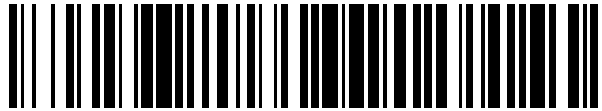


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 634 891**

51 Int. Cl.:

G06F 21/35 (2013.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **17.08.2009 PCT/EP2009/005954**

87 Fecha y número de publicación internacional: **18.02.2010 WO10018000**

96 Fecha de presentación y número de la solicitud europea: **17.08.2009 E 09777925 (0)**

97 Fecha y número de publicación de la concesión europea: **03.05.2017 EP 2318972**

54 Título: **Sistema de autorización con tarjeta y lector**

30 Prioridad:

15.08.2008 EP 08162479

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

29.09.2017

73 Titular/es:

**LEGIC IDENTSYSTEMS AG (100.0%)
Binzackerstrasse 41 Postfach 1221
8620 Wetzikon, CH**

72 Inventor/es:

KLOSA, KLAUS ULRICH

74 Agente/Representante:

CARPINTERO LÓPEZ, Mario

ES 2 634 891 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Sistema de autorización con tarjeta y lector

Campo de la invención

5 La presente invención se refiere a un sistema de autorización que comprende una tarjeta y un lector para una interacción lector - tarjeta, a un procedimiento de asignación entre sí del lector y la tarjeta para hacer operable la interacción lector - tarjeta y a un producto de programa informático para su uso en el sistema de autorización.

Antecedentes de la invención

10 Por el solicitante de la presente solicitud es conocido un sistema de autorización que comprende al menos una etiqueta sin contacto y un lector de la etiqueta con una lógica del lector, por ejemplo, un módulo de seguridad. El lector de la etiqueta interactúa de forma inalámbrica con las etiquetas tan pronto como las etiquetas son situadas en el campo de comunicación inalámbrica del lector. Para autenticar o autorizar la etiqueta o la etiqueta del lector, u operar una interacción segura entre el lector de la etiqueta y la etiqueta al menos un secreto es compartido entre el lector de la etiqueta y la etiqueta. Básicamente, el secreto consiste en un secreto de la etiqueta almacenado en la etiqueta (primer secreto) y un secreto del lector almacenado en el lector de la etiqueta (segundo secreto), de forma que los primero y segundo secretos se correspondan entre sí. En la respectiva autenticación y / o en el proceso de autorización, se verifica si el secreto del lector se corresponde con el secreto de la etiqueta o viceversa. La verificación se efectúa mediante una lógica del sistema de autorización, en general por la lógica del lector. En el sistema de autorización los secretos son utilizados para implementar diferentes niveles de seguridad. Un primer nivel es implementado utilizando un procedimiento de desafío - respuesta del estado de la técnica entre la etiqueta y el lector de la etiqueta. Un segundo nivel puede basarse en la codificación o en la encriptación de la comunicación entre la etiqueta y el lector de la etiqueta, por ejemplo utilizando un logaritmo DES. Un tercer nivel está relacionado con el acceso a los datos o aplicaciones almacenados en la etiqueta o en el lector de la etiqueta. Este nivel se realiza utilizando una clave de la etiqueta o una clave de aplicación almacenada en la etiqueta y la clave del lector almacenada o derivada del lector de la etiqueta. De acuerdo con el documento WO 97/34265 A1, el primer secreto, por ejemplo un sello, y el segundo secreto, por ejemplo, unos datos de lanzamiento, son sometidos a las reglas de un sistema de autorización jerárquico.

Debido al secreto compartido por los miembros del sistema de autorización, en particular la etiqueta y el lector de la etiqueta, el sistema de autorización es un sistema cerrado. La interacción solo puede tener lugar entre los miembros que comparten los secretos de correspondientes.

30 Son conocidos otros sistemas en los que el secreto del lector no está directamente almacenado en el lector de la etiqueta sino en un dispositivo interconectado al lector de la etiqueta, por ejemplo en un módulo de identidad de abonado (SIM) realizado como una etiqueta de contacto e interconectado con el lector de la etiqueta por medio de contactos eléctricos. Un inconveniente es la tasa (velocidad) de interacción limitada debido a la interfaz de contacto.

