
- un radioenlace de corto alcance (p. ej., Bluetooth u otra tecnología de radio de baja potencia)
- un enlace de infrarrojos de corto alcance (p. ej., la tecnología IrDA)

El terminal móvil recibe una señal numérica del capturador de datos de autenticidad (dispositivo de autenticación), pudiendo ser este último de esta manera cualquiera de:

- un detector de radiación electromagnética,
- un escáner (para marcados o códigos de barras visibles o invisibles),
- una cámara CCD o CMOS,
- un detector de propiedad magnética,
- etc.

La autenticación de un artículo es autónoma y se logra por la infraestructura del terminal móvil que soporta las aplicaciones basadas en tarjetas inteligentes (p. ej., *Java Card*). Los programas de autenticación que procesan las señales del capturador de datos, que pueden ser, p. ej., un escáner o una cámara, pueden descargarse desde un servidor remoto.

La recuperación de datos y el seguimiento de un artículo se logran con la ayuda de un servidor remoto y se inician desde el terminal móvil. El terminal móvil recibe datos numéricos del dispositivo capturador, pre-trata estos datos si es necesario, y a continuación lleva a cabo una operación de autenticación local, utilizando los datos de referencia y el programa descargado, o, de manera alternativa, envía los datos del capturador a un servidor central para el seguimiento o la autenticación remota.

Por tanto la invención se basa en la idea de utilizar un equipo de comunicación móvil disponible en general, como teléfonos móviles u ordenadores de bolsillo, agendas electrónicas, etc., que cuenta con acceso a una red de telefonía móvil de área amplia (WAN), como medio de interrogación para la autenticación de artículos, en particular documentos de seguridad. El dispositivo de autenticación está de esta manera integrado en el equipo de comunicación, de manera que el usuario no necesite llevar consigo un equipo adicional para la autenticación de dicho artículo, o contenido en un hardware accesorio al equipo de comunicación. En este último caso, el accesorio hardware puede unirse al equipo de comunicación por cable, o por un radioenlace (microondas), o por un enlace óptico (infrarrojos).

Por tanto un aspecto de la invención consiste en el uso de al menos una capacidad existente de un equipo de comunicación móvil para la autenticación de un artículo, en particular un documento de seguridad, junto con un dispositivo de autenticación comprendido en dicho equipo de comunicación o conectado a él. Dicha capacidad se refiere de manera notable al procesamiento de datos del equipo de comunicación móvil y las capacidades de almacenamiento, sus capacidades de transferencia de datos, sus capacidades de interfaz de usuario, sus capacidades de interfaz de máquina, así como su fuente de alimentación. Según la invención, al menos un elemento de este grupo puede conectarse funcionalmente con un dispositivo de autenticación.

Los teléfonos móviles y otros equipo de comunicación incluyen de manera notable componentes de almacenamiento y procesamiento de datos sobre la placa; dichos componentes se implementan en parte como hardware fijo del equipo, y en parte como módulos intercambiables, como tarjetas SIM o Java, o similares.

Los teléfonos móviles y otros equipo de comunicación están equipados además con un hardware de comunicación y el software correspondiente para soportar la transferencia de datos a través de la capacidad de comunicación

intrínseca del teléfono móvil por una red de telefonía móvil (WAN), que permite que el teléfono establezca un enlace con un servidor remoto e intercambie datos con él. Los estándares de transferencia de datos útiles incluyen:

- GSM (sistema global para las comunicaciones móviles) 9,6 kb/s
- EDGE (tasas de datos mejoradas para la evolución GSM) hasta 120 kb/s
- GPRS (sistema global de radio por paquetes) entre 53,4 y 144 kb/s.
- UMTS (sistema universal de telecomunicaciones móviles) 384 kb/s, en construcción 2 Mb/s.

Los teléfonos móviles y otros equipos de comunicación tienen también capacidades de interfaz de usuario, que permiten al equipo recibir instrucciones a través de una entrada de teclado, presentar información visual a través de un panel de visualización, capturar sonido a través de un micrófono, y presentar el sonido a través de un altavoz.

Los teléfonos móviles y otros equipos de comunicación tienen finalmente capacidades de interfaz de máquina, que permiten al equipo de comunicación intercambiar datos con otros equipo a través de un conector alámbrico, o a través de una red de área local (LAN) utilizando un radioenlace o un enlace óptico (infrarrojos, IrDA).

Con el fin de interactuar con el dispositivo de autenticación del equipo de comunicación, los artículos comprenden unos marcados correspondientes. En particular, dichos marcados pueden ser recubrimientos o características impresas que absorben y/o transforman la energía proporcionada por el dispositivo de autenticación del equipo de comunicación. El dispositivo de autenticación se habilita para detectar la respuesta del marcado a la interrogación y/o leer la información contenida en el marcado.

Dicho respuesta del marcado, que sirve para su autenticación, es notable y en primer lugar una característica física, como una absorción espectralmente selectiva de la radiación electromagnética, o una emisión espectralmente selectiva de la radiación electromagnética en respuesta a un suministro de energía, u otras características eléctricas o magnéticas medibles, etc.. En segundo lugar el marcado también puede llevar información, expresada por dichas características físicas, y por consiguiente legible. Dicha información puede representarse o bien mediante una distribución local concreta, aleatoria o determinista, de dichas características físicas en el artículo que lleva el marcado (almacenamiento de información localizada), o bien por una combinación concreta de dichas características físicas con unas características físicas adicionales (almacenamiento de información no localizada), o por una combinación de ambas.

Dichos marcados pueden comprender de manera notable un material de escamas o partículas, impreso para resultar en un patrón de distribución de escamas o partículas local aleatorio característico, en un área superficial dada, que puede ser leído y autenticado por el dispositivo de autenticación, y que confiere al artículo una identidad concreta.

La detección de señales de respuesta emitidas por dicho marcado en dicho artículo y/o lectura de la información local y/o no local contenida en dicho marcado es llevada a cabo por el dispositivo de autenticación comprendido en, conectado a, o enlazado al equipo de comunicación y/o, en el caso de una respuesta de radiación electromagnética visible, también a simple vista.

Según un aspecto importante de la invención, las capacidades intrínsecas del equipo de comunicación se utilizan para autenticar dicho marcado en dicho artículo. El equipo de comunicación tiene una notable capacidad de procesamiento y almacenamiento de datos sobre la placa y la capacidad de comunicar, es decir, intercambiar datos con instalaciones de procesamiento y almacenamiento de datos remotos. Además tiene al menos dos tipos de interfaces de usuario, que permiten que el usuario introduzca datos, y que el equipo de comunicación devuelva datos.

Según una forma de realización de la invención, la capacidad de tratamiento y almacenamiento de datos sobre la placa del equipo de comunicación se utiliza para llevar a cabo la función de autenticación localmente, es decir, para autenticar el artículo, en base a las señales o datos facilitados por el dispositivo de autenticación.

Dicha capacidad de procesamiento y almacenamiento de datos se utiliza de esta manera para soportar un algoritmo de autenticación, que puede estar contenido en un dispositivo de memoria del equipo de comunicación, como una tarjeta Java. Dicho algoritmo de autenticación puede de esta manera ser físicamente cargado en el equipo de comunicación en forma de un dispositivo en estado sólido que lo contiene, o de manera alternativa puede descargarse desde un servidor a través de un enlace telefónico. El resultado de la operación de autenticación llevada a cabo localmente es posteriormente presentado por el equipo de comunicación, o, de manera alternativa, por el dispositivo de autenticación externa conectado o enlazado a él.

Según una variante, la capacidad de comunicación del equipo de comunicación se utiliza para llevar a cabo la función de autenticación en un lugar remoto. Las señales o datos facilitados por el dispositivo de autenticación son transmitidas, después de un pre-procesamiento apropiado, por el equipo de comunicación a un servidor remoto que comprende una memoria, una base de datos de referencia, un procesador, así como dicho algoritmo de autenticación. El resultado de la operación de autenticación se transmite de vuelta al equipo de comunicación, donde

es presentado posteriormente, por el equipo de comunicación, o, de manera alternativa, por el dispositivo de autenticación conectado o enlazado a él externamente.

En una forma de realización del procedimiento, los medios de procesamiento y almacenamiento de datos del hardware del dispositivo de comunicación móvil se utilizan para llevar a cabo dicha autenticación localmente, de manera que al menos parte de dicho algoritmo de autenticación pueda ser descargado en el dispositivo de comunicación a través de un enlace telefónico, o, de manera alternativa, insertado en él en forma de chip de memoria, tarjeta Java, etc.

En otro procedimiento, el dispositivo de comunicación móvil transmite los datos a través de un enlace telefónico a un servidor remoto para la autenticación remota, y recibe de vuelta el resultado de la autenticación. Sin embargo, incluso en este caso, el equipo de comunicación móvil lleva a cabo parte del procesamiento de datos localmente, lo que puede incluir la compresión de datos, el modelado de datos, y la encriptación de datos (codificación/decodificación).

La descarga y/o subida de información entre dicho dispositivo de comunicación y dicho servidor remoto se lleva a cabo preferentemente utilizando una conexión encriptada segura. Una conexión segura, como saben los expertos en la materia, puede producirse en base al algoritmo "Rivest, Shamir, Adleman" (RSA).

El marcado sobre el que se aplica dicho procedimiento comprende al menos un elemento de seguridad, seleccionado del grupo que consiste en materiales magnéticos, materiales luminiscentes, materiales absorbentes espectralmente selectivos - preferentemente en el infrarrojo, materiales resonantes de radiofrecuencia, microchips transpondedores, y patrones de escamas o partículas.

A continuación se explicará la invención en mayor detalle con la ayuda de los dibujos adjuntos.

