(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 613 677**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/04 (2009.01)
H04L 9/08 (2006.01)
H04L 29/08 (2006.01)
H04L 9/32 (2006.01)
G06Q 20/32 (2012.01)
H04W 4/02 (2009.01)
H04W 64/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **23.01.2014 PCT/EP2014/051297**

(87) Fecha y número de publicación internacional: **31.07.2014 WO2014114699**

(96) Fecha de presentación y número de la solicitud europea: **23.01.2014 E 14701962 (4)**

(97) Fecha y número de publicación de la concesión europea: **21.12.2016 EP 2949096**

(54) Título: **Facilitación de los datos de posición mediante un protocolo de delimitación de distancia**

(30) Prioridad:

25.01.2013 DE 102013201245
04.02.2013 DE 102013201730

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.05.2017

(73) Titular/es:

BUNDESDRUCKEREI GMBH (100.0%)
Oranienstrasse 91
10969 Berlin, DE

(72) Inventor/es:

MORGNER, FRANK

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Facilitación de los datos de posición mediante un protocolo de delimitación de distancia

La invención se refiere a un procedimiento para la facilitación segura de los datos de posición de una unidad de localización a una tarjeta inteligente, así como una tarjeta inteligente correspondiente, una unidad de localización correspondiente y un producto de programa informático.

En el estado de la técnica se conocen procedimientos para la determinación fiable de la distancia espacial entre dos unidades o equipos separados físicamente. En particular el documento US 2011/0078549 A1 muestra un equipo lector para la determinación de la validez de una conexión con un transpondedor, que está diseñado para medir un tiempo de respuesta del transpondedor y autentificar el transpondedor en dos etapas separadas. Además, el documento da a conocer un transpondedor para la determinación de la validez de una conexión con un equipo lector, en donde el transpondedor está diseñado para facilitarle informaciones al equipo lector para la medición del tiempo de respuesta y para la autentificación en dos etapas separadas, en donde al menos una parte de los datos para la autentificación se transmite en un mensaje de comunicación entre el equipo lector y el transpondedor durante la medición del tiempo de respuesta.

Además, en el estado de la técnica se conocen distintos sistemas para la geolocalización de objetos móviles o para la facilitación de los datos de geolocalización. No obstante, los sistemas usados actualmente tienen la desventaja de que, por ejemplo, las informaciones GPS proceden de sensores que no se sitúan bajo el control de la tarjeta inteligente. Los datos de geolocalización no son fiables, ya que podrían proceder de otro sensor GPS, puesto más alejado, o haber sido falseados por un tercero ("man in the middle attack [ataque de intermediario]"). Los sistemas de geolocalización usados actualmente no están protegidos así frente a falsificaciones de los datos de posición transmitidos o frente a que una señal de un sensor "engañoso", que transmite indicaciones de posición erróneas, se superponga a la señal de sensor previsto realmente para el uso.

Finalmente por el estado de la técnica se conocen aplicaciones para el uso de los datos de geolocalización con las finalidades de la planificación y realización de viajes. En particular el documento US 2010/0280748 A1 da a conocer una planificación de rutas para un usuario con etapas para la determinación de un punto de inicio y de un punto objetivo para viajes multimodales, aplicación de criterios para la limitación del número de rutas candidatas en la base al punto de partida y objetivo, propuestas de una lista actualizada de las rutas candidatas entre el punto de partida y el punto objetivo, en donde se muestra la lista actualizada tras un retraso de forma automática y/o a una selección del usuario sobre la base de los criterios. En una configuración del procedimiento se procesan aquí los datos para la geolocalización del usuario.

Otro estado de la técnica se encuentra en los documentos EP2051475A2 y EP2247024A1.

Ante estos antecedentes se plantea el objetivo de procurarle a los datos de posición, que una tarjeta inteligente deriva de una fuente externa, la misma posición de confianza que le corresponde a los datos almacenados en la tarjeta inteligente.

Este objetivo se consigue respectivamente con las características de las reivindicaciones independientes. Configuraciones y perfeccionamientos preferidos están indicados en las respectivas reivindicaciones dependientes. Si no se pone de manifiesto expresamente lo contrario, las formas de realización de la invención se pueden combinar entre sí libremente.

Bajo un "chip" o "microchip" se entiende en cuestión un circuito integrado, que puede contener varios componentes electrónicos o elementos de circuito como transistores, resistencias, etc. Según la forma de realización un chip puede formar parte de ordenadores, móviles, en particular smarphones, cámaras digitales u otros equipos, preferentemente portátiles. Según algunas formas de realización el chip es componente de un documento, en particular de un documento de seguridad.

Como "tarjeta inteligente" o "documento" se designa en cuestión aquel soporte de datos, que presenta un microchip y una interfaz de comunicación unida con él, eléctricamente en contacto o sin contacto. Una interfaz sin contacto puede estar configurada en particular como antena para una transmisión de señales inalámbrica. Preferentemente la tarjeta inteligente puede intercambiar datos con un equipo lector apropiado. En el caso de la tarjeta inteligente se puede tratar de un documento de valor o de seguridad, como por ejemplo de un documento ID. Un documento ID pude ser, por ejemplo, un documento de identidad, en particular un carné de identidad, un pasaporte, un carné de conducir, un permiso de circulación, una documentación del vehículo o una tarjeta de empresa. En el caso del documento de valor se puede tratar de un medio de pago, en particular un billete de banco o una tarjeta de crédito. El documento también puede ser otra tarjeta de autorización, por ejemplo, una tarjeta de entrada, un billete de transporte, en particular un tique electrónico, una carta de porte o un visado. El cuerpo de documento del documento puede estar configurado de tipo libro, tal y como es el caso, por ejemplo, en algunos pasaportes.

Bajo una tarjeta inteligente también se entiende una así denominada etiqueta inteligente, que también se designa como tag RFID o etiqueta RFID. La tarjeta inteligente contiene preferentemente una interfaz para el intercambio de

datos sin contacto con el equipo lector. Según la forma de realización la tarjeta ejemplo en plástico y/o papel.

Bajo un "equipo lector" se entiende en cuestión un equipo de procesamiento de datos, que puede intercambiar datos con la tarjeta inteligente, a fin de autentificar la tarjeta inteligente o posibilitarle a la tarjeta inteligente el autenticarse en el equipo lector. Según las formas de realización, el equipo lector puede presentar una función criptográfica para la firma y/o autentificación respecto a la tarjeta inteligente, una función de pago u otra función para la realización de una transacción financiera, una función de identificación, en particular con reproducción de imágenes en un dispositivo de visualización. En particular el equipo lector puede implementar funcionalidades tal y como se conocen para equipos lectores de documentos de viaje legibles a máquina (MRTD), en particular protocolos criptográficos, como por ejemplo control de acceso básico (Basic Access Control, BAC) y/o control de acceso extendido (Extended Access Control, EAC). Según algunas formas de realización, el equipo lector puede estar configurado para leer los datos del documento.

En algunos escenarios de aplicación es necesario garantizar que sólo un equipo lector autorizado pueda acceder a los datos almacenados en la tarjeta inteligente, de modo que el equipo lector se debe autenticar antes de la lectura de estos datos respecto a la tarjeta inteligente. Preferentemente la autentificación contiene la confirmación de que el propietario de la tarjeta inteligente le ha puesto a disposición al equipo lector la tarjeta inteligente de forma intencionada para la lectura de los datos. Esto puede ocurrir, por ejemplo, porque el equipo lector le ha transmitido a la tarjeta inteligente datos, que eran visibles sobre la superficie de la tarjeta inteligente y se han detectado ópticamente por el equipo lector, como comprobación de que el usuario le ha mostrado la tarjeta inteligente (y los datos situados en ella y registrables ópticamente) al equipo lector de forma intencionada. Alternativamente también se puede usar un secreto introducido por el usuario en el equipo lector para la autentificación del equipo lector respecto a la tarjeta inteligente.

Bajo "datos de posición" se deben entender en cuestión aquellos datos que posibilitan una ubicación, es decir, localización, de un objeto determinado y en particular del sensor que ha determinado los datos de posición, en referencia a un punto fijo definido o un sistema de referencia definido de otra forma. En particular en el caso de los datos de posición se puede tratar de los datos que se han obtenido mediante la localización por radio y satélite, es decir, en particular de datos GPS (sistema de posicionamiento global), pero también de datos que se han obtenido mediante métodos de medida geodésicos (trilateración, angulación, método polar) u otros procedimientos (reconocimiento óptico del territorio, ecolocalización). Los datos de posición pueden estar especificados, por ejemplo, como coordenadas planares, coordenadas cúbicas, coordenadas polares o coordenadas geográficas, naturales o en un formato específico de la aplicación, por ejemplo como identificador de lugar o red. En el caso de los datos de posición se puede tratar así de identificaciones de redes u otros objetos o emisores de señales, que posibilitan de forma individual o en combinación una determinación de la posición del sensor.