35 En el estado de la técnica son conocidos otros sistemas de autorización cerrados con diferentes configuraciones acerca del momento y la forma de almacenar los secretos.

40 El documento WO 2008/034937 A1 divulga un sistema de comunicación que comprende un aparato y un dispositivo externo, por ejemplo una etiqueta sin contacto. El aparato comprende una unidad de control configurada para detectar un campo de radiofrecuencia y para cooperar con un módulo seguro, por ejemplo una tarjeta inteligente de contacto, una tarjeta SIM o un chip. El módulo seguro está permanentemente integrado, fijado de manera separable o montado de manera amovible dentro del aparato. Dependiendo de si el aparato actúa como un lector de la etiqueta (modo activo) o como una etiqueta (modo pasivo), la unidad de control controla la comunicación sin contacto o pasa el control a través del módulo seguro.

45 El documento EP 1 873 963 A1 se refiere a un procedimiento de autenticación para tarjetas de circuito integrado (tarjetas IC) en un sistema de autenticación entre una primera tarjeta de IC, por ejemplo un módulo de aplicación seguro (SAM) de un terminal, y una segunda tarjeta de IC de contacto interconectadas a través de un terminal por medio de los correspondientes secretos almacenados en la primera y segunda tarjetas de IC. En particular, al menos un número de identificación y / o autenticación es utilizado para autenticar la primera tarjeta de IC a partir de la segunda tarjeta de IC.

50 El documento US 2005/0103839 A1 divulga un sistema de autorización cerrado con tres dispositivos: un terminal, un módulo de seguridad, por ejemplo una tarjeta de IC, y una unidad de identificación y autorización (IAL) físicamente separada. En la IAL es almacenada en una memoria la información necesaria para la identificación de un usuario. Esta información es comparable con un PIN introducido por un usuario en un sistema realizado sin una IAL. La IAL es utilizada para convertir en obsoleta la introducción de un PIN. La interacción entre el terminal y la tarjeta de IC es una interacción o bien de contacto o bien sin contacto, la interacción entre la tarjeta de IC y la IAL es inalámbrica.

55 El documento WO 2006/117009 A1 divulga un procedimiento de gestión de una unidad periférica, por ejemplo una tarjeta de memoria de un terminal de una red de comunicación mediante una unidad segura, por ejemplo una unidad

de identidad de abonado (tarjeta SIM). Se implementa una arquitectura en la que se habilita la operación de la tarjeta de memoria solo en presencia de la tarjeta SIM, que es capaz de autenticar la tarjeta de memoria. Debido a la funcionalidad fiable de la tarjeta SIM, la tarjeta de memoria se convierte en una segunda unidad fiable controlada por la tarjeta SIM. No se habilita una modificación del secreto almacenado en la unidad segura independiente del propio segundo secreto.

El documento US 2008/0076475 A1 divulga un sistema móvil que incluye una tarjeta SIM y un circuito de comunicación. Este circuito de comunicación interactúa con un dispositivo externo, en particular un lector de etiqueta, por medio de una primera interfaz inalámbrica, y con la tarjeta SIM por medio de una segunda interfaz inalámbrica. Se dispone un sistema y una tarjeta SIM con una pluralidad de diferentes interfaces de comunicación o de protocolos de comunicación. No se habilita una modificación del secreto almacenado en el lector de la tarjeta.

El documento EP 1 942 470 A1 se refiere a un sistema de autenticación que comprende un lector y unos primero y segundo medios de autenticación y unos medios de metaautenticación previstos como una portadora entre diferentes medios de autenticación y el lector. El sistema se refiere a un sistema de autenticación para simplificar la elaboración de medios de autenticación, especialmente medios de autenticación para una aplicación diferente.

El documento WO 02/05225 A1 divulga un procedimiento para la inicialización de soportes de datos móviles sobre estaciones de lectura / escritura descentralizadas dedicadas, dentro del marco de un sistema de autorización. Los datos de inicialización son creados en un proceso de autorización por unos medios de autorización y enviados a una estación de lectura / escritura autorizada descentralizada a través de una red en una comunicación segura, de acuerdo con las normas de seguridad correspondientes al sistema de autorización. El soporte de datos móviles es inicializado con los datos de inicialización y / o los datos de inicialización son enviados a través de la red hacia una estación de lectura / escritura descentralizada, tras lo cual se inicializa la estación de lectura / escritura. El procedimiento de inicialización anterior permite nuevas posibilidades de aplicación y uso de dichos sistemas.