Breve descripción de los dibujos

Fig. 1 muestra una vista esquemática de la invención, que se refiere a un sistema de autenticación para artículos, en particular productos de marca y documentos de seguridad ("producto"): un capturador de datos de autenticidad, como una cámara, un escáner o un detector de radiación electromagnética, se conecta o enlaza a un dispositivo de comunicación móvil 1, capaz de llevar a cabo el procesamiento de datos locales (tarjeta inteligente), y capaz de comunicarse con un servidor remoto (base de datos).

Fig. 2 muestra una vista esquemática de una forma de realización de ejemplo de un dispositivo de comunicación 1 para la autenticación de artículos, como puede utilizarse en la presente invención.

Fig. 3 muestra una vista esquemática de un dispositivo de autenticación y un artículo 2 a autenticar: la Fig. 3a muestra una primera forma de realización del dispositivo, que utiliza una cámara con microchip CMOS C en modo de copia por contacto con iluminación trasera L; la Fig. 3b muestra una segunda forma de realización del dispositivo, que utiliza una cámara con microchip CMOS C en el modo de obtención de imágenes con iluminación frontal L; la Fig. 3c muestra una vista esquemática de un documento a autenticar utilizando los dispositivos de la Fig. 3a o Fig. 3b, que lleva un marcado 21.

Fig. 4 muestra una forma de realización particularmente útil del marcado de seguridad 21, que se base en un patrón que confiere identidad de partículas o escamas con unas propiedades físicas concretas, combinado con una numeración de micro-texto.

Descripción detallada de la invención

Según la Fig. 1 el dispositivo de comunicación móvil 1 utilizado para la autenticación de un artículo puede ser un teléfono móvil, un ordenador de bolsillo, una agenda electrónica, un terminal electrónico o una cámara, que cuenta con acceso a una red de telefonía móvil de área amplia (WAN). Dicho equipo de comunicación 1 (Fig. 2) puede comprender un alojamiento 10, un conector de terminal alámbrico 11a, un puerto de comunicación IR 11b y/o un transmisor/receptor RF 11c. De esta manera puede hacerse uso concreta de componentes funcionales del dispositivo de comunicación ya existentes, como un micrófono 13, botones de teclado 9, un panel de visualización 14 y un altavoz 15, para llevar a cabo la función de autenticación, gestionar la interacción con el usuario y, opcionalmente, presentar los contenidos de datos. Los expertos en la materia conocen todos estos componentes y no necesitan ser descritos adicionalmente en el presente documento. Dicho dispositivo de comunicación puede además operarse móvil respectivamente fijo. Por supuesto, también es posible un uso de una combinación de dichos componentes funcionales del equipo de comunicación.

El dispositivo de autenticación o capturador de datos de autenticidad, destinado a interactuar fundamentalmente con dicho artículo o documento a autentificar, está comprendido en el dispositivo de comunicación, o enlazado localmente a él mediante un enlace alámbrico, mediante un puerto de comunicación IR o mediante un puerto transmisor/receptor RF.

La Fig. 3 muestra un ejemplo de un dispositivo de autenticación o capturador. El artículo 2 a autenticar puede ser un artículo o un documento, en particular un documento de seguridad. El artículo 2 puede ser plano con dos superficies, y lleva al menos un marcado 21. Dicho marcado es preferentemente una tinta impresa, con la propiedad de transformar y absorber específicamente la energía proporcionada por dicho dispositivo de autenticación. Dicha energía puede ser radiación electromagnética y/o energía eléctrica o de campo magnético, que se transforma mediante al menos un componente de dicha tinta en una respuesta característica, que a su vez puede ser capturada por dicho dispositivo de autenticación. De manera opcional, dicho dispositivo de autenticación también es capaz de leer información manifiesta o encubierta localizada o no localizada transportada por medio de dicha tinta en dicho artículo o documento.

En un primer tipo de forma de realización de la invención, como se muestra en la Figura 3a, el dispositivo de autenticación es un chip de microcámara CMOS C, integrado en un teléfono móvil 1. Dicho chip de cámara está equipado con una placa de interfaz de fibra óptica P, para tomar una imagen de una parte de la superficie de dicho documento 2 en transparencia, utilizando iluminación contraluz L y un modo de obtención de imágenes de copia por contacto 1:1. El chip de cámara CMOS C es una microcámara digital de un solo chip, que comprende un sistema de sensores de píxeles activos 256 x 256, junto con el sistema de circuitos de lectura de cámara necesario, integrado en un área de 4,8 x 6,4 mm. Esto corresponde a un tamaño de píxel individual de 18 µm. Los sensores de píxeles activos soportan una cierta cantidad de procesamiento de señales de píxel activado, como p. ej., la regulación de sensibilidad automática, o un control de tiempo de la sensibilidad de píxel (denominados píxeles de demodulación síncrona). Tanto la fuente de luz L como el chip de cámara C se conectan a un procesador µp del teléfono móvil. La placa de fibra óptica P es un conducto de imágenes muy corto, dispuesto en la parte superior del chip de cámara a fin de evitar que el chip sea arañado por el contacto con el documento 2 o el entorno. Opcionalmente, puede estar presente un filtro óptico F en la trayectoria del haz, con el fin de seleccionar/delimitar el rango de longitudes de onda de sensibilidad de la cámara.

De manera alternativa, puede utilizarse un sistema de lentículos de plástico bidimensional en lugar de la placa de fibra óptica P. Los expertos en la materia conocen dispositivos como los chips de cámara CMOS de sensor de píxeles activos, las placas de fibra óptica, y los sistemas de lentículos y no necesitan ser explicados adicionalmente en la presente.

En una forma de realización alternativa, representada en la Fig. 3b, se utiliza una lente 3 de distancia focal corta f en lugar del conjunto de " copia por contacto " utilizando una placa de fibra óptica. En este caso, la imagen en el documento puede ampliarse o reducirse eligiendo correspondientemente el plano del objeto OP y el plano de imagen IP. De esta manera el chip de cámara C se ubica en el plano de imagen IP de la lente 3 y se utiliza una placa de vidrio G para definir el plano del objeto OP. Las ubicaciones respectivas O e i (distancias desde el centro de la lente LP) del plano del objeto OP y el plano de imagen IP se relacionan con la longitud focal f de la lente por la fórmula de lente:

$$f^{-1} = O^{-1} + i^{-1}$$

Elegir O = i = 2f resulta en una imagen del objeto 1:1 (marcado 21) en el chip de cámara C. Opcionalmente, puede disponerse un filtro óptico F antes del chip de cámara, con el fin de seleccionar el rango de longitudes de onda de sensibilidad. Opcionalmente, utilizando esta forma de realización, el documento puede iluminarse desde la parte frontal mediante un iluminador L ubicado detrás de la placa de vidrio G que define el plano del objeto OP.

Según la invención, el dispositivo se utiliza para obtener una imagen de micro indicios en un área de 5 x 5 mm presente en una esquina de dicho documento 2. Dichos micro indicios se imprimen con una tinta que comprende un pigmento luminiscente. Dicho pigmento puede excitarse mediante la fuente de luz L y tiene emisión de luminiscencia retardada con un comportamiento de subida y disminución de intensidad característica en función del tiempo. En particular, dicha fuente de luz L puede elegirse para ser un sistema cuadrada de 5 x 5 mm de cuatro chips de diodos planos que emiten luz UV (que emiten a una longitud de onda de 370 nm), cubiertos por una placa de vidrio de protección, y dicho pigmento luminiscente en dicha tinta puede elegirse para ser un fósforo oxisulfuro dopado con europio de la fórmula Y_2O_2S:Eu.

Para autenticar el documento 2, el área de código 21 se inserta en el dispositivo de autenticación y se sostiene bien entre la placa de vidrio de la fuente de luz L y la placa de fibra óptica P, o se presiona contra la placa de vidrio G que define el plano del objeto, respectivamente, del dispositivo de autenticación. El proceso de autenticación es regulado por un procesador µP del teléfono móvil, según un programa concreto almacenado en la memoria del procesador, o contenido en, p. ej., una tarjeta Java. La autenticación comprende las etapas de i) encender la fuente de luz L

durante un intervalo de tiempo corto (p. ej., 1 ms), ii) controlando correspondientemente los píxeles activos del chip de cámara CMOS, medir la intensidad de la luminiscencia retardada al menos una primera vez después de apagar la fuente de luz, iii), opcionalmente, repetir la etapa i) y medir la luminiscencia retardada una o más veces más después de apagar la fuente de luz, iv) retener sólo los píxeles que muestran las características de intensidad específicas en los momentos de la medición, v) autenticar la imagen formada por los píxeles retenidos en etapa iv).

El proceso de medición, según la invención, es controlado por la memoria y el procesador interno del teléfono móvil, en la medida en que las variables del proceso de medición no se implementan de manera fija en el dispositivo de autenticación, sino más bien son suministradas por el teléfono móvil, por medio de, p. ej., una descarga o datos de referencia y un protocolo de medición suministrado de otra manera, que pueden estar contenidos en una tarjeta Java o similar. En la presente forma de realización, la selección de las características de disminución de la luminiscencia correctas para el pigmento luminiscente a detectar constituye un primer conjunto de tales variables del proceso de medición.

Los datos de lectura de la cámara CMOS se transfieren posteriormente al medio de procesamiento y almacenamiento del teléfono móvil, donde son autenticados localmente, por dichos datos de referencia y protocolo de medición suministrado de otra manera o descargados. Dicha autenticación puede adoptar la forma de una correlación estadística. Si S es la imagen de señal medida, representada por un vector de 256 x 256 (es decir, 65.536) valores de intensidad correspondientes a la resolución de la cámara, y R es una imagen de referencia correspondiente, representada por un vector similar, el producto interior normalizado (escalar) de ambos vectores $(<S/S>*<R/R>)^{-1/2*}<S/R>$ representa una medida de similitud; de hecho, para S = R este producto es 1. Pueden aplicarse esquemas de ponderación y pretratamiento apropiados a S y R antes de la correlación. Por supuesto pueden utilizarse otras formas de comparación y otros algoritmos para la evaluación de datos, de manera que se dedique un interés concreto a la compresión de datos y los algoritmos de transformación, así como a los algoritmos de decodificación/comparación rápidos, que evitan tiempos de cálculo excesivos.