Bajo una "unidad de localización" se entiende a continuación un equipo o un componente de equipo que es capaz de detectar automáticamente la propia posición. La posición propia es específica en forma de datos de posición y se puede determinar por la unidad de localización, por ejemplo automáticamente a intervalos regulares y/o tras recibir una petición de otro equipo, por ejemplo por la tarjeta inteligente, y se le puede enviar a éste.

Bajo una tarjeta inteligente, que está "separada espacialmente" de una unidad de localización, se entiende en cuestión una tarjeta inteligente que no contiene la unidad de localización como uno de sus componentes. La separación espacial puede ser, por ejemplo, de al menos 10 cm, según otras formas de realización por encima de 100 cm.

Bajo la transmisión de datos usando un protocolo criptográfico se entiende a continuación una transmisión de los datos en forma encriptada, por ejemplo mediante clave asimétrica o simétrica.

El término "protocolos de delimitación de distancia" designa en cuestión los protocolos criptográficos que proporcionan un indicio real suficientemente difícil de falsificar de que la distancia espacial de dos unidades físicas no sobrepasa una distancia máxima predeterminada. Los protocolos de delimitación de distancia usuales se basan en que una de las unidades físicas le envía un desafío a la otra y gracias al intervalo de tiempo hasta la recepción de una respuesta puede calcular a qué distancia se puede situar físicamente la unidad física que responde como máximo a lo largo del recorrido de transmisión seleccionado. En este cálculo entran magnitudes conocidas, como por ejemplo la velocidad de la transmisión de datos en la respectiva tecnología de transmisión de datos usada (velocidad de la luz con radio, velocidad del sonido con ultrasonidos) y preferentemente también el tiempo de procesado para la generación y para el envío de la respuesta. Mediante la duración entre el envío del desafío hasta la recepción de la respuesta se puede determinar una estimación de la distancia espacial entre las unidades físicas y con ello también si ésta sobrepasa o no una distancia máxima predeterminada. En el caso de un protocolo de delimitación de distancia se puede tratar, por ejemplo, de un procedimiento de desafío - respuesta. Por ejemplo, para los protocolos de delimitación de distancia se menciona, p. ej. en Gerhard Hanek, Markus Kuhn: "*An RFID distance-bounding protocol*", procedente de SecureComm 2005 y en Stefan Brands, David Chaum: "*Distance-bounding protocols (extendes abstract)*" procedente de Eurocrypt ‘93.

Una "autentificación" de una unidad de localización respecto a una tarjeta intelig
de una comprobación (de fecha verificable) de una propiedad pretendida de la unidad de localización respecto a la tarjeta inteligente ("autenticación") en combinación con el examen de esta comprobación y aceptación de la autenticidad de la propiedad pretendida por parte de la tarjeta inteligente (autentificación en el sentido más estricto). Mientras que una autenticación se refiere así a las etapas que se deben realizar por la unidad de localización, el término de la "autentificación en el sentido más estricto se refiere a las etapas que se deben realizar por la tarjeta inteligente, "autentificación" en general sobre todo el proceso.

En un aspecto la invención se refiere a un procedimiento para la facilitación de los datos de posición a una tarjeta inteligente. El procedimiento comprende una sección para la recepción o para la determinación de los datos de posición de una unidad de localización por la unidad de localización, en donde la unidad de localización está separada espacialmente de la tarjeta inteligente. En el caso de la unidad de localización se puede tratar, por ejemplo, de un sensor GPS o, por ejemplo, de un equipo que está integrado en un vehículo, por ejemplo autobús o tren, y recibe un identificador de una parada actual de, por ejemplo, un puesto central de planificación del tráfico, el conductor del vehículo u otra instancia. Además, el procedimiento comprende una sección para la transmisión de los datos de posición de la unidad de localización a la tarjeta inteligente a través de una interfaz sin contacto usando un protocolo criptográfico Además, el procedimiento comprende una sección para la ejecución de un protocolo de delimitación de distancia entre la tarjeta inteligente y la unidad de localización, en donde el protocolo de delimitación de distancia concluye satisfactoriamente precisamente luego cuando la distancia espacial entre la tarjeta inteligente y la unidad de localización no sobrepasa una distancia máxima predeterminada. Finalmente el procedimiento prevé, en el caso de la conclusión satisfactoria del protocolo de delimitación de distancia, la ejecución de una función de tarjeta inteligente, en donde la función de tarjeta inteligente usa los datos de posición determinados como datos de posición que especifican la posición actual de la tarjeta inteligente.

El procedimiento puede ser ventajoso dado que los datos de posición transmitidos se pueden transmitir de modo y manera especialmente seguros. Mediante el uso de un protocolo criptográfico se impide la lectura o una manipulación dirigida de los datos transmitidos. Con ello el protocolo de delimitación de distancia garantiza que los datos de posición recibidos también proceden realmente de una unidad de localización cuya distancia de la tarjeta inteligente es menor o igual a la distancia máxima. Así no es posible que un "emisor interferente, que está a mayor distancia y lo compensa, por ejemplo, con una intensidad de señal más elevada, manipule la tarjeta inteligente mediante la transmisión de datos de posición falsos durante su funcionamiento. También es ventajoso el uso de un protocolo de delimitación de distancia para el aseguramiento de la proximidad espacial y por consiguiente de la credibilidad de la unidad de localización, dado que la unidad de localización se puede usar por una multiplicidad de tarjetas inteligentes de diferentes fabricantes, funciones y oferentes de servicios referidos a la tarjeta inteligente. No es necesario que, por ejemplo, para las tarjetas inteligentes de pago y tarjetas inteligentes de sistemas de peaje se coloque respectivamente una unidad de localización propia adaptada especialmente a la tarjeta inteligente correspondiente. La condición previa es sólo que la tarjeta inteligente y la unidad de localización realicen de forma interactiva un protocolo de delimitación de distancia y puedan intercambiar los datos de posición.

Según las formas de realización, la distancia máxima examinada durante el protocolo de delimitación de distancia se configura al estar en el fabricante de la tarjeta inteligente o durante la inicialización específica al cliente de la tarjeta inteligente o en un instante cualquiera posterior por parte de un usuario, un programa de tarjeta inteligente o editor de la tarjeta inteligente. Según el escenario de aplicación e intensidad de señal de la unidad de localización, la distancia máxima puede ser de uno o varios centímetros, pero también hasta varios metros.

Según las formas de realización, la tarjeta inteligente es una tarjeta SIM o una tarjeta inteligente de un documento de seguridad. La unidad de localización puede determinar los datos de posición, por ejemplo, mediante GPS, LPS, WLAN, ultrasonidos, tecnología de radio o Bluetooth. El protocolo de delimitación de distancia se puede basar, por ejemplo, en ultrasonidos o radiación electromagnética, en particular microondas, ondas de radio, luz visible o luz infrarroja.

Por ejemplo, una tarjeta inteligente, que se usa como medio de pago para el uso en medios de transporte públicos, podría contener unos ficheros de configuración con una distancia máxima examinada, que sea suficientemente pequeña para poder distinguir entre diferentes estaciones. La distancia máxima examinada puede ser así de varios metros, eventualmente también varios cientos de metros. No obstante, si la tarjeta inteligente se debe usar en combinación con la unidad de localización, para identificarse por ejemplo en una caja y activar su cuenta para el pago, se requiere una elevada resolución para excluir una confusión con otra persona en la cola de espera.

Según las formas de realización, la distancia máxima se predetermina por el protocolo de delimitación de distancia. Según algunas formas de realización, la distancia máxima está almacenada en una configuración en la tarjeta y se puede editar por el usuario y/o diferentes aplicaciones de la tarjeta inteligente o cambiarse a otro valor. Esto puede ser ventajoso ya que la tarjeta inteligente se puede usar mediante reconfiguración para una multiplicidad de escenarios de aplicación.