En un estado cerrado del sistema de autorización de la técnica (en lo sucesivo designado como sistema de autorización estándar o sistema estándar), el secreto, en particular el secreto del lector, es almacenado en el lector de la etiqueta, o bien en una lógica, en una memoria o en otra etiqueta lógicamente conectada al lector de la etiqueta, por ejemplo a un módulo de identidad de abonado. Si el secreto del lector tiene que ser modificado entonces la lógica, la memoria o la otra etiqueta tiene que ser sustituida. Dicho cambio de hardware del lector de la etiqueta es engorroso y puede ser difícil de llevar a cabo. Así mismo, debido a la funcionalidad fiable del secreto del lector, dichos cambios pueden no ser de ningún modo requeridos. Por ello, el lector de la etiqueta a menudo está diseñado de una forma que no permite el fácil acceso o sustitución del hardware o de partes del hardware en las cuales está almacenado el secreto del lector. Debido a estos inconvenientes, los lectores de la etiqueta de un sistema estándar no pueden ser fácilmente modificados o actualizados para interactuar con etiquetas de otro sistema estándar.

Sumario de la invención

Es un objeto de la presente invención resolver al menos algunos de los inconvenientes de la técnica anterior. En particular, es un objeto de la presente invención proporcionar un sistema de autorización potenciado que sea compatible con los sistemas de autorización existentes (sistemas en operación, sistemas instalados).

De acuerdo con la presente invención, estos objetivos se consiguen en particular por medio de las características de las reivindicaciones independientes. Así mismo, otras formas de realización ventajosas se desprenden de las reivindicaciones dependientes y de la descripción.

El sistema de autorización comprende un lector para una interacción lector - tarjeta con una tarjeta, un módulo lógico configurado para asignar entre sí el lector y la tarjeta y para hacer operable la interacción lector - tarjeta en base a los datos de lector del lector y a los datos de la tarjeta de la tarjeta, de forma que los datos del lector y los datos de la tarjeta sean datos de autorización del sistema de autorización.

De acuerdo con la presente invención, los objetivos expuestos se consiguen en especial porque el módulo lógico está también configurado para leer por medio de un dispositivo de interfaz sin contacto los datos procedentes de un dispositivo de almacenamiento de autorización, y para asignar el lector a la tarjeta en base a los datos del dispositivo para hacer operable la interacción lector - tarjeta.

Así, la presente invención prescinde del esquema conocido de los sistemas de autorización estándar de sustitución del hardware del lector de la etiqueta para modificar el secreto del lector (datos de autorización) almacenados en el lector de la tarjeta. En concreto, la presente invención rompe con el esquema habitual de los sistemas estándar de almacenar modificaciones de datos de autorización en el lector de la etiqueta. En un sistema de autorización potenciado de acuerdo con la presente invención (en lo sucesivo sistema de autorización), en vez de en el lector, las modificaciones de los datos de autorización u otras informaciones relacionadas con un lector (en lo sucesivo datos del lector) son almacenadas en un dispositivo de almacenamiento de autorización (ASD) inalámbrico que está interconectado de forma inalámbrica con el lector.