En una forma de realización alternativa, dichos datos se transmitan a un servidor remoto para la autenticación, utilizando la capacidad de comunicación del teléfono móvil, y dicho servidor remoto transmite de vuelta a los teléfonos móviles el resultado de la operación de autenticación. El resultado de la autenticación se presenta en ambos casos utilizando la capacidad de visualización de datos del teléfono móvil. La capacidad de procesamiento de datos del teléfono móvil se utiliza en el presente documento para comprimir y encriptar los datos para una transmisión rápida y segura, y para desencriptar el resultado recibido.

La autenticación fuera de línea (local) en relación con un teléfono móvil o equipo de comunicación móvil similar tiene notablemente la ventaja de ahorrar tiempo de conexión (el teléfono móvil no debe estar conectado mientras se lleva a cabo la verificación de la autenticidad), al tiempo que mantiene el beneficio de los datos de referencia y protocolo de operación descargados. De esta manera, ni el teléfono móvil ni el dispositivo de autenticación contienen datos sensibles cuando están fuera de uso. El sistema de autenticación es además extremadamente flexible como para cambiar los algoritmos de autenticación o datos de referencia; una única conexión a servidor maestro remoto es suficiente para reprogramarlo para una aplicación diferente. El mismo hardware puede servir así a un gran número de destinos de aplicaciones diferentes, que es una ventaja decisiva especialmente para las aplicaciones de oficina de aduana, donde debe verificarse un gran número de artículos diferentes.

En otra forma de realización más del primer tipo, particularmente útil para los documentos de identidad, el marcado de seguridad es un patrón aleatorio de partículas o escamas ópticamente autenticables, aplicado sobre un microtexto impreso, como se muestra en la Fig. 4. Dicho patrón aleatorio de partículas se produce recubriendo sobre dicho documento impreso, al menos en parte, con un barniz transparente que contienen dichas partículas ópticamente autenticables en una concentración apropiada. Dicho barniz de recubrimiento superior puede tener adicionalmente una función de protección, y dichas partículas ópticamente autenticables pueden tener características ópticas concretas, como una reflectividad espectralmente selectiva, una apariencia de color dependiente del ángulo, luminiscencia, polarización, etc. Dicho micro-texto de recubrimiento superior es preferentemente una micro-numeración, con un tamaño de letra inferior a 1 mm, preferentemente inferior a 0,5 mm.

Dicha micro-numeración individualiza el documento, pero por sí misma no es suficiente para conferir una identidad (los números solos podrían copiarse notablemente a un documento falsificado). El documento numerado se individualiza por medio de las partículas distribuidas al azar y físicamente identificables (autenticables) comprendidas en el recubrimiento superior.

El proceso de autenticación correspondiente se basa en un registro combinado, por el chip de cámara, del micronúmero del documento, rodeado por su patrón de partículas único, de manera que las características ópticas de dichas partículas pueden verificarse adicionalmente para las propiedades físicas auténticas. Una imagen de referencia de un "patrón combinado con micronúmeros" del documento auténtico se almacena en un servidor remoto, al que se transmite la solicitud de autenticación, junto con los datos de imagen registrados del documento en cuestión. De esta manera sólo se transmiten los píxeles de imagen del patrón con las propiedades físicas previstas correctas.

En una forma de realización del segundo tipo de la invención, el dispositivo de autenticación es un micro-espectrómetro para llevar a cabo un análisis espectral en el intervalo de longitudes de onda del infrarrojo cercano (NIR, 700 nm a 1100 nm), contenido en un accesorio del teléfono móvil, que está unido por cable a él a través del conector de clavijas múltiples del hardware del teléfono.

Dicho micro-espectrómetro consiste en una fuente de luz incandescente, que ilumina un punto concreto de la muestra, y un dispositivo de guía de ondas planas/rejilla de enfoque como se describe en DE 100.10.514 A1, montado en un sistema de fotodetectores con 256 píxeles sensibles a la luz dispuestos linealmente. En formas de realización alternativas, también pueden utilizarse sistemas de fotodetectores con más o menos píxeles, que resultan en una resolución espectral diferente. Los expertos en la materia conocen tales conjuntos de micro-espectrómetros, así como su modo de funcionamiento.

Dicho sistema de fotodetectores es leído por circuitos electrónicos sobre la placa, y la información espectral resultante, es decir, la intensidad de reflexión difusa de la muestra en función de la longitud de onda de la luz, se transmite a través del enlace alámbrico al procesador del teléfono móvil, que lleva a cabo la autenticación localmente, o transmite los datos a un servidor remoto, como se ha descrito anteriormente.

La característica espectral a detectar puede ser una tinta impresa que contiene un pigmento de naftalocianina, como octabutoxinaftalocianina de cobre descrito en DE 43 18 983 A1. Este pigmento tiene un pico de absorción característico en el infrarrojo, a una longitud de onda de 880 nm, al tiempo que es prácticamente incoloro en el intervalo visible del espectro. El micro-espectrómetro puede utilizarse para detectar tintas que contienen 2-5% de este pigmento, añadido como elemento de seguridad a los "colores ordinarios"; la información espectral completa obtenida indica no sólo la presencia de sólo un absorbedor de infrarrojos, sino también la naturaleza química correcta de este absorbedor, como se deduce de la ubicación y la forma del pico de absorción.

En una forma de realización alternativa, el espectrómetro se utiliza para detectar las emisiones luminiscentes de las tintas impresas. P. ej., una tinta que contiene un 5% de un pigmento de vanadato de itrio dopado con neodimio (YVO_4:Nd) se excita con un LED que emite color amarillo (a una longitud de onda de 600 nm). El multiplete de emisión de Nd^{3+} a 879 nm, 888 nm y 914 nm, con sus intervalos de intensidad característicos, se mide con el micro-espectrómetro y se interpreta en términos de una característica de autenticidad. Otros pigmentos luminiscentes que contienen neodimio, como p. ej., Y_2O_2S:Nd, muestran una forma de curva diferente de la emisión en torno a los 900 nm, y por lo tanto pueden utilizarse para representar características de autenticidad diferentes. Las mezclas de pigmentos luminiscentes que contienen neodimio pueden emplearse también, para producir un número aún mayor de posibles variedades espectrales, que pueden distinguirse en la forma de la curva de su espectro de emisión.

En todavía una forma de realización alternativa, el espectrómetro se diseña para funcionar en la parte más alejada del intervalo de longitudes de onda NIR (900 nm a 1750 nm), utilizando un sistema de fotodetectores lineal InGaAs y una rejilla de espectrómetro correspondiente. En este intervalo espectral, pueden utilizarse ciertos materiales que contienen tierras raras, así como ciertos colorantes tina que contienen radicales (p. ej., los descritos por J. Kelemen en Chimia 45 (1991), p. 15-17), como componente que absorbe el infrarrojo de una tinta. Es fácil para los expertos en la materia concebir aplicaciones análogas fuera de los dominios de las longitudes de onda mencionadas, como p. ej., en el ultravioleta o en el dominio visible del espectro electromagnético, así como en el dominio de infrarrojo medio (2,5 µm a 25 µm), que corresponde a las frecuencias de las vibraciones moleculares.

Los datos espectrales pueden correlacionarse con datos de referencia formando un producto interior normalizado $(\langle S/S\rangle^{*}\langle R/R\rangle)^{-1/2^{*}}\langle S/R\rangle$ de los vectores de señal (S) y de referencia (R), utilizando el pretratamiento y la ponderación en su caso, como se ha descrito anteriormente. Los datos espectrales pueden analizarse notablemente aplicando las mismas herramientas matemáticas de Componente Principal o Análisis Factorial, que permiten remontar las variaciones espectrales observadas a las concentraciones individuales de los tintes o pigmentos que constituyen la parte absorbente de la tinta.

En una forma de realización del tercer tipo de la invención, el dispositivo de autenticación es un escáner de mano de imagen óptica, enlazado al teléfono móvil a través de un enlace de radiofrecuencia (microondas) de tipo "Bluetooth". "Bluetooth" es un sistema de transferencia de datos de radiofrecuencia (RF) estandarizado para redes de área local (LAN), que opera en la banda ISM (“Industrial Scientific Medecine”) libre a 2,4 GHz (2,400-2,4835 GHz), que comprende 78 canales RF modulados en frecuencia, que son aprovechados en el modo de salto de frecuencia de espectro ensanchado. La potencia de salida de RF puede variar de 1 mW a 100 mW, dependiendo de la velocidad de transmisión a alcanzar. Una potencia de salida de 1 mW permite establecer una comunicación de RF segura en varias decenas de metros incluso dentro de un edificio; la RF penetra bastante bien a través de paredes y objetos no metálicos. En el caso de un enlace "Bluetooth" o un enlace de RF similar, el dispositivo de comunicación móvil puede por lo tanto mantenerse moderadamente alejado del dispositivo de autenticación.

El escáner de imágenes portátil es un dispositivo de tipo lápiz como se conoce en la técnica para el escaneado a mano y la traducción de palabras o líneas de texto, p. ej., el "Pocket Reader" de Siemens AG. El dispositivo utilizado

contiene una rueda rodante para detectar la velocidad de escaneado, una fuente de luz LED de infrarrojos que emite a una longitud de onda de 950 nm como un iluminador, un sistema de fotodetección lineal con un sistema óptico de obtención de imágenes, precedido por un filtro pasa banda con una ventana de transmisión de 950 nm-1000 nm, y un chip procesador con memoria para analizar los datos escaneados. Además tiene una línea de visualización y botones táctiles para comentarios de operador. El escáner contiene un módulo de comunicación Bluetooth, para conectarse a un módulo similar contenido en el teléfono móvil. Los datos escaneados se transmiten a través de este enlace al teléfono móvil, donde se procesan o se transmiten adicionalmente como se ha indicado anteriormente.