Según las formas de realización, el procedimiento comprende además una autentificación de la unidad de localización respecto a la tarjeta inteligente. A este respecto, se requiere una autentificación satisfactoria para la ejecución de la función de tarjeta inteligente. La autentificación se puede realizar, por ejemplo, mediante un

protocolo criptográfico, como por ejemplo PACE. La autentificación también se mediante la realización del protocolo de delimitación de distancia y la constatación de que la unidad de localización se sitúa a una distancia de la tarjeta inteligente igual o menor que la distancia máxima. Una realización "satisfactoria" del protocolo de delimitación de distancia provoca así una autentificación de la unidad de localización respecto a la tarjeta inteligente. Esto puede acelerar el procedimiento, dado que ya la ejecución satisfactoria del protocolo de delimitación de distancia sirve para la autentificación y no se requieren otras etapas de intercambio de datos entre la tarjeta inteligente y unidad de localización.

Según las formas de realización, el protocolo de delimitación de distancia se basa en un protocolo de desafío - respuesta.

Según las formas de realización, tanto la tarjeta inteligente como también la unidad de localización poseen una memoria protegida en la que están almacenadas una o varias claves criptográficas. La memoria protegida protege la clave frente a una lectura no autorizada. En el caso de las claves se puede tratar de claves simétricas o asimétricas, en particular de claves privadas de un par de claves asimétricas. Las claves mencionadas se usan para transmitir los datos de posición en base al protocolo criptográfico, es decir, de forma codificada. Las claves necesarias para la realización del protocolo de delimitación de distancia también pueden estar almacenadas en las memorias protegidas. Preferentemente el nivel de seguridad de la memoria de la tarjeta se corresponde con el nivel de seguridad de la memoria de la unidad de localización.

Según las formas de realización, la ejecución del protocolo de delimitación de distancia prevé el uso al menos de una primera y una segunda clave criptográfica. La primera clave criptográfica está almacenada de forma segura en un primer medio de almacenamiento protegido de la tarjeta inteligente. La segunda clave criptográfica está almacenada en un segundo medio de almacenamiento protegido de la unidad de localización.

Según las formas de realización, los datos de posición comprenden una multiplicidad de identificador de lugar, que identifican en su globalidad un lugar en donde se sitúa la unidad de localización. Alternativamente a ello los datos de posición comprenden un identificador de lugar, que identifica un lugar en donde se sitúa la unidad de localización. Un lugar de este tipo puede ser, por ejemplo, un territorio geográfico, por ejemplo, una ciudad, un distrito, un edificio, un cuarto dentro de un edificio o también una zona espacial.

Según las formas de realización, cada identificador de lugar de la multiplicidad de identificadores de lugar representa un identificador de red. Cada identificador de red identifica una red de comunicación de datos en cuya área de emisión se sitúa la unidad de localización que determina estos datos de posición. En el caso de la red de comunicación de datos se puede tratar, por ejemplo, de redes WLAN de hogares privados y/o instituciones públicas. Alternativamente a ello también se puede tratar de áreas de emisión de distintos radioemisores, cuyos identificadores de red puede detectar la unidad de localización. Por ejemplo, el sistema de radiodifusión de datos (Radio Data System, RDS) posibilita la transmisión de informaciones adicionales a través de la red de radio. Estas informaciones adicionales pueden contener en particular el nombre del servicio de programa (PS) que indica el nombre del emisor en forma de hasta 8 caracteres alfanuméricos. El nombre de la red WLAN dado individualmente o el nombre de emisor PS puede servir aquí respectivamente como identificador de red.

En combinación con una tarjeta geográfica, en la que está contenidos los territorios de las redes individuales, inclusive sus áreas de superposición, es posible así reconocer mediante uno o varios identificadores de red un determinado lugar geográfico o un territorio geográfico y determinar su identificador de lugar. A este respecto, la tarjeta puede estar almacenada en la unidad de localización o la tarjeta inteligente o en un ordenador alejado al que tiene acceso la tarjeta inteligente o unidad de localización. Alternativamente a la tarjeta también se puede usar una tabla de asociación, que a cada combinación de identificadores de red le asigna un identificador de lugar. A este respecto, un identificador de lugar es un identificador de un lugar o territorio determinado.

Según las formas de realización, el procedimiento comprende además una determinación de un identificador de lugar mediante la multiplicidad de identificadores de lugar. La determinación se puede realizar por parte de la tarjeta inteligente con la ayuda de una tarjeta o una tabla de asociación. Alternativamente a ello la determinación también se puede realizar por la unidad de localización, en donde la unidad de localización tiene al menos acceso de lectura a la tarjeta geográfica o la tabla de asociación, que están almacenadas en una memoria que está acoplada de forma operativa con la unidad de localización. La expresión "acoplada de forma operativa con la unidad de localización" designa un medio de almacenamiento que forma parte integral de la unidad de localización o que está conectado con la unidad de localización a través de una red. A este respecto, la unidad de localización tiene al menos acceso de lectura a los datos del medio de almacenamiento.

Por ejemplo, la determinación del identificador de lugar se puede realizar a partir de varios identificadores de red de la siguiente manera: la unidad de localización se sitúa en un territorio dentro del que se pueden recibir las señales de radio de los emisores S1, S4 y S5 con una intensidad de señal que se sitúa por encima de un valor umbral predeterminado. No obstante, las señales de otros radioemisores, como por ejemplo S3 o S455 no se reciben en este territorio o no con intensidad suficiente. La unidad de localización puede haber almacenado una tarjeta geográfica o una tabla de asociación, la cual asocia a una combinación determinada de identificaciones de red {S1, S4 y S5} exactamente un identificador de lugar ("territorio nº 388"). Este identificador de lugar se determina con la

ayuda de la tarjeta o de la tabla de asociación por parte de la unidad de localizaci
de posición a la tarjeta inteligente. Alternativamente la tarjeta geográfica o la tabla de asociación también se puede situar en un medio de almacenamiento que está acoplado de forma operativa con un servidor remoto. En este caso la unidad de localización le envía una consulta al servidor que contiene los tres identificadores de red S1, S4 y S5. La consulta se puede enviar a través de una red, por ejemplo internet. El servidor determina con ello usando la tarjeta o la tabla de asociación el identificador de lugar y se lo devuelve a la unidad de localización. La unidad de localización le transmite entonces el identificador de lugar a la tarjeta inteligente como los datos de posición. Alternativamente la unidad de localización también le puede enviar los identificadores de red determinados como los datos de posición a la tarjeta inteligente, siempre y cuando la tarjeta inteligente sea capaz de determinar éstos para la determinación de un identificador de lugar (sólo en interoperación con un servidor remoto).

Alternativamente el un identificador de lugar se determina aplicando un robusto algoritmo de mapeo. Un robusto algoritmo de mapeo es, por ejemplo, un robusto algoritmo Hash, sobre indicaciones de lugar "continuas/confusas". Los datos GPS son, por ejemplo, datos de posición con una exactitud limitada determinada. La misma unidad de localización puede suministrar por ello dos datos de posición GPS diferentes, que se desvían ligeramente entre sí, en el caso de una determinación doble de su posición. Mediante el uso de un robusto algoritmo de mapeo, por ejemplo, también en forma de una asignación de los identificadores de lugar no de un valor de datos GPS determinado, sino de un área de datos GPS, se puede posibilitar una derivación de un identificador de lugar unívoco.

Según las formas de realización, la realización de la función de tarjeta inteligente contiene una o varias de las siguientes etapas:

- liberación del medio de almacenamiento protegido de la tarjeta inteligente para posibilitar la lectura de los datos protegidos por la unidad de localización o por otro sistema de procesamiento de datos; en este caso se puede tratar, por ejemplo, de datos personales del usuario para el que se ha personalizado la tarjeta, es decir, por ejemplo datos de dirección, indicaciones de edad, cuentas bancarias o similares; y/o

- registro de los datos de posición con la finalidad de la protocolización de un rastro de movimiento de la tarjeta inteligente; estos protocolos o rastros de movimiento se pueden usar para distintos sectores de uso, como por ejemplo sistemas de peaje, para la protocolización de recorridos de desplazamiento o caminos de marcha, etc.