- Es posible acceder a los datos del lector almacenados en el ASD, si el lector comprende una interfaz sin contacto y el dispositivo de almacenamiento de autorización está dispuesto en alguna parte dentro de un rango de comunicación (rango de interacción) del lector. La interfaz sin contacto es utilizada para la interacción sin contacto entre el lector y el ASD (en lo sucesivo, interacción lector - dispositivo). O bien la interfaz sin contacto del lector es configurable para dicha interacción o bien una interfaz del ASD (en lo sucesivo interfaz de dispositivo) es compatible con la interfaz sin contacto. Debido a la interconexión inalámbrica o a la interacción inalámbrica, respectivamente, entre el lector y el ASD, y en especial cuando el ASD se ejecuta como un dispositivo pasivo energizado por el lector por medio de la conexión inalámbrica, no se requiere una conexión cableada entre el lector y el ASD, ni para la interacción no prevista para el ASD.
- 5
- 10 Esto da como resultado potenciaciones del sistema de autorización con respecto a la configuración (montaje) del sistema, por ejemplo, a la introducción de nuevos dispositivos del sistema, por ejemplo una nueva especie / tipo de lectores o tarjetas; la asignación entre sí de los diferentes dispositivos del sistema; la habilitación de una salvaguardia de compatibilidad del sistema, la compatibilidad inversa y retrofiabilidad; la implementación de características de seguridad mejoradas o adicionales; y la implementación de aplicaciones nuevas o adicionales.
- 15 Mediante la introducción del dispositivo de almacenamiento de autorización, el sistema de autorización es avanzado desde un sistema de "dos elementos" (sistema estándar) a un sistema de "tres elementos". El sistema de "dos elementos" básicamente comprende el lector y una tarjeta y las interacciones principales se llevan por tanto a cabo entre el lector y la tarjeta. El sistema de "tres elementos" también comprende el dispositivo de almacenamiento de autorización y las interacciones principales se producen entre el lector y la tarjeta, y entre el lector y el ASD.
- 20 Transmitida (tunelizada) por el lector, en el sistema de "tres elementos", también puede tener lugar una interacción entre la tarjeta y el ASD. Desde la perspectiva de la tarjeta, la interacción entre el lector y el ASD puede estar oculta, respectivamente se produce funcionalmente oculta. Según se describe más adelante, una ventaja adicional de la introducción del ASD es las posibilidades emergentes de controlar o incluso hacer operable la interacción entre el lector y la tarjeta o cualquier otra interacción efectuada o transmitida por el lector.
- 25 Por ejemplo, el módulo lógico del sistema de autorización es implementado como una lógica de lector, una lógica de tarjeta o como una lógica de dispositivo, configuradas para manejar datos, en particular datos de autorización o para ejecutar una aplicación, y conectado a o dispuesto en el lector, la tarjeta o el dispositivo de almacenamiento de autorización, respectivamente.
- 30 La tarjeta comprende unos datos almacenados de la tarjeta y una interfaz de la tarjeta para una interacción lector - tarjeta entre el lector y la tarjeta. El lector comprende unos datos almacenados de la tarjeta y una interfaz de la tarjeta para la interacción lector - tarjeta, una interfaz de lector de contacto o sin contactos y una interfaz sin contacto. El dispositivo de almacenamiento de autorización comprende unos datos almacenados del dispositivo y una interfaz del dispositivo para una interacción sin contacto. El dispositivo de almacenamiento de autorización está conectado de forma inalámbrica con el lector durante la interacción lector - dispositivo entre el lector y el dispositivo
- 35 de almacenamiento de autorización y / o durante una interacción tarjeta - dispositivo entre la tarjeta y el dispositivo de almacenamiento de autorización, transmitida por el lector (y debido a que la retransmisión depende de la interacción lector - dispositivo). La interacción lector - dispositivo y la interacción tarjeta - dispositivo resulta operable mediante el módulo lógico y son implementadas por medio de la interfaz del dispositivo y de la interfaz sin contacto.
- 40 En una forma de realización, el sistema de autorización comprende una unidad periférica y / o un anfitrión. La unidad periférica o el anfitrión, o ambos, están lógicamente conectados al lector y comprenden unos medios para una interacción de unidad / anfitrión - lector entre el lector y la unidad periférica, respectivamente el anfitrión. Como alternativa o adicionalmente, la unidad periférica y / o el anfitrión comprenden unos medios para una interacción de unidad / anfitrión - tarjeta entre la tarjeta y la unidad periférica, respectivamente el anfitrión, en la que la interacción de unidad / anfitrión - tarjeta es transmitida por el lector.
- 45 En una forma de realización adicional del sistema de autorización, el dispositivo de almacenamiento de autorización está dispuesto separado de la interfaz sin contacto por una distancia esencialmente fija (con respecto al lector), al menos durante la interacción lector - dispositivo o la interacción tarjeta - dispositivo y / o durante una cualquiera de las interacciones llevadas a cabo o transmitidas por el lector. En otra forma de realización adicional, el ASD puede estar dispuesto a una distancia permanentemente fija.
- 50 En general, los datos del lector son una parte de los datos de autorización utilizados en el sistema de autorización (datos del sistema). Los datos del lector se corresponden sin ambigüedades con los datos de otros dispositivos (miembros) del sistema de autorización, por ejemplo los datos de la tarjeta, que forman otra parte de los datos de autorización. Los datos de autorización son utilizados para asignar los diferentes dispositivos del sistema de autorización, por ejemplo el lector, la tarjeta o el ASD entre sí o con el sistema de autorización, respectivamente. Los
- 55 datos de autorización son también utilizados para asignar la aplicación implementada dentro del sistema de autorización al sistema de autorización o a los dispositivos del sistema, respectivamente. Por ejemplo, la aplicación es almacenada en el lector, la tarjeta, el dispositivo de almacenamiento de autorización, la unidad periférica y / o el anfitrión. Conjuntamente, los diferentes dispositivos pertenecientes al mismo sistema de autorización (que comparten la pertenencia al sistema o la correspondencia con los datos del sistema) abarcan el sistema de