El marcado de seguridad en este ejemplo es un patrón invisible de absorción de IR impreso con una tinta que contiene un 10% de $YbVO_4$ como el pigmento de absorción de IR.

En una forma de realización de cuarto tipo de la invención, el dispositivo de autenticación es un escáner de mano de imágenes magnéticas, enlazado al teléfono móvil a través de un enlace de conexión de infrarrojos de tipo IrDA. IrDA es un protocolo de transferencia de datos ópticos para redes de área local (LAN), definido por la asociación de datos infrarrojos. Utiliza un enlace de transmisión de infrarrojos en el intervalo de longitudes de onda de 850 nm – 900 nm, en base a IR-LEDs o diodos láser como emisores y fotodiodos como receptores. La velocidad de transferencia de datos normal para un enlace en serie se especifica como 9,4 kb por segundo, pero las velocidades de transferencia de 2,4 kb/s, 19,2 kb/s, 38,4 kb/s, 57,6 kb/s, 115,2 kb/s, 0,576 Mb/s, 1,152 Mb/s y 4,0 Mb/s también son soportadas con el enlace óptico. La intensidad de emisión de luz está en el intervalo de algunos milivatios a unas decenas de milivatios, lo que permite una comunicación óptica en un intervalo de unos decímetros hasta unos pocos metros. Por tanto el dispositivo de autenticación debe mantenerse en contacto óptico con el teléfono móvil durante la operación.

El escáner de imágenes magnéticas se basa en un sistema lineal de sensores integrados de campo magnético, que puede ser del tipo magneto-resistivo (GMR) o el de efecto Hall. Tales elementos, que son conocidos por los expertos en la materia, p.ej. a partir de US 5.543.988, detectan la presencia de campos magnéticos locales, como los resultantes de un material impreso permanentemente magnetizado, y envían las señales de salida eléctricas correspondientes. Pueden utilizarse para mapear las distribuciones de campo magnético a lo largo de una línea o sobre un área superficial.

En esta forma de realización, se utiliza una tinta que contiene un material magnético "duro" (permanente), como hexaferrita de estroncio ($SrFe_{12}O_{19}$), para imprimir el marcado. Tales materiales están disponibles en Magnox, Pulaski VA, bajo el nombre de "Mag-Guard", y tienen valores de coercitividad de 3.000 Oersted o más. El pigmento se magnetiza permanentemente después de la impresión, aplicando un campo magnético correspondientemente fuerte en determinadas zonas del documento. La imagen magnética así almacenada no se borra en condiciones normales de uso, y por lo tanto puede servir como característica de seguridad permanente. Para leer la imagen, el escáner magnético se mueve sobre el sitio correspondiente en el documento, y los datos escaneados se transmiten a través del enlace de IR al teléfono móvil, donde se procesan o se transmiten adicionalmente como se ha indicado anteriormente.

En todavía otra forma de realización alternativa, se disolvió un derivado soluble de silicio-naftalocianina, que absorbe en el intervalo de longitudes de onda de 850-900 nm y re-emite a 920 nm, en una tinta líquida y se aplicó mediante impresión flexográfica sobre una lámina de envase tipo blíster en forma de código de barras del producto. Este código de barras del producto se leyó con la ayuda de un lector de código de barras en forma de lápiz especialmente diseñado, conectado a una agenda electrónica del tipo "comunicador" NOKIA. El lector de código de barras comprendía un LED de 880 nm como fuente de excitación. La luz de excitación se delimitó mediante un filtro pasa banda a 880±10 nm. La emisión luminiscente del código de barras se detectó mediante un fotodiodo de silicio, cuyo intervalo de sensibilidad espectral se delimitó mediante un filtro pasa banda a 920±10 nm. Dicho fotodiodo de silicio es parte de una foto-IC del tipo S4282-11 de Hamamatsu. Dicho foto-IC permite una detección sincrónica óptica notable bajo la luz de fondo; genera una señal piloto de 10 kHz para activar la excitación del LED, y es sensible exclusivamente a las señales de respuesta que se corresponden con la señal piloto en frecuencia y fase. Dicho foto-IC, LED de excitación, y filtros ópticos se disponen dentro de un alojamiento con forma de lápiz del lector de código de barras, junto con unas guías de luz de plástico para guiar la luz desde el LED hasta la punta del lápiz, y la emisión desde el documento de vuelta al foto-IC. El foto-IC en este lector de código de barras envía una señal de salida digital, que es representativa de la presencia o ausencia de luminiscencia en la punta del lápiz.

En otra forma de realización, el equipo de comunicación móvil contiene componentes para llevar a cabo una verificación de autenticidad física simple en un documento de seguridad. En este ejemplo, una fuente de luz UV (p. ej., un UV-LED que emite a 370 nm con 1 mW de potencia de salida óptica) irradia una ubicación determinada que contiene una característica de seguridad en dicho documento. Dicha característica de seguridad se imprime con una tinta que contiene el compuesto luminiscente de línea estrecha Y_2O_2S:Eu que tiene una emisión visible en el rojo, a 625 nm. La respuesta luminiscente a 625 nm es registrada por un fotodetector de silicio a través de un filtro pasa banda óptico de línea estrecha de 625 ± 1 nm. Para distinguir la respuesta luminiscente de la de luz de fondo ambiental, se enciende y se apaga la fuente de excitación a intervalos cortos, y el fotodetector se hace sensible sólo a la diferencia entre los estados de la "excitación encendida " y "excitación apagada". Como resultado de la prueba se emite una señal de "auténtico"/"falsificado". La señal resultante puede presentarse como una señal visual y/o sonora; esto último, es decir, el uso de los altavoces del equipo de comunicación móvil para anunciar el resultado del

ensayo, es una opción particularmente útil para las personas ciegas. Se entenderá que pueden utilizarse otros materiales luminiscentes, que emiten a otras longitudes de onda en la parte del espectro UV, visible o infrarrojo, en combinación con otros filtros y configuraciones de detector para observar la emisión luminiscente en el contexto de la invención.

En una variante de la forma de realización anterior, una tinta luminiscente con un tiempo de disminución de la luminiscencia característico se utiliza para imprimir la característica de seguridad, y el tiempo de disminución de la luminiscencia se evalúa a través de una determinación de la función de transferencia de modulación de la emisión luminiscente, utilizando una secuencia de excitación de pulsos a varias frecuencias de repetición de pulso: p. ej., la tinta contiene el compuesto luminiscente Y_2O_2S:Nd, que emite a una longitud de onda de 900 nm con un tiempo de disminución de la luminiscencia del orden de los 70 µs. La luminiscencia es excitada por un LED de 370 nm, que es modulado por una señal de baja frecuencia de frecuencia f. La respuesta de luminiscencia se detecta en fase con respecto a la frecuencia de modulación f, de manera que se suprimen de manera eficaz las contribuciones de luz de fondo. Cuando se escanea la frecuencia de modulación f de 1 kHz a 20 kHz, se observa una caída de la señal detectada a 14 kHz; por encima de esta frecuencia, la luminiscencia ya no es capaz de transferir la modulación de la fuente de excitación. Esta caída de la función de transferencia de modulación es una medida del tiempo de disminución de la luminiscencia. Por tanto se envía una señal "auténtica" sólo si se ha detectado un tiempo de disminución de la luminiscencia correcto a la longitud de onda de respuesta. Se entenderá que otros materiales luminiscentes y otras configuraciones para determinar el tiempo de disminución de la luminiscencia pueden utilizarse en el contexto de la invención.

Otra forma de realización proporciona la autenticación de dispositivos o tintas ópticamente variables a través del reconocimiento de las características de reflexión espectral dependientes del ángulo características de estos artículos. Las características de reflexión dependientes del ángulo están muy relacionadas con materiales concretos y con los correspondientes, a menudo caros, procesos de fabricación, y por lo tanto difíciles de falsificar. La forma de realización para la autenticación de tintas ópticamente variables es una variante de la forma de realización basada en micro-espectrómetro descrita anteriormente. Se utilizan dos micro-espectrómetros, o, preferentemente, un espectrómetro doble para recoger la luz prácticamente paralela del artículo o documento a dos ángulos de visualización predefinidos, uno correspondiente a una vista casi ortogonal y la otra casi rasante. En la forma de realización, estos ángulos de observación se eligieron a 22,5° y a 67,5° con respecto a la normal respecto a la superficie de la muestra impresa y la divergencia del rayo de la luz recogida se mantuvo dentro de los ±10°. La muestra se ilumina preferentemente con luz incandescente difusa que incide desde el sitio opuesto.

En una forma de realización adicional, el equipo de comunicación se diseña para detectar una radiofrecuencia característica o resonancia de microondas en dicho artículo. Dicha resonancia puede ser una resonancia natural de un material, p. ej., puede aprovecharse la línea de resonancia magnética nuclear interna del metal cobalto en su propio campo magnético (resonancia nuclear ferromagnética, ubicada a aproximadamente 214 MHz). El documento de seguridad se marca con un parche de tinta que contiene cobalto metálico en polvo. La unidad de detección comprende un generador de frecuencia a 214 MHz, una bobina de excitación/detección, un receptor a 214 MHz, y una unidad de conmutación rápida. La bobina se acerca a la muestra (parche de tinta) bajo prueba, y sus terminales se conmutan rápidamente hacia adelante y hacia atrás entre el generador de frecuencia y el receptor a 214 MHz. El material de resonancia ferromagnética se excita durante la fase de generador de frecuencia de la bobina, e irradia energía de RF (disminuciíón por inducción libre) durante la fase de receptor de la bobina. La presencia de material de resonancia ferromagnética que responde a 214 MHz aparece así como una señal en el receptor de RF, del que puede deducirse un resultado de autenticación. Se entenderá que pueden utilizarse otros materiales resonantes de microondas o de RF naturales, así como otras configuraciones de detector en el contexto de la invención.