- realización de una transacción electrónica, en particular de una transacción bancaria; esta puede comprender por ejemplo un pago de productos en una caja, una entrada en un evento, etc.; y/o

- compra electrónica de billete de transporte o elevación automática de un peaje en base a los datos de posición; y/o

- liberación de una funcionalidad bloqueada de un hardware, que está conectado con la tarjeta inteligente de forma operacional. En el caso de la funcionalidad de hardware se puede tratar en particular de:

• un mecanismo para quitar el seguro de un arma de fuego; esto puede ser ventajoso dado que un arma está disponible luego, por ejemplo, sólo en el entorno próximo de uno o varios campos de tiro, que están provistos de una unidad de localización especial; así se puede reducir claramente la posibilidad de un mal uso, en particular de armas de fuego portátiles usadas de forma privada;

• de un mecanismo de desencadenamiento de un dispositivo de explosión;

• un mecanismo para la mezcla de líquidos y/o sustancias; esto puede garantizar, por ejemplo, que las sustancias peligrosas, con tendencia por ejemplo a explosiones, sólo se puedan procesar o mezclar entre sí dentro de zonas especialmente seguras en el entorno de una unidad de localización correspondiente;

• un movimiento mecánico del hardware o de uno de sus componentes, en particular el cierre o apertura de un circuito electrónico o el cierre o apertura de un dispositivo de cierre (puerta, cierre de un recipiente, barrera de acceso a un territorio geográfico, dispositivo de cierre de un componente o de un componente de equipo, etc.) o la emisión de una señal de aviso o accionamiento.

La combinación de un protocolo criptográfico para la transmisión de los datos de posición con un protocolo de delimitación de distancia puede ser especialmente ventajosa, dado que, por un lado, el protocolo criptográfico protege los datos de posición frente a la manipulación y mediante el protocolo de delimitación de distancia se puede conseguir de forma implícita una autentificación de la unidad de localización respecto a la tarjeta inteligente. Una unidad de localización se puede identificar por consiguiente, por ejemplo, como una unidad de localización próxima espacialmente de un tipo especial, por ejemplo, del tipo especial de "unidad de localización de estado de cierre ".

En otro aspecto la invención se refiere a una tarjeta inteligente. La tarjeta inteligente contiene:

- un medio de almacenamiento para el almacenamiento protegido de al menos una clave criptográfica;

- una interfaz sin contacto para la recepción de los datos de posición de una unidad de localización. La recepción se realiza usando un protocolo criptográfico utilizando la al menos una clave criptográfica;

- un módulo de delimitación de distancia (módulo DB), que está configurado pa
delimitación de distancia entre la tarjeta inteligente y la unidad de localización. El protocolo de delimitación de distancia contiene la confirmación por parte de un examinado de que éste se sitúa dentro de una distancia máxima espacial de un examinador. Preferentemente la tarjeta inteligente actúa como el examinador y la unidad de localización como el examinado.

- una función de tarjeta inteligente que sólo se puede ejecutar en el caso de una comprobación satisfactoria de que la unidad de localización se sitúa dentro de la distancia máxima espacial de la tarjeta inteligente. La función de tarjeta inteligente usa los datos de posición transmitidos como datos de posición que indican la posición actual de la tarjeta inteligente.

Según las formas de realización, la tarjeta inteligente comprende además un módulo de autentificación, que está configurado para la autentificación de la unidad de localización. Sólo en el caso de una autentificación satisfactoria de la unidad de localización se usan los datos de posición transmitidos como datos de posición que indican la posición actual de la tarjeta inteligente, por parte de la función de tarjeta inteligente. En algunas formas de realización, el módulo de delimitación de distancia de la tarjeta inteligente también opera simultáneamente como módulo de autentificación, cuando la autentificación se basa en la ejecución satisfactoria del protocolo de delimitación de distancia.

En otro aspecto la invención se refiere a un sistema con una unidad de localización. La unidad de localización comprende:

- un módulo de localización que está configurado para la recepción o determinación de los datos de posición de la unidad de localización;

- un medio de almacenamiento para el almacenamiento protegido de al menos una clave criptográfica;

- una interfaz para la transmisión sin contacto de los datos de posición a una tarjeta inteligente, en donde la transmisión se realiza utilizando un protocolo criptográfico usando la al menos una clave criptográfica;

- un módulo de delimitación de distancia (módulo DB), que está configurado para la ejecución de un protocolo de delimitación de distancia entre la unidad de localización y la tarjeta inteligente. El protocolo de delimitación de distancia concluye satisfactoriamente precisamente luego cuando la distancia espacial entre la unidad de localización y la tarjeta inteligente no sobrepasa una distancia máxima predeterminada.

Según las formas de realización, la unidad de localización comprende además un módulo de autentificación, que está configurado para la autentificación de la unidad de localización respecto a la tarjeta inteligente. En algunas formas de realización, el módulo de autentificación también puede estar personificado en el módulo de delimitación de distancia de la unidad de localización, cuando la autentificación de la unidad de localización respecto a la tarjeta inteligente se basa en la realización satisfactoria del protocolo de delimitación de distancia, es decir, en la comprobación de que la unidad de localización se sitúa dentro de la distancia máxima espacial a la tarjeta inteligente.

Según las formas de realización, el sistema comprende la tarjeta inteligente que está configurada según una de las formas de realización mencionadas arriba o una combinación de las características de formas de realización cualesquiera.

Además, las formas de realización de la invención se explican más en detalle en referencia a los dibujos. Muestran:

Figura 1 un diagrama de bloques de una tarjeta inteligente, de una unidad de localización y de un terminal,

Figura 2 un diagrama de flujo de una forma de realización de un procedimiento según la invención,

Figura 3 un escenario de aplicación para una tarjeta inteligente y unidad de localización según la invención en un sistema de detección de recorrido, y

Figura 4 un escenario de aplicación alternativo para una tarjeta inteligente y unidad de localización según la invención en un sistema de detección de recorrido.

Los elementos de las formas de realización siguientes, que se corresponden entre sí, se caracterizan con las mismas referencias.

La figura 1 muestra una tarjeta inteligente 102 con un medio de almacenamiento 104 protegido. La memoria contiene una o varias claves 120a para la ejecución del protocolo de delimitación de distancia. La memoria puede contener otra clave 138a para la transmisión protegida de los datos de posición de la unidad de localización a la tarjeta inteligente. Además, la memoria protegida puede contener los datos 121, por ejemplo, datos personales de un usuario al que se le asocia la tarjeta inteligente. Los datos se pueden componer, por ejemplo, de informaciones de cuentas del usuario, claves de firmas o similares. La tarjeta inteligente es capaz de realizar un protocolo de delimitación de distancia a través de un módulo 123a en interacción con un módulo 123b correspondiente de la

unidad de localización 130. Además, la tarjeta inteligente posee un procesador función de tarjeta inteligente 110 usando los datos de posición, preferentemente después de una autentificación de la unidad de localización en la tarjeta inteligente. Los datos de posición se determinan por la unidad de localización 130 mediante su módulo de localización 134, por ejemplo un sensor GPS, y se le transmiten a la tarjeta inteligente a través de preferentemente una interfaz sin contacto 118 de la unidad de localización. A este respecto, la transmisión de los datos de posición discurre preferentemente en base a un protocolo criptográfico 114 para garantizar que los datos de posición transmitidos ni se puedan leer ni manipular. Para ello se pueden usar, por ejemplo, claves simétricas 138a, 138b, que están almacenadas respectivamente en un medio de almacenamiento 104, 136 protegido de la tarjeta inteligente o de la unidad de localización. El protocolo de delimitación de distancia a usar, inclusive una distancia máxima predefinida, está almacenado en la tarjeta inteligente. La tarjeta inteligente puede disponer de interfaces correspondientes, que le permiten al usuario de la tarjeta inteligente o a un administrador modificar la distancia máxima que se examina durante la ejecución del protocolo de delimitación de distancia.

Preferentemente la tarjeta inteligente también dispone de una interfaz 108 para intercambiar datos con un equipo lector 124 de un terminal 160. En el caso de la interfaz 108 se puede tratar de una interfaz sin contacto o de una con contacto, que favorecen preferentemente protocolos apropiados (por ejemplo, PACE con una interfaz sin contacto) para la autentificación del equipo lector y/o para la transmisión de datos segura.

La tarjeta inteligente puede estar conectada de forma operativa con un hardware 150, que proporciona una funcionalidad de hardware 152 determinada. Por ejemplo, en el caso del hardware 150 se trata de un arma de fuego portátil que contiene la tarjeta inteligente. En el caso de la funcionalidad de hardware se puede tratar de la liberación de la funcionalidad de disparo de la herramienta. En este caso la función de tarjeta inteligente 110 puede consistir en examinar si una unidad de localización 130 de un campo de tiro se ha autentificado satisfactoriamente en el módulo de autentificación 116 de la tarjeta inteligente y si adicionalmente se han recibido los datos de posición por parte de la unidad de localización, los cuales a través del protocolo de delimitación de distancia proceden de forma fiable de una unidad de localización próxima dentro de la distancia máxima predefinida, de modo que se garantiza que la autentificación también se ha ejecutado realmente por una unidad de localización dentro de la zona protegida de un campo de tiro y por consiguiente la tarjeta inteligente y el arma de fuego portátil también se sitúan dentro de esta zona protegida. En este caso la ejecución de la función de tarjeta inteligente 110 contiene la emisión de una señal al hardware 150 para la liberación de la funcionalidad de tiro. Cuando en la tarjeta inteligente o un servicio interoperable con ésta o servidor que ofrece este servicio están almacenadas las coordenadas de varios campos de tiro, el arma de fuego portátil se puede usar correspondientemente en varios campos de tiro, no obstante, no fuera de una zona protegida semejante.