autorización cerrado. La asignación entre sí es una característica del sistema de autorización que afecta a la seguridad, a la interoperabilidad, la reconfigurabilidad o retroajustabilidad del sistema de autorización.

5 En general, los datos de autorización son manejados por el módulo lógico del sistema de autorización. El módulo lógico comprende un producto de programa informático y una unidad de procesamiento, por ejemplo un microprocesador (uP). Los datos de autorización pueden ser manejados únicamente en un módulo lógico, por ejemplo en la lógica del lector. Como alternativa, pueden utilizarse más de un módulo lógico al mismo tiempo o con posterioridad al manejo de los datos de autorización.

10 El dispositivo de almacenamiento de autorización puede ser utilizado para almacenar otro tipo de datos (que no sean datos de autorización) utilizados en el sistema de autorización y manejados por el módulo lógico del sistema de autorización.

Además de para la autorización, los datos pueden ser utilizados con otras finalidades, por ejemplo:

- a) Implementar los diferentes niveles de seguridad del sistema conocidos en la técnica anterior;
- 15 b) Hacer operable una interacción llevada a cabo o transmitida por el lector, en particular una interacción lector - tarjeta entre el lector y una tarjeta, con otro dispositivo del sistema de autorización (en este caso, los datos pueden ser considerados sistema relacionado);
- c) Hacer ejecutable una aplicación, en particular para utilizar el lector para controlar el acceso a o la ejecución de la aplicación almacenada en la tarjeta (en este caso, los datos pueden ser considerados aplicación relacionada).

20 Los mismos datos o datos derivados pueden ser utilizados para implementar uno cualquiera de los objetivos descritos, o una combinación de los mismos.

25 Los datos del dispositivo almacenados en el ASD pueden representar una sustitución completa de los datos del lector o solo una corrección (actualización) de los datos del lector. Un aspecto de la invención es utilizar el dispositivo de almacenamiento de autorización para almacenar los datos del lector, en particular los datos de autorización, que no puedan ser almacenados en el lector - o que no deban ser almacenados en el lector, por ejemplo, debido a consideraciones relativas a la potenciación de la seguridad del sistema. Por consiguiente, el módulo lógico está configurado para utilizar los datos del dispositivo para alterar los datos del lector para hacer operable la interacción lector - tarjeta. Otro aspecto de la invención es utilizar el ASD para almacenar datos de otros dispositivos del sistema de autorización, por ejemplo datos relacionados con el dispositivo periférico o datos relacionados con tipos especiales de tarjetas, por ejemplo una tarjeta de monitorización. Un ejemplo de una tarjeta de monitorización sería una tarjeta utilizada para leer periódicamente informaciones acerca de las interacciones llevadas a cabo por el lector, con fines de contabilidad / licencias.