De manera alternativa, puede aprovecharse una resonancia producida artificialmente, debido a un circuito LC eléctrico, un dipolo metálico, un elemento piezoeléctrico (cristal de cuarzo, dispositivo de onda acústica de superficie (SAW), etc.), o un elemento magnetostrictivo. La configuración del detector es análoga a la de detección de resonancia de microondas o frecuencia de radio natural. Los expertos en la materia conocen todas estas tecnologías y no necesitan ser descritas adicionalmente en este documento. El equipo de comunicación está de esta manera equipado específicamente con los componentes necesarios que incluyen las unidades de detección.

Todavía una forma de realización más se basa en materiales magnéticos amorfos como marcador, como $Co_{25}Fe_{50}Si_{15}$ o similares, que muestran magnetización fácil con baja coercitividad (< 5 Oe), alta cuadratura de la curva de histéresis, y un efecto Barkhausen correspondientemente alto. Los expertos en materia de aplicaciones de vigilancia electrónica de artículos (EAS) conocen estos materiales y los correspondientes equipos de lectura.

A continuación, se da un ejemplo de un ciclo de autenticación, que utiliza un dispositivo de autenticación de micro-espectrómetro según la forma de realización del segundo tipo. El artículo a autenticar es un sello de impuesto, tal como es emitido para el cobro de impuestos de las bebidas alcohólicas por las agencias estatales. El sello de impuesto lleva un parche de tinta impresa, que muestra una característica espectral concreta en el espectro de reflectancia infrarrojo difuso en el intervalo de los 700 nm a 1000 nm. Dicha característica espectral concreta se produce mediante la mezcla a la tinta de un pigmento absorbedor de infrarrojos, que puede ser de los tipos mencionados anteriormente.

El equipo de autenticación comprende un dispositivo de autenticación, que está unido por cable a un teléfono móvil a través de un conector en serie del teléfono. El teléfono móvil comprende una tarjeta de chip con procesador y memoria, capaz de interactuar con el dispositivo de autenticación. El dispositivo de autenticación comprende un micro-espectrómetro con un sistema óptico de captación, montado en un sistema fotodetector lineal de 256 píxeles, una pequeña fuente de luz incandescente, así como electrónica de digitalización y adquisición de datos para el sistema fotodetector y una interfaz para la transferencia de datos desde y hasta el puerto serie del teléfono móvil. El dispositivo autenticador se alimenta con batería del teléfono móvil.

Para autenticar el sello de impuesto en cuestión, el algoritmo de autenticación correspondiente (programa), así como el espectro de absorción de infrarrojos de referencia, son primero descargados al teléfono mediante una llamada a un servidor remoto protegido con contraseña. Los datos de referencia y de programa se instalan en la tarjeta de chip del teléfono y el programa se lanza a través de una entrada de teclado correspondiente en el teléfono. El dispositivo de autenticación se sitúa en el sello de impuesto, en la parte superior del parche de tinta a autenticar, y se lanza la medición presionando una tecla en el teléfono móvil. La lámpara incandescente y el micro-espectrómetro están encendidos, y se adquiere un espectro de reflectancia difusa y se almacena en la tarjeta de chip del teléfono móvil. A continuación el dispositivo de autenticación se apaga inmediatamente de nuevo, para ahorrar batería. Todo el ciclo de medición tarda menos de un segundo.

Los datos medidos (S), se almacenan como un vector de 256 puntos de datos de intensidad espectral (S_i) que representa el intervalo de longitudes de onda desde 700 nm hasta 1000 nm, se pretrata apropiadamente, p. ej., restando el valor de intensidad medio (s_{medio}) de cada uno de los puntos espectrales (s_i: = s_i-s_{medio}). Igualmente, los datos de referencia descargados (R) se almacenan como un vector de 256 puntos espectrales (r_i) correspondiente al mismo rango de longitudes de onda. Preferentemente, los datos de referencia son normalizados, es decir, $\Sigma\, r_i^2 = 1$.

La similitud de los datos medidos (S) y los datos de referencia (R) se verifica a través del coeficiente de correlación $c = \Sigma\, r_i s_i/(\Sigma s_i^2)^{1/2}$, se da por hecho que R se normaliza. Si el coeficiente de correlación c es igual a 1, las formas de onda (espectro de reflectancia) de los datos de referencia y los datos medidos son iguales. En general, c puede tomar cualquier valor entre -1 y + 1. La muestra medida se declara auténtica si c está por encima de un criterio limitante descargado previamente y definido correspondientemente c_{lim}.

El procesador en el teléfono móvil lleva a cabo estas operaciones, y presenta un mensaje de "auténtico" o "falsificado" en la unidad de visualización del teléfono móvil. También puede presentarse una señal acústica a través del altavoz del teléfono móvil.

De manera alternativa, las desviaciones de los datos de referencia y los datos medidos normalizados pueden utilizarse como un criterio de decisión. Con este objetivo, los datos medidos (S) se normalizan primero, de manera que $\Sigma\, s_i^2 = 1$. Se da por hecho que los datos de referencia (R) se normalizan también. La desviación media $d = (\Sigma(s_i-r_i)^2/N)_{1/2}$, con N = número de puntos de muestreo (256 en nuestro caso), es una medida de divergencia entre los datos medidos (S) y los de referencia (R), que pueden verificarse contra dicho criterio de decisión. Si d es superior a un criterio definido correspondientemente d_{lim}, la muestra medida se declara una falsificación.

Dicha autenticación de muestras puede ocurrir fuera de línea una vez que se han descargado los datos de referencia y el algoritmo de autenticación, utilizando el dispositivo de autenticación simple conectado al teléfono móvil. El resultado de la autenticación se presenta fuera de línea. Opcionalmente puede retenerse en la memoria del teléfono, junto con los identificadores del artículo escaneado o la entrada de usuario y similares, para una subida posterior al servidor remoto.

De manera alternativa, dicho algoritmo también puede llevarse a cabo en el servidor remoto; en cuyo caso el teléfono móvil simplemente sube los datos medidos (S), en su caso junto con los identificadores del artículo escaneado o la entrada de usuario y similares, al servidor remoto, y recibe de vuelta el resultado de la operación de autenticación. En este caso, el servidor remoto puede protocolizar directamente la operación de autenticación.

El software de autenticación se distribuye preferentemente sólo a un número limitado de usuarios autorizados, a los que se ha dado acceso al mismo a través de las claves de cifrado y las contraseñas correspondientes. Preferentemente, la transferencia de datos entre el dispositivo de comunicación y el servidor remoto es segura, es decir, está protegida por las claves de cifrado/descifrado correspondiente.

Hasta el momento, sólo se ha considerado la autenticación de las características físicas. En una forma de realización más avanzada, la verificación también comprende la lectura de información lógica en dicho artículo. En un ejemplo, un código de barras 1-D ó 2-D, impreso en el artículo con tinta magnética, se lee con la ayuda de un sistema de sensores magnéticos unidimensional o bidimensional (p. ej., del tipo magnetorresistivo, o del tipo efecto Hall) y evaluado en términos de autenticidad del artículo en cuestión. Los elementos del sensor magnético del tipo magnetorresistivo comercialmente disponible, p. ej., el KMZ-51 de Philips. Pueden disponerse en sistemas y tienen suficiente sensibilidad para medir los campos magnéticos débiles, como el campo de la tierra. Un sistema de sensores de efecto Hall ha sido descrito en US 5.543.988. La ejecución de un detector de tinta magnética para los

documentos se describe en US 5.552.589. Se entenderá que dicho código de barras y la unidad detectora correspondiente también pueden producirse con una tecnología diferente a la magnética: p. ej., absorción de UV, absorción de IR, absorción del visible de banda estrecha, luminiscencia en el campo UV-visible-IR, impresión dieléctrica o metálica, etc.

En una versión más simple, la lectura de información se basa en un detector de un solo canal, combinado con un escaneado manual de la zona sensible del artículo a autenticar. La luminiscencia simple, las unidades de sensor metálicas y magnéticas descritas anteriormente en este documento pueden utilizarse ventajosamente con este propósito. Se entenderá que la unidad de detección de un solo canal puede producirse nuevamente en cualquier tecnología que se preste a una lectura de la información desde un soporte.

La lectura de la información del artículo puede combinarse con una reproducción visual o audible de determinados contenidos de información. En particular, utilizando la presentación audible, puede producirse un detector/autenticador para las personas ciegas, que, después de la autenticación de la moneda, sonoramente anuncia la denominación y la unidad monetaria respectiva.

Una forma de realización concreta se basa en la información almacenada dentro de un microchip transpondedor, contenido en o sobre dicho artículo. Los microchips unidos sobre el hilo de seguridad de un billete, que utilizan las partes metalizadas del mismo como su antena, son factibles y se han presentado a la comunidad de seguridad. En esta forma de realización, un transmisor de espectro ensanchado contenido en el equipo de comunicación, o en un accesorio, se utiliza para interrogar el microchip transpondedor y leer la información almacenada para fines de verificación. Los expertos en la materia conocen los chips del transpondedor que operan en la tecnología de espectro ensanchado en las bandas de frecuencia necesarias (p. ej., la banda ISM de 2,4 GHz). Se entenderá nuevamente que, en el contexto de la invención, la comunicación con el microchip transpondedor puede basarse en cualquier tecnología viable y no se limita al protocolo de comunicación de espectro ensanchado mencionado.