En el caso del terminal 160 se puede tratar de un sistema de procesado de datos, que es interoperable por sí mismo o en conexión con un servicio o servidor remoto con la tarjeta inteligente. Así, por ejemplo, en el caso del terminal se puede tratar de un terminal de caja, que posee un equipo lector 124 que está configurado para leer los datos ópticos sobre la tarjeta inteligente (por ejemplo con la MRZ - "machine readable zone (zona legible a máquina)" a través de una interfaz óptica, a fin de autentificarse en la tarjeta inteligente y leer los datos 121 del medio de almacenamiento 104 a través de otra interfaz 108. Estos datos pueden representar informaciones de cuentas y usarse por el terminal o servicio remoto para cargar en la cuenta del usuario automática un porte, por ejemplo, para la entrada en el campo de tiro o para el uso del arma.

Una multiplicidad de otros tipos de hardware y funcionalidades de hardware 152 correspondientes se usan en otras formas de realización, en particular aquellas que presuponen un peligro para el usuario o tercero y que por ello sólo se deben activar en los lugares donde se puede presuponer que la funcionalidad del hardware no daña al usuario ni a terceros.

La figura 2 muestra un diagrama de flujo del procedimiento según una forma de realización de la invención. En la etapa 202 una unidad de localización 130 determina o recibe los datos de posición que indican la posición de la unidad de localización. Por ejemplo, la unidad de localización puede contener un módulo de localización 134 en forma de un sensor GPS. En la etapa 204 los datos de posición se le transmiten de la unidad de localización a la tarjeta inteligente a través de una interfaz sin contacto en forma codificada. Esto sirve en particular para la confidencialidad de los datos de posición y para la protección de los datos frente a manipulaciones. En la etapa 206 se ejecuta un protocolo de delimitación de distancia entre la tarjeta inteligente y la unidad de localización. En la etapa 208 la tarjeta inteligente examina si la unidad de localización pudo comprobar satisfactoriamente que la unidad de localización se sitúa dentro de la distancia máxima espacial de la tarjeta inteligente. Si sale bien la comprobación, la tarjeta inteligente ejecuta una función de tarjeta inteligente 110 en la etapa 210, en donde la función de tarjeta inteligente usa los datos de posición transmitidos. Si no fue posible la comprobación, se puede interrumpir el procedimiento en este punto o incluir uno o varios otros bucles del programa con las etapas 202-208. La tarjeta inteligente puede disponer, por ejemplo, de un servicio que examina a intervalos regulares si se han transmitido datos de posición de una unidad de localización a la tarjeta inteligente. La unidad de localización puede disponer de un servicio que determina la propia posición a intervalos regulares y/o examina a intervalos regulares si se ha recibido una solicitud o desafío para la realización de un protocolo de delimitación de distancia por una tarjeta inteligente. Si el procedimiento prevé una autentificación de la unidad de localización respecto a la tarjeta inteligente, la etapa 206 se puede realizar antes o después de la autentificación o también representar por sí misma en combinación con la etapa 208 la autentificación, en donde la autentificación es satisfactoria cuando la tarjeta

inteligente constata que la unidad de localización se sitúa dentro de la di delimitación de distancia.

La figura 3 muestra un escenario de aplicación de las formas de realización de la invención en el contexto de una detección automática de viajes para medios de transporte públicos. Un vehículo 300, por ejemplo un autobús o un tren, está equipado de una unidad de localización LE4 integrada y un terminal T. En el caso del terminal T se puede tratar, por ejemplo, de un terminal que está contactado por una red de satélites con un servidor de un proveedor de servicios bancarios. El terminal dispone de un equipo lector 124 e interfaces 108 apropiadas para leer los datos, que son necesarios para la ejecución del proceso de pago, del medio de almacenamiento 104 de una tarjeta inteligente 102 de un pasajero. Preferentemente el terminal se sitúa en las puertas del vehículo o se sitúa un terminal en cada puerta del vehículo. Con cada acceso de un pasajero con la tarjeta inteligente se realiza una autentificación automática del terminal respecto a la tarjeta inteligente y a la inversa, constatando el terminal la identidad del pasajero y protocolizando también en que parada ha subido el pasajero. Cuando el pasajero abandona de nuevo el vehículo en otra parada, un terminal en la puerta de vehículo correspondiente constata igualmente la identidad del pasajero y protocoliza en que parada ha abandonado el pasajero el vehículo. Estas informaciones se pueden usar para la elaboración automática de una factura por el uso del vehículo. A este respecto, el terminal no constata las paradas actuales durante la subida o descenso de un pasajero, sino que mejor dicho se determinan cada vez actualmente los datos de posición o identificadores correspondientes de las paradas por parte de la unidad de localización LE4, y se le transmiten a la tarjeta inteligente tal y como se describe arriba. La tarjeta inteligente ejecuta una funcionalidad de la tarjeta inteligente que incluye que al menos al entrar y abandonar el vehículo (a través de una puerta en cuya proximidad se sitúa un terminal) se transmiten los datos de posición actuales (aquí así paradas de acceso o abandono) de la tarjeta inteligente al terminal. Preferentemente esta transmisión se produce sin contacto para configurar la bajada y subida de los pasajeros tan eficientemente como sea posible.

La tarjeta inteligente se le asocia así a un pasajero al que pertenece la tarjeta inteligente. La unidad de localización LE4 forma parte integral del vehículo y es capaz de determinar su propia posición de forma dinámica durante la marcha, en donde la exactitud de la posición determinada es al menos suficiente para clarificar las estaciones individuales en las que suben y bajan los pasajeros. La unidad de localización LE4 puede estar configurada como sensor GPS, pero también se puede tratar de una unidad de localización semiautomática, en la que el conductor pone la posición determinada actualmente por LE4 y comunicada eventualmente a la tarjeta inteligente respecto a la actual parada H1, H2 o H3 durante cada detección. Alternativamente en cada parada puede estar montado un sensor de señales, por ejemplo, un radiotransmisor, que le envía una señal a la unidad de localización LE4 interna al vehículo a fin de posibilitarle que determine y mantenga actualizada su posición actual dentro de, por ejemplo, un plano de líneas de red.

El pasajero al que se le asocia la tarjeta inteligente 102 puede entrar en el vehículo 300, por ejemplo, en la parada H1. Mientras, antes o directamente después de la subida en el vehículo, el usuario se puede autentificar frente a la tarjeta inteligente, por ejemplo, mediante la introducción de un PIN o de una contraseña o mediante datos biométricos. Además, el usuario puede activar una funcionalidad de pago correspondiente de su tarjeta inteligente, lo que en algunos casos puede hacer necesaria una nueva autentificación respecto a una lógica de aplicación determinada. Por ejemplo, el operador de una red ferroviaria o red de transporte de cercanías de una ciudad podría ofrecer una lógica de aplicación correspondiente para la detección automática del viaje y pago, que el pasajero debe instalar en su móvil y autentificarse en ésta. El operador de la red ferroviaria o de cercanías podría dotar a su cliente también con una tarjeta inteligente personalizada, en la que estén contenidas todas las informaciones de cuenta necesarias del cliente para posibilitar una facturación y/o cargo en cuenta automático.

Bajo una "contraseña" se entiende a continuación una serie de caracteres alfanuméricos y/o caracteres especiales. Un PIN se compone preferentemente de pocas cifras (por ejemplo cuatro) y de signos alfanuméricos. No obstante, según el requisito de seguridad también son posibles PINs con cifras adicionales y que se componen de cifras o una mezcla de caracteres alfanuméricos y especiales. Según las formas de realización de la invención, la contraseña está almacenada en el documento. La contraseña para la autentificación del usuario respecto a la tarjeta inteligente puede estar colocada también en forma de una zona legible a máquina (MRZ) sobre la tarjeta inteligente de manera detectable ópticamente (por ejemplo impresa, relieve, etc.). La contraseña puede estar impresa sobre la tarjeta inteligente de manera detectable ópticamente, adicionalmente al almacenamiento, también en forma de un "número de tarjeta de acceso" (Card Access Number, CAN), es decir, un número impreso sobre la tarjeta inteligente, y posibilitarle a un equipo lector una autenticación respecto a la tarjeta inteligente mediante el CAN.