30 El almacenamiento de los datos de autorización en el dispositivo de almacenamiento de autorización en vez de en el lector hace posible modificar los datos del lector sin tener que modificar el hardware del lector. En la práctica, el intercambio de los datos del lector se efectúa en la mayoría de los casos, (se realiza, implementa) mediante una modificación del software del lector (software de sustitución) o añadiendo y ejecutando una aplicación adicional (nueva) (aplicación de sustitución) al menos una parte de la aplicación de sustitución, cuando se ejecuta, tiene por finalidad llevar a cabo la interacción lector - dispositivo. Mediante el software de sustitución o de la aplicación de sustitución, el lector está configurado para interactuar con el ASD y para manejar los datos del dispositivo, si son aplicables. El software de sustitución se realiza mediante sustitución, cambio, corrección o actualización que esté operando el lector (software de operación del lector). El software o la aplicación para llevar a cabo la interacción lector - dispositivo comprende unos comandos (que incluyen códigos, subprogramas, etc.) que sean ejecutados por el lector o por el software del lector además de los comandos ejecutados con respecto a otras interacciones del lector.

45 Dentro de un sistema de autorización, pueden efectuarse cambios del software de manejar más fácil y ofreciendo más posibilidades que las modificaciones del hardware. Así mismo, a menudo además de una modificación del hardware también es necesaria, no obstante, una modificación del software. Por tanto, utilizando el almacenamiento de autorización de acuerdo con la invención, puede efectuarse de manera más rentable una transformación o un avance de los sistemas estándares existentes.

50 El software o la aplicación para llevar a cabo la interacción lector - dispositivo se proporciona mediante un módulo lógico del sistema de autorización, por ejemplo la lógica del lector. Como alternativa, se utiliza la lógica del dispositivo de almacenamiento de autorización, siempre que tenga lugar una interacción básica del lector y del ASD en base a la cual el ASD pueda enviar al lector los respectivos comandos que serán ejecutados por el lector.

55 Un aspecto adicional de la invención es el hecho de que el dispositivo de almacenamiento de autorización está físicamente separado de la interfaz sin contacto. La separación física permite un emplazamiento seguro del ASD con respecto a un montaje espacial seguro del sistema de autorización. La separación física básicamente no puede modificarse debido a la posición definida del ADS con respecto al lector o a la interfaz sin contacto, respectivamente.

para mejorar aún más la seguridad del sistema de autorización, el ASD está configurado para que resulte inoperable cuando es alejado de la distancia fija. Por ejemplo, unos medios para llevar a cabo la inoperabilidad comprenden una unidad de energía para energizar una memoria del ASD en el que los datos del dispositivo están almacenados. La propia unidad de energía es energizada de forma inalámbrica por el lector, por ejemplo por medio del campo RF que es periódicamente emitido por el lector al verificar la presencia de la tarjeta. Por ejemplo, la unidad de energía está configurada para borrar los datos del dispositivo, en el caso de que la energía caiga por debajo de un umbral predefinido. Las caídas de energía por debajo del umbral cuando la unidad de energía ya no está energizada por el lector, debido a que el ASD ha sido retirado de la distancia fija o debido al rango de interacción del lector.

Para mejorar la seguridad del sistema de autorización, en una forma de realización, el lector está configurado para llevar a cabo un procedimiento de verificación de la presencia del ASD o una señal de interacción procedente del ASD. La verificación se utiliza para diagnóstica y determinar si la distancia fija entre el dispositivo de almacenamiento de autorización inalámbrico y la interfaz sin contacto no ha sido alterada de una forma que afecte al montaje espacial. El módulo lógico está configurado para verificar que la distancia fija no ha sido alterada.

Otro aspecto de la separación física de la distancia fija es el grado de libertad relativo al punto donde instalar o fijar el dispositivo de almacenamiento de autorización. En una forma de realización del sistema de autorización, el ASD es fijado sobre el lector, en la mayoría de los casos en una manera en la que el ASD queda oculto (no visible). Si se desea, el ASD puede ser visible para un usuario del lector. Si el recinto del lector puede ser fácilmente retirado, por ejemplo para acceder al hardware del lector, entonces el ASD puede ser colocado dentro del lector. Si el recinto del lector no puede ser fácilmente retirado, pero el completo lector puede ser retirado de, por ejemplo, la pared sobre la cual el lector está montado, entonces el ASD puede ser fijado sobre el lado trasero del lector encarado hacia la pared. Cuando el lector no puede ser retirado en modo alguno de, por ejemplo, la pared, el ASD puede ser colocado a continuación del lector, ya sea sobre el lado de la pared sobre el cual el lector está montado (delantero), en la pared, por ejemplo en un retranqueo, o incluso sobre el otro lado de la pared (trasero).