En una forma de realización particularmente preferente, se hace uso de las instalaciones de comunicación del equipo de comunicación para una verificación cruzada de la información de autenticidad de dicho artículo, específicamente de un documento, en particular de un documento de seguridad con los datos de la autoridad expedidora de dicho artículo. Los documentos de seguridad (p. ej., billetes de banco, tarjetas de crédito, pasaportes, tarjetas de identidad, tarjetas de acceso, carnets de conducir, etc.) pueden marcarse notablemente a su identidad física mediante una serie de formas: incorporación de las distribuciones aleatorias de fibras o partículas de colores, luminiscentes, metálicas, magnéticas u otras fibras o partículas en el sustrato de plástico o papel del documento; impresión de parches de tinta que contienen distribuciones aleatorias de determinadas partículas detectables de dichos tipos; marcados por chorro de tinta o láser del documento de seguridad con un patrón aleatorio apropiado; etc.

Estos datos de identidad, que son únicos para el artículo de que se trate, pueden ser vinculados por la autoridad expedidora al número de serie del documento de seguridad concreto, y los datos de correlación resultantes pueden quedar disponibles en una base de datos para fines de verificación cruzada. La característica que confiere identidad del documento de seguridad es detectada por un detector apropiado incorporado en el equipo de comunicación, y los datos de identidad resultantes se envían, junto con el número de serie impreso del documento de seguridad, a la base de datos de la autoridad expedidora. A continuación de devuelve una respuesta de "sí" o "no" al remitente para confirmar o para no confirmar la autenticidad física de del documento de seguridad en cuestión.

En un ejemplo de esta forma de realización, un parche de tinta que contienen partículas opacas de un tamaño de 30-50 µm se aplica al artículo mediante serigrafía. Las partículas son preferentemente planas y pueden elegirse, p. ej., de entre los grupos de escamas de pigmento ópticamente variable, escamas de aluminio o escamas de polímero opaco. La concentración de escamas en la tinta se dispone de manera que el número de escamas por cm^2 se elige preferentemente para ser del orden de 10 a 100.

El patrón de escama, que es característico para cada artículo individual, se detecta dentro de un área bien definida del documento en translucidez mediante un elemento sensor CCD bidimensional, aplicado en el modo de copia por contacto sobre la zona en cuestión. El elemento sensor CCD tiene unas dimensiones típicas de 0,5 pulgadas por 0,5 pulgadas (es decir, 12 x 12 mm) con, dependiendo del tamaño de píxel, 256 x 256, 512 x 512 ó 1024 x 1024 píxeles activos. En el contexto del presente ejemplo, resultó ser suficiente un sensor de 512 x 512 pixeles. Tales elementos y electrónica de control correspondiente están comercialmente disponibles. Según la técnica, una placa de fibra óptica se inserta preferentemente entre la superficie del sensor y la impresión, a fin de proteger el sensor de la suciedad y los daños mecánicos, sin degradar su rendimiento de resolución óptica.

La primera verificación del artículo así marcado con el sensor CCD se lleva a cabo después de la impresión, y la imagen resultante de micropuntos oscuros se almacena, junto con el número de serie del documento, en la base de datos de la autoridad expedidora. Tras la autenticación por un usuario, el documento se aplica sobre un elemento sensor correspondiente contenido en el equipo de comunicación, y la imagen resultante de micropuntos oscuros se envía, junto con el número de serie del documento, a la base de datos de la autoridad expedidora, donde se

determina el grado de correspondencia con los datos almacenados originalmente mediante un algoritmo, y el resultado de autenticación se devuelve como una respuesta de "Sí" o "No" al usuario.

Nuevamente, el detector para detectar la información de identidad del documento puede ser de cualquier tecnología que se preste a la finalidad: son posibles detecciones de transmisión óptica, luminiscencia, magnética, dieléctrica, radio-frecuencia y otros tipos de detección; además el sensor puede ser del tipo de canal único (escaneado manual), de sistema lineal, de área bidimensional; y el procedimiento de verificación de la identidad puede llevarse a cabo con la introducción manual del número de serie del documento de seguridad, o de una manera totalmente automatizada.

Por consiguiente, la invención se basa preferentemente en un sistema para la autenticación de un artículo, en particular un documento de seguridad, con al menos un marcado. Dicho sistema comprende un dispositivo de comunicación móvil de red de área amplia (WAN), conectado o unido a un dispositivo de autenticación. Dicho marcado refleja o emite radiación electromagnética y/o muestra unas características eléctricas o magnéticas concretas en respuesta a una interrogación por dicho dispositivo de autenticación. Dicho marcado puede contener adicionalmente información lógica, vectorizada a través de dicha radiación o características, y dicha respuesta característica e información lógica son capturadas por dicho dispositivo de autenticación. Dicho sistema comprende además un servidor remoto, que incluye un hardware y un software para establecer un enlace con dicho dispositivo de comunicación móvil a través de una red de área amplia y para intercambiar datos con ella, dichos datos comprendiendo notablemente un software de autenticación y/o datos de autenticación y/o datos de referencia. Dicho servidor remoto también puede llevar a cabo operaciones de autenticación de manera centralizada. Opcionalmente dicho sistema comprende unos medios para encriptar/desencriptar la transferencia de datos entre dicho servidor remoto y dicho dispositivo de comunicación.

La invención se refiere además a un artículo a autenticar, en el que el marcado del artículo está interactuando con el dispositivo de autenticación del equipo de comunicación.

La invención se refiere en particular a un artículo, en el que una pluralidad de al menos un tipo de partículas o escamas autenticables ópticamente se disponen dentro del marcado, formando un patrón aleatorio característico que confiere identidad.

La invención se refiere en particular a un artículo, en el que un código de barras bidimensional o unidimensional invisible se dispone en el marcado, que lleva información lógica característica acerca del artículo.

La invención se refiere en particular a un artículo, en el que un portador de información magnética se dispone dentro del marcado, que lleva información lógica característica acerca del artículo.

La invención se refiere en particular a un artículo que lleva un marcado de seguridad láser, que comprende información lógica característica acerca del artículo.

La invención se refiere en particular a un artículo que lleva un transpondedor de radiofrecuencia, que comprende información lógica característica acerca del artículo.

Es fácil para los expertos en la materia concebir otras modificaciones según las cuales puede realizarse la invención. Estos pueden incluir notablemente el uso de un equipo de comunicación móvil diferente de los teléfonos móviles, dado que dicho equipo tiene una capacidad de procesamiento y almacenamiento de datos, comunicación inalámbrica, y entrada-salida de interfaz de usuario y de máquina. Estas formas de realización incluyen adicionalmente el uso de otros accesorios sensores, tales como lectores de códigos de barras en forma de lápiz, escáneres láser o unidades de procesamiento de imágenes externas. Estas formas de realización incluyen adicionalmente el uso de otros accesorios sensores, como lectores de códigos de barras con forma de lápiz, escáneres láser, o unidades de obtención de imágenes externas. Estas variantes también incluyen el aprovechamiento de otros efectos físicos además de los mencionados como características que confieren seguridad característica. Tales efectos pueden incluir notablemente absorción UV magnetostricción, efecto Barkhausen, resonancia de RF o de microondas, propiedades dieléctricas, y demás.

REIVINDICACIONES

1. Procedimiento para la autenticación de un artículo, en particular un documento de seguridad, que comprende al menos un marcado, con la ayuda de un dispositivo de comunicación móvil seleccionado del grupo que consiste en teléfonos móviles, ordenadores de mano, y agendas electrónicas, en el que el dispositivo de comunicación móvil se acopla a un capturador de datos de autenticación seleccionado del grupo que consiste en un detector de radiación electromagnética, un escáner, una cámara CCD o CMOS, y un detector de propiedad magnética, dicho procedimiento comprendiendo las etapas de:

(a) detectar una señal de respuesta, que es emitida por dicho marcado en respuesta a una energía aplicada, utilizando dicho capturador de datos de autenticación y un algoritmo de medición;
(b) correlacionar dicha señal de respuesta detectada con datos de referencia;
(c) generar un resultado de autenticación utilizando un algoritmo de autenticación y los datos de referencia;
(d) generar una señal de salida representativa de dicho resultado de autenticación; en el que dicho procedimiento comprende las etapas preliminares de:
(e) descargar un algoritmo de autenticación y de medición desde un servidor remoto o una base de datos a la memoria de dicho dispositivo de comunicación móvil;
(f) descargar datos de referencia desde un servidor remoto a la memoria de dicho dispositivo de comunicación móvil.
en el que el algoritmo de medición, el algoritmo de autenticación y los datos de referencia se corresponden con el capturador de datos de autenticación seleccionado y el marcado del artículo a autenticar.

2. Procedimiento según la reivindicación 1, en el que:

(a) dicho marcado se activa por exposición a energía, preferentemente a radiación electromagnética y/o campos eléctricos o magnéticos, procedentes de dicho capturador de datos de autenticación;
(b) dicha señal de respuesta detectada es radiación electromagnética y/o características eléctricas o magnéticas emitidas o reflejadas por dicho marcado en respuesta a dicha energía.

3. Procedimiento según la reivindicación 1 ó 2, que comprende:

subir la señal de respuesta detectada a un servidor remoto para la autenticación;
autenticar dicha señal de respuesta detectada en dicho servidor remoto, utilizando un algoritmo de autenticación correspondiente y datos de referencia correspondientes, produciendo así un resultado de autenticación; y
descargar el resultado de autenticación del servidor remoto al dispositivo de comunicación móvil.

4. Procedimiento según la reivindicación 3, en el que dicha descarga y/o subida se lleva a cabo utilizando una conexión encriptada segura.