Además, la tarjeta inteligente ejecuta un protocolo de delimitación de distancia con la unidad de localización LE4 durante o inmediatamente después de entrar el pasajero en el vehículo y recibe los datos de posición de la unidad de localización, los cuales se pueden componer, por ejemplo, de un identificador de la parada actual H1. Mientras que el vehículo 300 se mueve de la parada H1 a través de la H2 hacia la parada H3, la unidad de localización LE4 transmite continuamente a intervalos de tiempo determinados sus datos de posición actuales y ejecuta adicionalmente el protocolo de delimitación de distancia con la tarjeta inteligente a intervalos de tiempo regulares, de modo que la tarjeta inteligente "puede garantizar" que los datos de posición proceden de una unidad de localización fiable, próxima espacialmente. Además, la posición actual de la unidad de localización se actualiza en cada cambio de las paradas.

Los identificadores de las respectivas paradas actuales le se transmiten así localización a la tarjeta inteligente del pasajero durante toda la marcha o al menos al subir y bajar, en donde al menos al subir o bajar se transmite la parada de inicio o la parada objetivo de la tarjeta inteligente en la ejecución de la funcionalidad de la tarjeta inteligente 110 al terminal. El terminal puede protocolizar las paradas de subida y bajada del pasajero o almacenarlas en un servidor central. El terminal también puede elaborar una factura por el trayecto recorrido realmente por el pasajero para el caso individual o, por ejemplo, en base mensual o anual, y también cargarla en cuenta eventualmente de forma automática en la cuenta del pasajero. En la protocolización y/o elaboración de factura o cargo en cuenta, el terminal colabora preferentemente con otros ordenadores, por ejemplo, servidores de bases de datos y de aplicaciones, que ofrecen servicios de almacenamiento o protocolización o pago correspondientes, en donde los servidores están localizados típicamente en centros de cálculo remotos.

La figura 4 muestra una forma de realización alternativa del escenario de aplicación arriba descrito. El escenario de aplicación de la figura 4 se diferencia del representado en la figura 3 esencialmente en que a cada parada se le asocia de forma fija una unidad de localización LE1-LE3. Al contrario de lo descrito en la figura 3, así no es necesario que el vehículo 300 mismo disponga de una unidad de localización correspondiente, cuyos datos de posición se actualizan continuamente durante la marcha. Mejor dicho a cada unidad de localización de la figura 4 se le asocia de forma fija su información de posición correspondiente. Así, por ejemplo, la unidad de localización LE1 siempre le puede transmitir el identificador de lugar H1' a la tarjeta inteligente como los datos de posición, mientras que la unidad de localización LE2 siempre transmite el identificador de lugar H2' o la unidad de localización LE3 siempre el identificador de lugar H3'. Típicamente la distancia máxima 302 preconfigurada en la tarjeta inteligente para el protocolo de delimitación de distancia es algo mayor para el escenario de aplicación según la figura 4 que según la figura 3, dado que la unidad de localización según la fig. 4 se sitúa fuera del vehículo 300.

REIVINDICACIONES

1. Procedimiento para la facilitación de los datos de posición para una tarjeta inteligente (102) con secciones para:

- la recepción (202) o determinación de los datos de posición de una unidad de localización (130) por la unidad de localización (130), en donde la unidad de localización (130) está separada espacialmente de la tarjeta inteligente (102);

- la transmisión (204) de los datos de posición de la unidad de localización (130) a la tarjeta inteligente (102) a través de una interfaz (118) sin contacto usando un protocolo criptográfico (114);

- la ejecución (206) de un protocolo de delimitación de distancia (112) entre la tarjeta inteligente (102) y la unidad de localización (130), en donde el protocolo de delimitación de distancia (112) concluye satisfactoriamente precisamente luego cuando la distancia espacial entre la tarjeta inteligente (102) y la unidad de localización (130) no sobrepasa una distancia máxima predeterminada;

- la ejecución (210) de una función de tarjeta inteligente (110) con conclusión satisfactoria del protocolo de delimitación de distancia (112), en donde la función de tarjeta inteligente (110) usa los datos de posición transmitidos como datos de posición que indican la posición actual de la tarjeta inteligente (102).

2. Procedimiento según la reivindicación 1, que comprende además la autentificación de la unidad de localización (130) respecto a la tarjeta inteligente (102) mediante comprobación en el curso de la ejecución del protocolo de delimitación de distancia (112) que la unidad de localización (130) se sitúa dentro de la distancia máxima espacial.

3. Procedimiento según una de las reivindicaciones anteriores, en donde la distancia máxima se predetermina por el protocolo de delimitación de distancia (112).

4. Procedimiento según una de las reivindicaciones anteriores, en donde el protocolo de delimitación de distancia (112) se basa en un protocolo de desafío - respuesta.

5. Procedimiento según una de las reivindicaciones anteriores, en donde la ejecución del protocolo de delimitación de distancia prevé el uso al menos de una primera (120a) y una segunda clave criptográfica (120b), en donde la al menos primera clave criptográfica está almacenada de forma segura en un primer medio de almacenamiento (104) protegido de la tarjeta inteligente, en donde la al menos segunda clave criptográfica está almacenada en un segundo medio de almacenamiento (136) protegido de la unidad de localización.

6. Procedimiento según una de las reivindicaciones anteriores, en donde los datos de posición comprenden:

- una multiplicidad de identificadores de lugar, que en su totalidad identifican un lugar en el que se sitúa la tarjeta inteligente (102) y/o la unidad de localización (130); o

- un identificador de lugar, que identifica un lugar en el que se sitúa la tarjeta inteligente (102) y/o la unidad de localización (130).

7. Procedimiento según la reivindicación 6, en donde cada identificador de lugar de la multiplicidad de identificadores de lugar representa un identificador de red, en donde cada identificador de red identifica una red de comunicación de datos, en cuya región de emisión se sitúa la tarjeta inteligente (102) y/o la unidad de localización (130), que determina estos datos de posición.

8. Procedimiento según una de las reivindicaciones anteriores, en donde la ejecución de la función de tarjeta inteligente (110) comprende las secciones para:

- la liberación del medio de almacenamiento (104) protegido de la tarjeta inteligente (102) para hacer posible la lectura de los datos protegidos (121) por la unidad de localización (130) o por otro sistema de procesamiento de datos (160); y/o

- el registro de los datos de posición con la finalidad de la protocolización de un rastro de movimiento de la tarjeta inteligente (102); y/o

- la realización de una transacción electrónica, en particular de una transacción bancaria; y/o

- la realización de una compra electrónica de billete de transporte o una elevación automática de un peaje en base a los datos de posición; y/o

- la liberación de una funcionalidad de hardware (152) bloqueada de un hardware (150), que está conectado con la tarjeta inteligente (102) de forma operacional.

9. Procedimiento según la reivindicación 8, en donde la funcionalidad de hardware (152) bloqueada determinada para la liberación está concretizada en:

- un mecanismo para quitar el seguro de un arma de fuego;

- un mecanismo de desencadenamiento de un dispositivo de explosión;

- un mecanismo para la mezcla de líquidos y/o sustancias; o

- un movimiento de otro tipo del hardware o uno de sus componentes.

10. Tarjeta inteligente (102) que presenta:

- un medio de almacenamiento (104) para el almacenamiento protegido de al menos una clave criptográfica (138a);

- una interfaz (118) sin contacto para la recepción de los datos de posición de una unidad de localización (130), en donde la recepción se realiza utilizando un protocolo criptográfico (114) usando la al menos una clave criptográfica;

- un módulo de delimitación de distancia (módulo DB) (123a), que está configurado para la ejecución de un protocolo de delimitación de distancia (112) respecto a una unidad de localización (130), en donde el protocolo de delimitación de distancia concluye satisfactoriamente precisamente luego cuando la distancia espacial a la unidad de localización (130) no sobrepasa una distancia máxima predeterminada;

- una función de tarjeta inteligente (110), que sólo se puede ejecutar en el caso de una conclusión satisfactoria del protocolo de delimitación de distancia, en donde la función de tarjeta inteligente (110) usa los datos de posición transmitidos como datos de posición que indican la posición actual de la tarjeta inteligente (102).