En una forma de realización, el dispositivo de almacenamiento de autorización es ejecutado en o se materializa como cualquier tipo conocido de portadora de datos físicos, sin contacto (inalámbricos), por ejemplo una tarjeta (una tarjeta adicional), una pegatina, una marca, un inserto electrónico, una etiqueta, un testigo, un colgante o un circuito integrado (un chip). El ASD puede ser autoadhesivo. Para mejorar la seguridad, el ASD autoadhesivo se realiza de una manera en el que el ASD es físicamente destruido y, por tanto, resulta inoperable cuando se extrae. La destrucción física puede ser implementada de una manera en la que la interfaz del dispositivo sea permanentemente perturbada por una memoria del ASD en la que estén almacenados los datos del dispositivo.

En otra forma de realización del sistema de autorización, el dispositivo de almacenamiento de autorización o los datos del dispositivo, respectivamente, están configurados para hacer operables, por medio del respectivo módulo lógico, al menos una interacción efectuada o transmitida por el lector. La retransmisión por el lector significa que el lector es utilizado para retransmitir una interacción que tiene lugar entre dispositivos del sistema distintos del lector con respecto a los comandos de interacción que se ejecutan y a los datos de extremo a extremo que se intercambian. En general, el ASD está relacionada con una de las siguientes interacciones:

- a) la interacción lector - dispositivo; b) la interacción lector - tarjeta; c) la interacción dispositivo - tarjeta; d) la interacción de unidad lector - anfitrión; e) la interacción de unidad / tarjeta - anfitrión; y / o f) la interacción de unidad / dispositivo - anfitrión. Como alternativa o adicionalmente, el ASD o los datos del dispositivo pueden hacer ejecutable la aplicación. Como alternativa, los datos del dispositivo junto con al menos uno de los datos de la tarjeta o de los datos del lector están configurados de la misma manera.

Desde un punto de vista externo (por ejemplo el punto de vista del usuario del sistema de autorización, en particular el usuario de la tarjeta), otro aspecto de la invención debe apreciarse en el hecho de que el dispositivo de almacenamiento de autorización está funcionalmente oculto. Los datos, por ejemplo, los datos del lector, son desplazados hasta el interior de un dispositivo de almacenamiento de autorización indetectable (SASD). Con respecto a, por ejemplo, la interacción lector - tarjeta, funcionalmente oculta significa que para la tarjeta o para la aplicación almacenada en la tarjeta, aparece como si toda la interacción tenga lugar con el lector, aunque el lector puede también interactuar con el ASD para hacer operable la interacción lector - tarjeta. En particular, parece como si los datos de la tarjeta se correspondieran con los datos del lector almacenados en el lector, también en un caso en el que no esté almacenado en el lector ningún dato correspondiente al lector y los datos correspondientes efectivos sean los datos del dispositivo almacenados en el ASD.

Desde un punto de vista externo, la tarjeta o cualquier otro dispositivo del sistema de autorización está interactuando solo con el lector, con independencia de si los datos correspondientes requeridos por el lector sean efectivamente los datos del lector almacenados en el lector o los datos del dispositivo almacenados en el ASD, o una combinación de estos.

Ocultar física o funcionalmente el dispositivo de almacenamiento de autorización en el sistema de autorización es un aspecto adicional que se refiere a la seguridad del sistema o a la protección del sistema. Cuando los datos, por ejemplo los datos del dispositivo, son almacenados en el dispositivo de almacenamiento de autorización, resulta más difícil piratear, atacar, derrotar o sortear el sistema, en particular los datos del lector. Este es en concreto el caso, si

no se conoce en modo alguno (desde un punto de vista externo) que un ASD o SASD es utilizado en el sistema de autorización.

5 Otra forma de realización del sistema de autorización se caracteriza porque los datos del dispositivo almacenado en el dispositivo de almacenamiento de autorización son utilizados para alterar (sustituir, corregir, actualizar) los datos del lector almacenados en el lector. Los datos del dispositivo están sustituyendo los datos del lector que han sido originalmente configurados y utilizados para hacer operable una de las interacciones llevadas a cabo o transmitidas por el lector, por ejemplo la interacción lector – tarjeta.