5. Procedimiento según una de las reivindicaciones 1 a 4, en el que dicho marcado comprende al menos un material seleccionado del grupo que consiste en un material magnético, un material luminiscente, un material que absorbe los infrarrojos, un material resonante de radiofrecuencia o en el que dicho marcado comprende un patrón de escamas o partículas característico.

6. El procedimiento según una de las reivindicaciones 1 a 5, en el que dicha señal de respuesta detectada también comprende información que está incluida en dichas características físicas y por consiguiente es legible.

7. Unidad para la autenticación de un artículo, en particular un documento de seguridad, que comprende al menos un marcado, dicho marcado mostrando un comportamiento físico característico en respuesta a una energía de activación, preferentemente radiación electromagnética y/o campos eléctricos o magnéticos, dicha unidad comprendiendo:

(a) un dispositivo de comunicación móvil seleccionado del grupo que consiste en teléfonos móviles, ordenadores de mano, y agendas electrónicas, y con capacidades de procesamiento y almacenamiento de datos, capacidades de transferencia de datos, capacidades de interfaz de usuario, y capacidades de interfaz de máquina;
(b) un capturador de datos de autenticación seleccionado del grupo que consiste en un detector de radiación electromagnética, un escáner, una cámara CCD o CMOS, y un detector de propiedad magnética, y acoplado a dicho dispositivo de comunicación móvil, dicho capturador de datos de autenticación comprendiendo un dispositivo para producir dicha energía de activación y para detectar dicho comportamiento físico característico de dicho marcado,
(c) dicho dispositivo de comunicación móvil comprendiendo hardware y/o software para conectar dicho dispositivo de comunicación móvil a un servidor remoto que contiene software de autenticación y datos de referencia de autenticación,

(d) opcionalmente hardware y/o software para encriptar la transferencia de datos entre dicho dispositivo de comunicación y dicho servidor remoto;
(e) medios adaptados para la descarga de un algoritmo de autenticación y de medición desde el servidor remoto o una base de datos a la memoria de dicho dispositivo de comunicación móvil;
(f) medios adaptados para descargar datos de referencia desde el servidor remoto a la memoria de dicho dispositivo de comunicación móvil,

en el que el algoritmo de medición, el algoritmo de autenticación y los datos de referencia se corresponden con el capturador de datos de autenticación seleccionado y el marcado del artículo a autenticar.

8. La unidad para la autenticación de la reivindicación 7, en la que el capturador de datos de autenticación se acopla al dispositivo de comunicación móvil a través de una conexión por cable a un puerto, o un radioenlace de corto alcance, o un enlace de infrarrojos de corto alcance.

9. La unidad para la autenticación de la reivindicación 7, en la que el capturador de datos de autenticación está integrado en el dispositivo de comunicación móvil.

10. La unidad para la autenticación de la reivindicación 7, en la que el capturador de datos de autenticación comprende un sistema óptico de obtención de imágenes basado en el modo de obtención de imágenes de copia por contacto (Fig. 3a).

11. Sistema para la autenticación de artículos, en particular un documento de seguridad, que comprende al menos un marcado, dicho marcado mostrando un comportamiento físico característico en respuesta a una energía de activación, preferentemente radiación electromagnética y/o campos eléctricos o magnéticos, dicho sistema comprendiendo:

(a) una unidad para la autenticación de acuerdo con cualquiera de las reivindicaciones 7 a 10;
(b) un servidor remoto que comprende hardware y/o software para comunicarse con dicha unidad para la autenticación, un software de autenticación, y/o datos de referencia de autenticación.

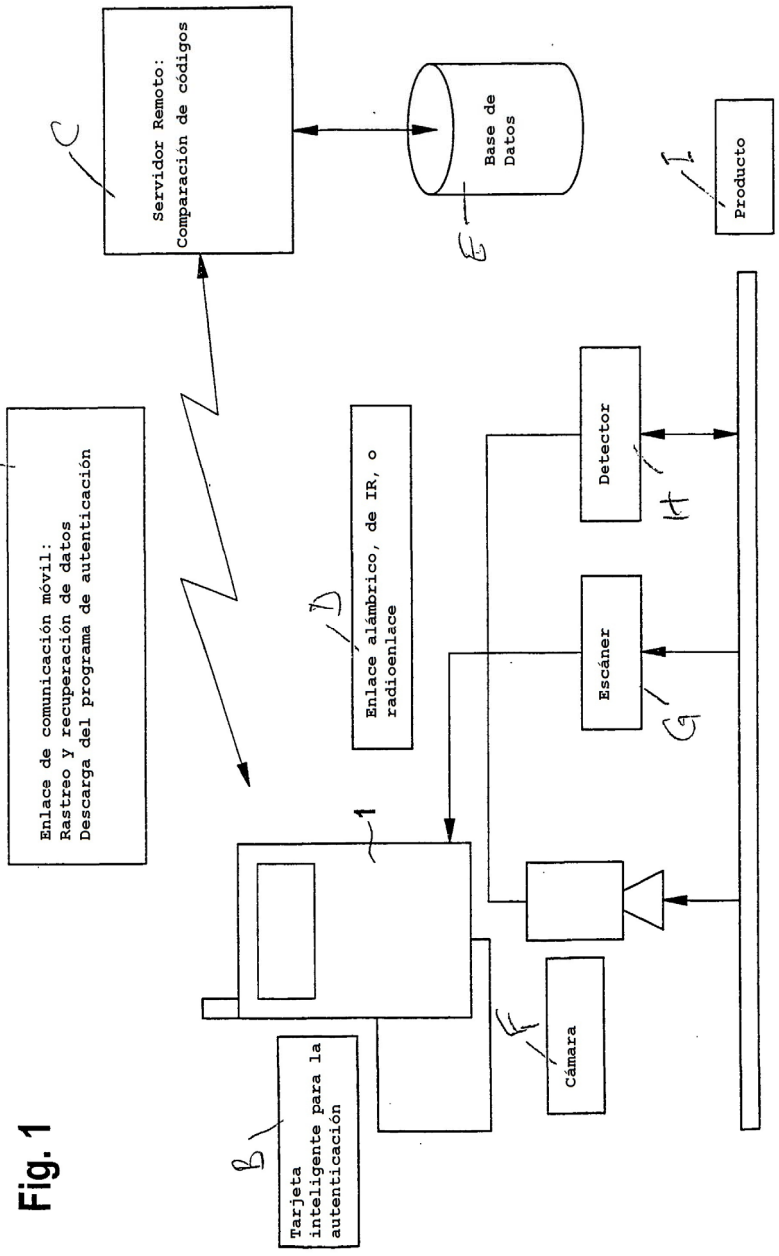
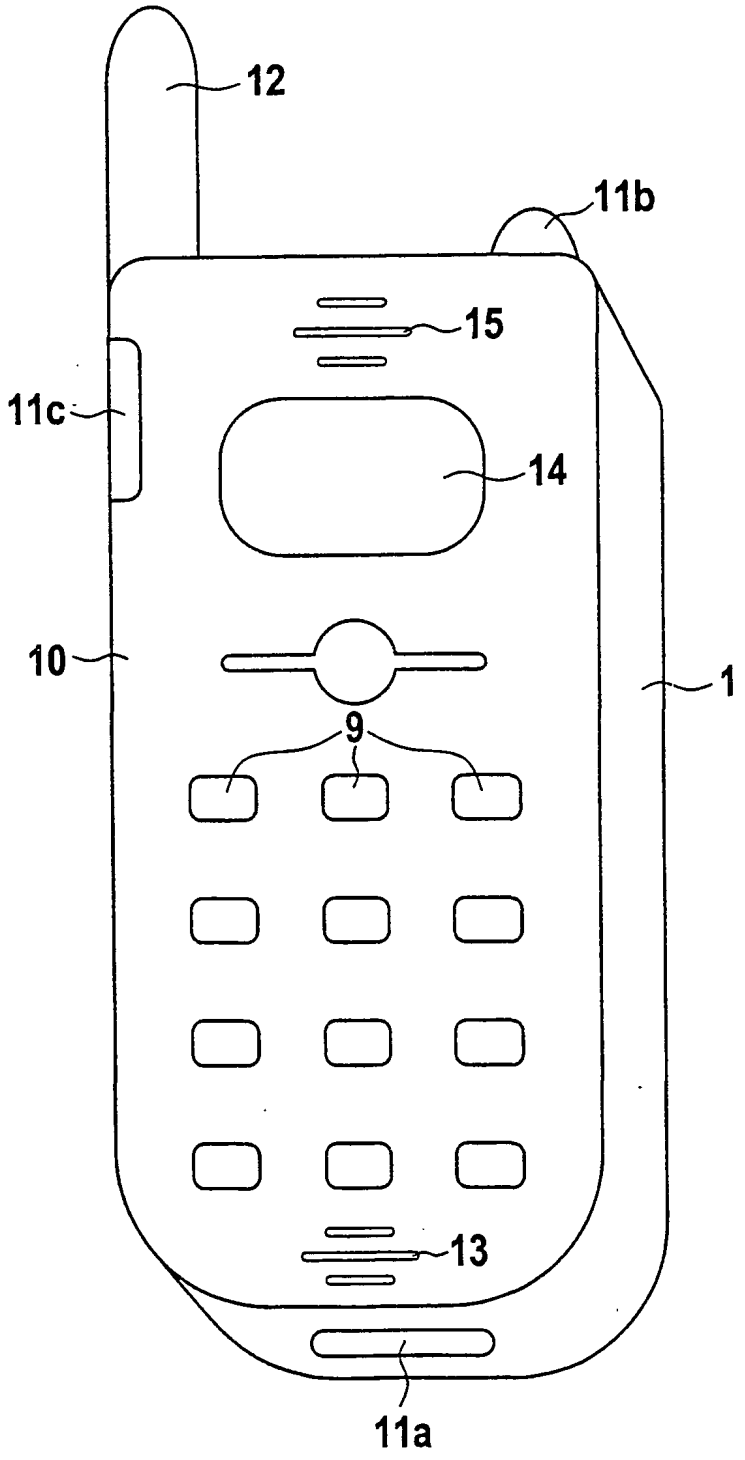