11. Tarjeta inteligente (102) según la reivindicación 10, que comprende además un módulo de autentificación (116), que está configurado para la autentificación de la unidad de localización (130) por la tarjeta inteligente (102), en donde sólo en el caso de una autentificación satisfactoria de la unidad de localización (130) se usan los datos de posición transmitidos como datos de posición que indican la posición actual de la tarjeta inteligente (102).

12. Sistema que contiene una unidad de localización (130), en donde la unidad de localización comprende:

- un módulo de localización (134) que está configurado para la recepción o determinación de los datos de posición de la unidad de localización;

- un medio de almacenamiento (136) para el almacenamiento protegido de al menos una clave criptográfica (138b);

- una interfaz (118) para la transmisión sin contacto de los datos de posición a una tarjeta inteligente, en donde la transmisión se realiza utilizando un protocolo criptográfico (114) usando la al menos una clave criptográfica (138b);

- un módulo de delimitación de distancia (módulo DB) (123b), que está configurado para la ejecución de un protocolo de delimitación de distancia entre la unidad de localización (130) y la tarjeta inteligente (102), en donde el protocolo de delimitación de distancia concluye satisfactoriamente precisamente luego cuando la distancia espacial entre la tarjeta inteligente (102) y la unidad de localización (130) no sobrepasa una distancia máxima (302) predeterminada.

13. Sistema según la reivindicación 12, en donde la unidad de localización (130) comprende además un módulo de autentificación (140), que está configurado para la autentificación de la unidad de localización (130) respecto a la tarjeta inteligente (102).

14. Sistema según una de las reivindicaciones 12 o 13, que comprende además la tarjeta inteligente (102), en donde la tarjeta inteligente (102) está configurada según una de las reivindicaciones 10 u 11.

15. Sistema según una de las reivindicaciones 12 a 14,

- en donde la tarjeta inteligente (102) es una tarjeta SIM o una tarjeta inteligente de un documento de seguridad y/o

- en donde la unidad de localización (130) determina los datos de posición mediante GPS, LPS, WLAN, ultrasonidos, tecnología de radio o Bluetooth y/o

- en donde el protocolo de delimitación de distancia se basa en ultrasonidos o radiación electromagnética, en particular microondas, ondas de radio, luz visible o luz infrarroja.

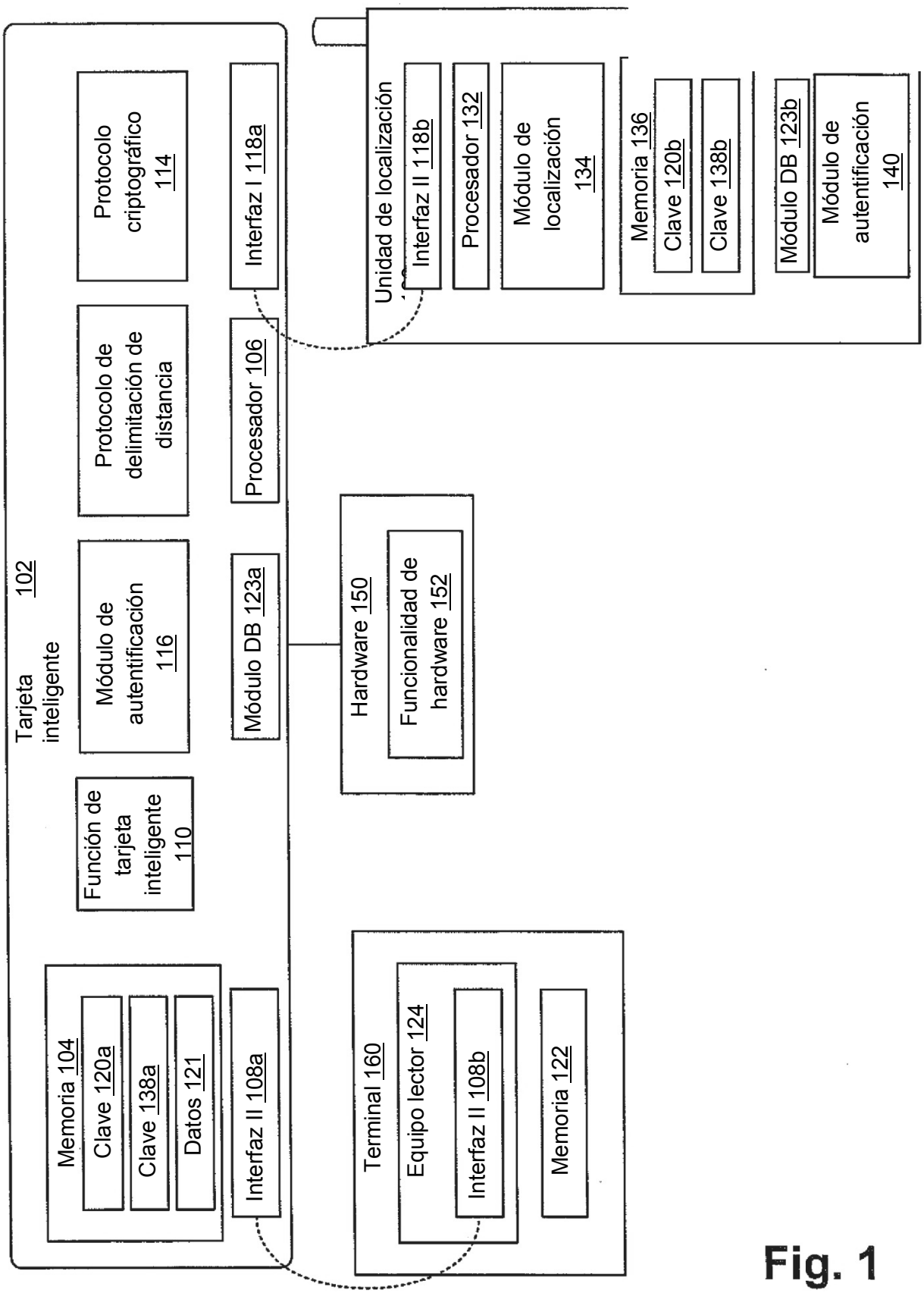
Tarjeta inteligente 102
Protocolo criptográfico 114
Protocolo de delimitación de distancia
Módulo de autentificación 116
Función de tarjeta inteligente 110
Memoria 104
Clave 120a
Clave 138a
Datos 121
Interfaz I 118a
Procesador 106
Módulo DB 123a
Interfaz II 108a
Hardware 150
Funcionalidad de hardware 152
Unidad de localización
Interfaz II 118b
Procesador 132
Módulo de localización 134
Memoria 136
Clave 120b
Clave 138b
Módulo DB 123b
Módulo de autentificación 140
Terminal 160
Equipo lector 124
Interfaz II 108b
Memoria 122