Servidor Remoto:
Comparación de códigos
C
Base de Datos
E
Producto
I
Enlace de comunicación móvil:
Rastreo y recuperación de datos
Descarga del programa de autenticación
A
Enlace alámbrico, de IR, o radioenlace
D
Detector
H
Escáner
G
1
Cámara
F
Tarjeta inteligente para la autenticación
B

Fig. 1

Fig. 2



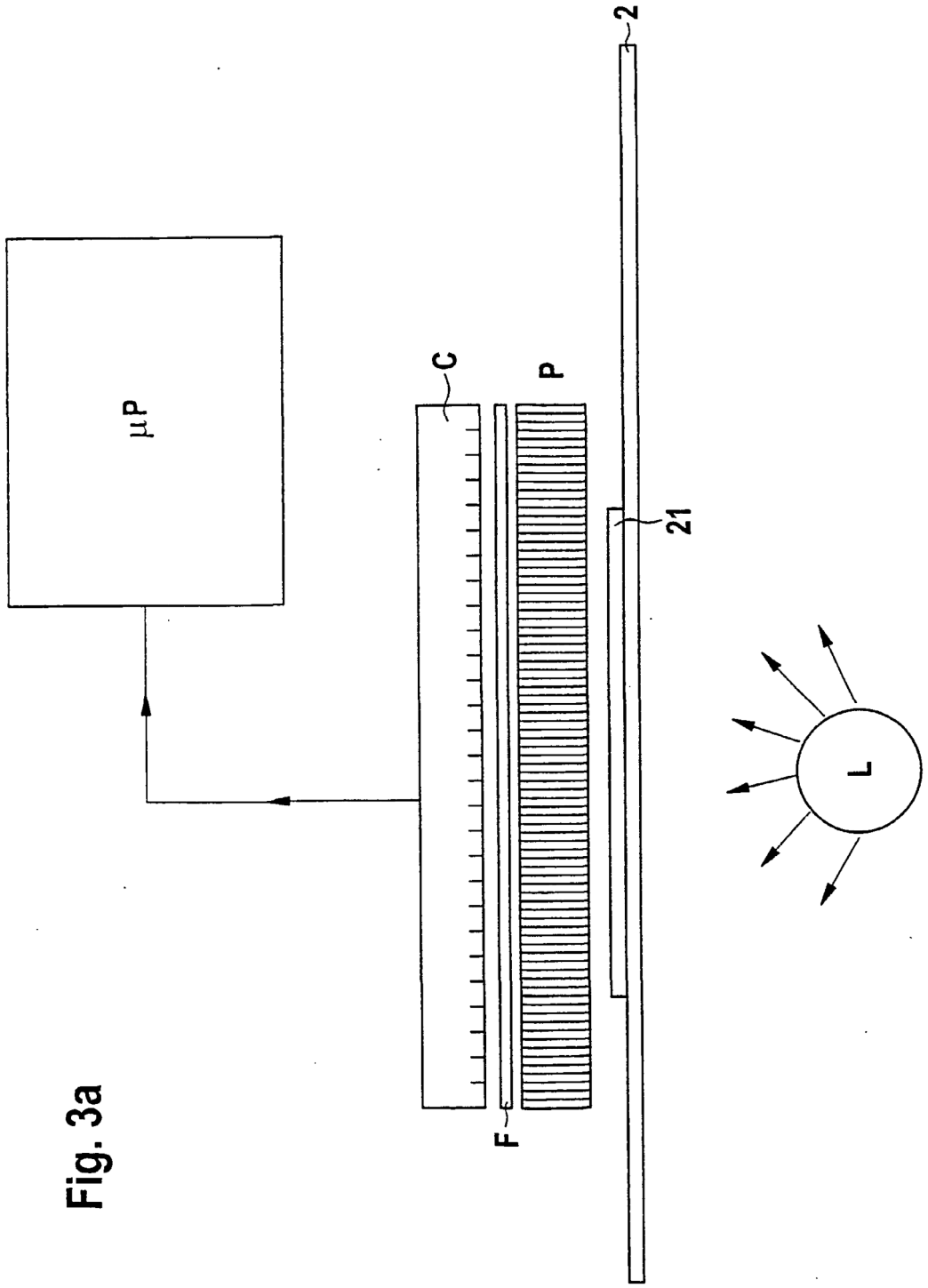


Fig. 3a

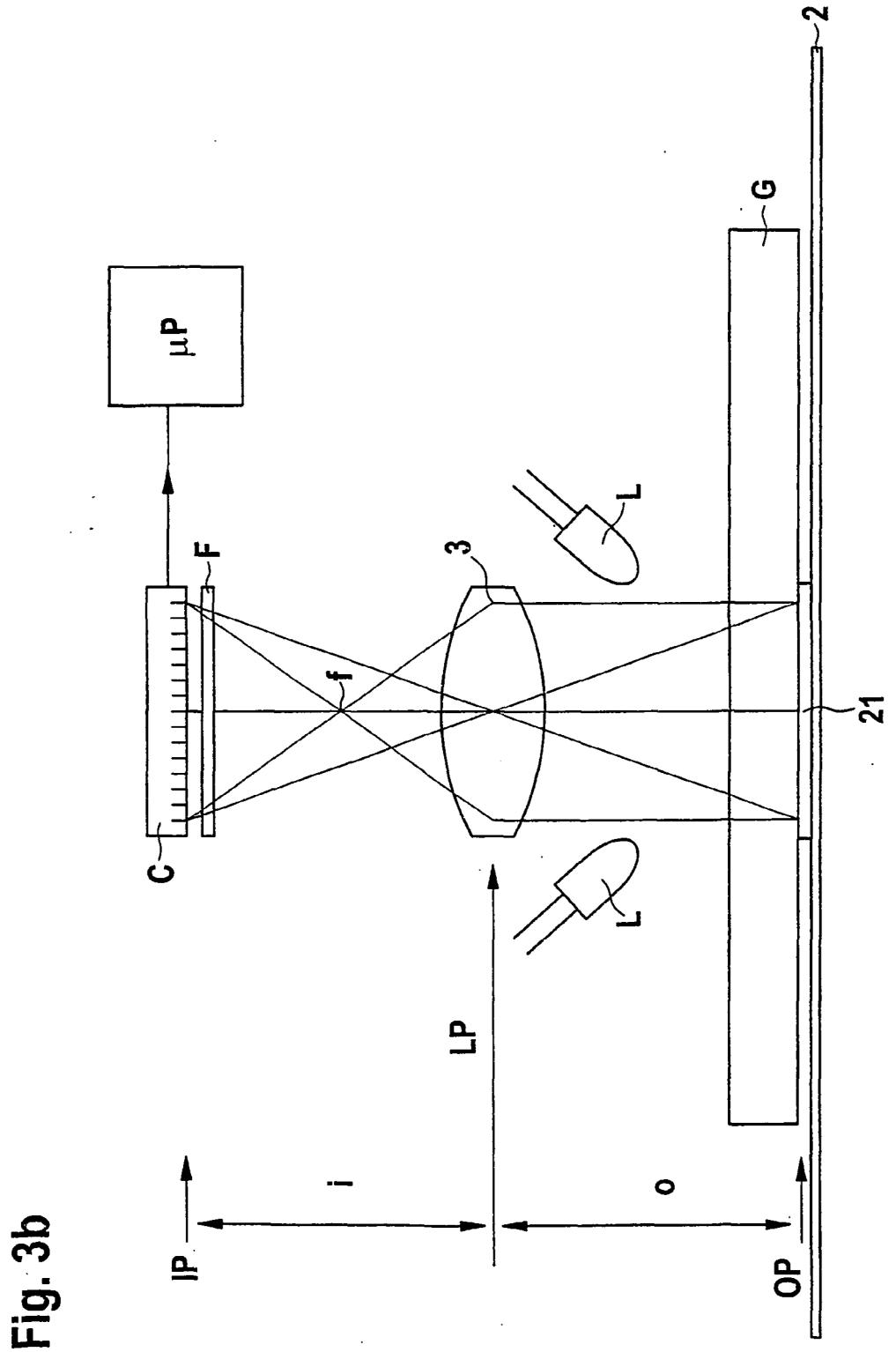


Fig. 3b

Fig. 3c

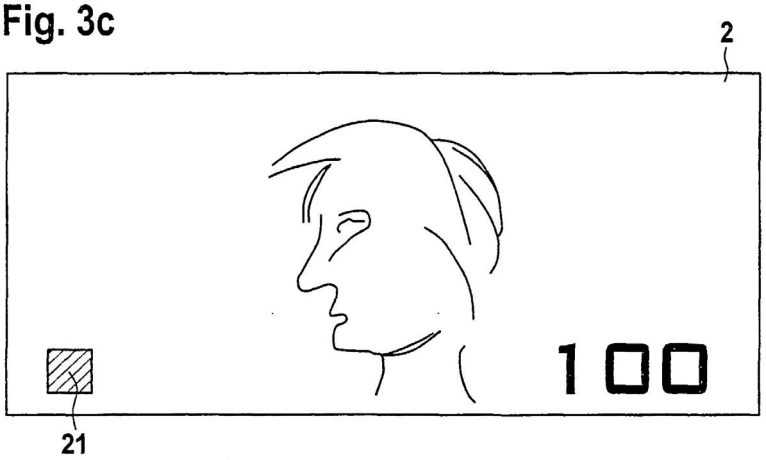


Fig. 4