Fig. 1

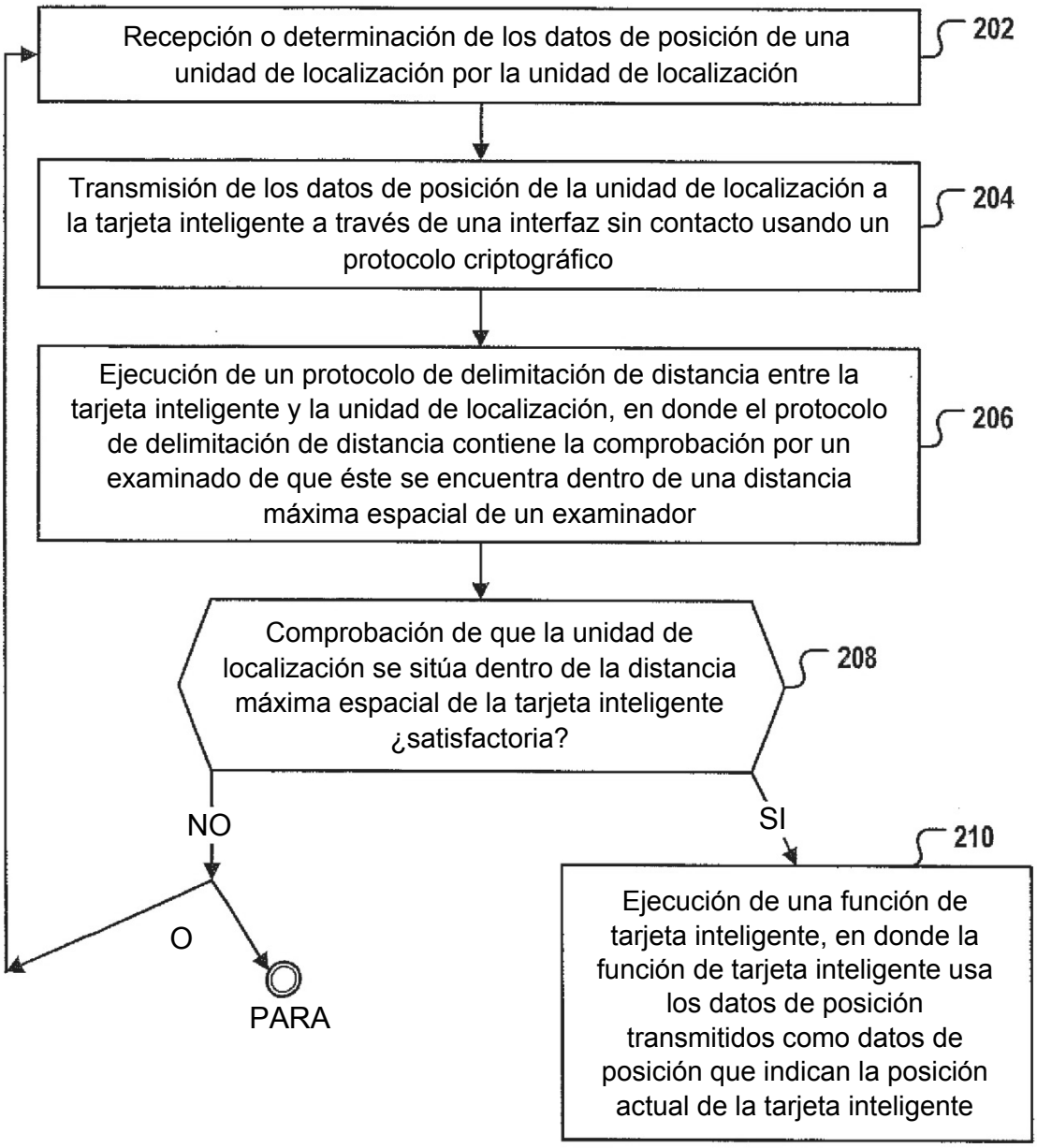
Recepción o determinación de los datos de posición de una unidad de localización por la unidad de localización
202
Transmisión de los datos de posición de la unidad de localización a la tarjeta inteligente a través de una interfaz sin contacto usando un protocolo criptográfico
204
Ejecución de un protocolo de delimitación de distancia entre la tarjeta inteligente y la unidad de localización, en donde el protocolo de delimitación de distancia contiene la comprobación por un examinado de que éste se encuentra dentro de una distancia máxima espacial de un examinador
206
Comprobación de que la unidad de localización se sitúa dentro de la distancia máxima espacial de la tarjeta inteligente ¿satisfactoria?
208
NO
SI
O
PARA
210
Ejecución de una función de tarjeta inteligente, en donde la función de tarjeta inteligente usa los datos de posición transmitidos como datos de posición que indican la posición actual de la tarjeta inteligente

Fig.2

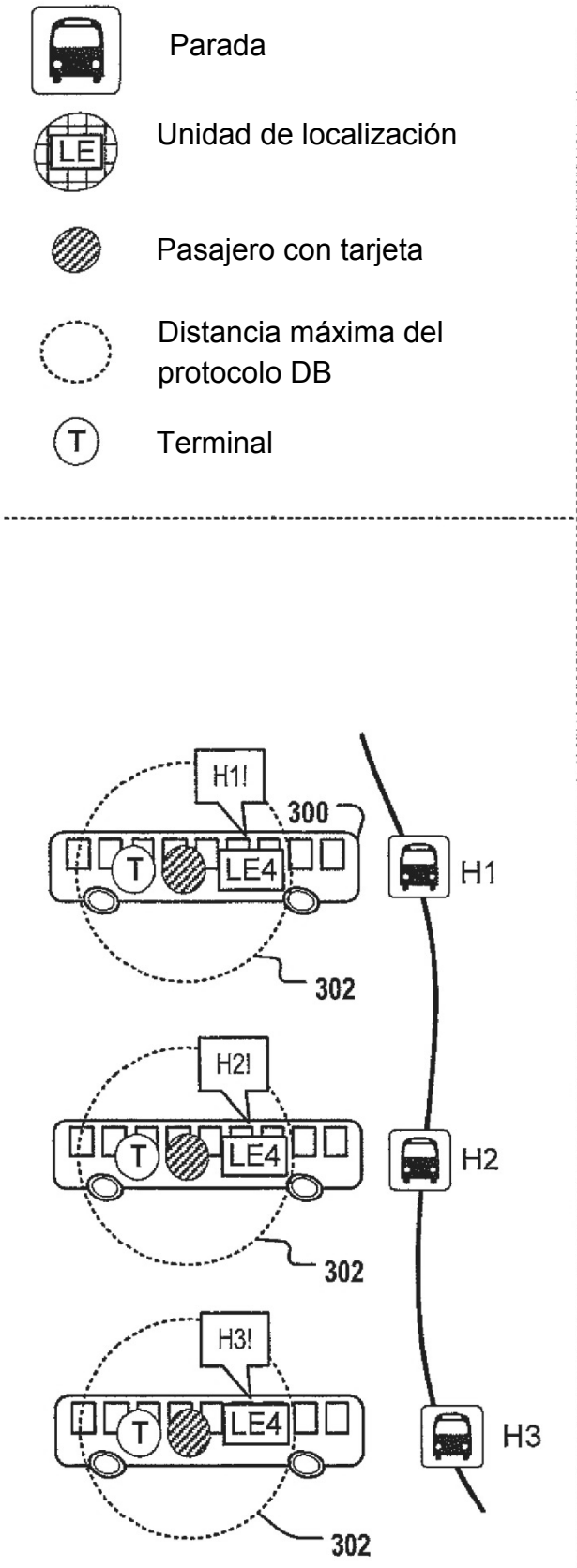
Parada
LE
Unidad de localización
Pasajero con tarjeta
Distancia máxima del protocolo DB
T
Terminal
H1!
300
LE4
H1
302
H2!
LE4
H2
302
H3!
LE4
H3
302

Fig. 3

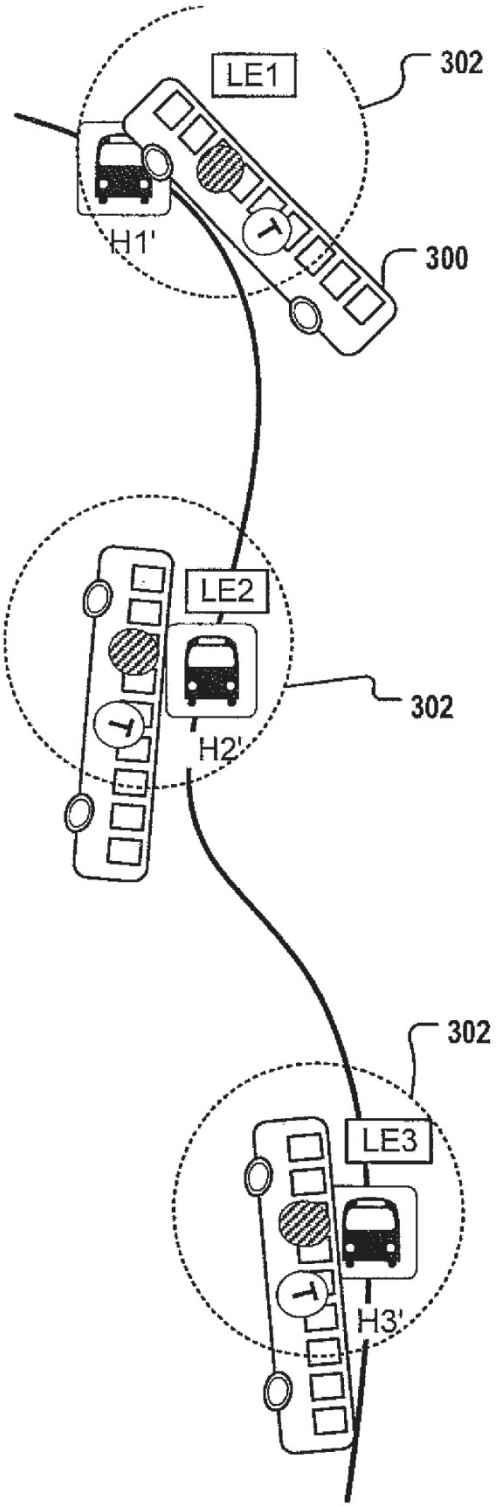
LE1
302
H1'
300
LE2
302
H2'
302
LE3
H3'

Fig. 4