10 Un aspecto de alteración de datos, por ejemplo los datos del lector, por los datos del dispositivo está relacionado con la posibilidad emergente de potenciar (hacer genéricos) los sistemas de autorización existentes, por ejemplo un sistema estándar, manteniendo al tiempo la funcionalidad del sistema existente. El ejemplo siguiente muestra la forma en que una potenciación es realizable: un primer sistema de autorización cerrado, en el que, por ejemplo, la pertenencia del sistema se define por unos primeros datos de habilitación o secreto de habilitación, puede ser potenciado para incluir una segunda tarjeta con unos segundos datos de la tarjeta utilizados para definir la pertenencia del sistema. Esto se efectúa asignando un ASD al lector de dicho primer sistema y asignando los datos del dispositivo almacenados en el ASD para que coincidan con los segundos datos de la tarjeta. A continuación, los datos del dispositivo básicamente actúan como los segundos datos del lector. El ejemplo siguiente muestra otra realización de potenciación: incluir un segundo sistema de autorización cerrado, en el que la pertenencia del sistema se defina por unos segundos datos de habilitación o un secreto de habilitación, en un primer sistema de autorización cerrado, los segundos datos de habilitación que faltan en el lector del primer sistema son almacenados en el ASD asignado a dicho lector del primer sistema. Un tercer ejemplo sería: fusionar un primero y un segundo sistemas de autorización cerrados para formar el sistema de autorización, los primeros datos de habilitación que faltan en el lector del segundo sistema son almacenados en el primer ASD asignado al segundo lector, y los segundos datos de habilitación que faltan en el lector del primer sistema son almacenados en el segundo ASD asignado al primer lector.

25 Por medio del dispositivo de almacenamiento de autorización o los datos del dispositivo, respectivamente, pueden realizarse sistemas de autorización de un nivel más genérico en los que diferentes sistemas de autorización o tarjetas diferentes se incluyan o fusionen (datos del sistema de diferente significado, que definan la pertenencia del sistema, que son diferentes para el sistema o para las respectivas tarjetas). En particular, el almacenamiento de autorización es utilizado para hacer que sean genéricos los lectores del sistema diferente con respecto a los datos del lector o a los datos del sistema diferente que faltan (que no están almacenados) en el lector, respectivamente. Básicamente, el sistema de autorización de acuerdo con la invención se impone sobre sistemas de autorización existentes.

30 Desde un punto de vista externo, parece como si, por ejemplo, el sistema de autorización existente (sistema estándar) es una parte integrante del sistema de autorización; y / o el sistema de autorización estuviera configurado (montado, implementado, instalado) para incluir el sistema de autorización existente. Esto es importante con respecto a la compatibilidad hacia atrás o retroajustabilidad, en el caso de que un sistema de autorización existente deba ser convertido en un sistema de autorización reteniendo al tiempo (salvaguardando) una funcionalidad completa.

40 Otro aspecto de hacer genérico el sistema de autorización diferente o los (hechos genéricos) lectores del sistema diferente, respectivamente, está relacionado con los propietarios / proveedores. Si los datos o la pertenencia del sistema está relacionada con los propietarios / proveedores, entonces el dispositivo de almacenamiento de autorización proporciona un medio para que un primer propietario / proveedor consiga acceder a y utilice el sistema de autorización de otro (un segundo) propietario / proveedor. El propietario / proveedor puede referirse al propietario / proveedor de diferentes sistemas, al propietario / proveedor de diferentes tarjetas o incluso al propietario / proveedor de diferentes aplicaciones.

45 En una forma de realización del sistema de autorización, el dispositivo de almacenamiento de autorización, los datos del dispositivo, o los datos del dispositivo junto con al menos unos datos entre los datos de la tarjeta o los datos del lector, - es utilizado por medio de al menos un respectivo módulo lógico configurado de manera correspondiente – para hacer operable un segundo sistema de autorización, una segunda tarjeta o una segunda aplicación de un segundo propietario / proveedor en base a un segundo sistema de datos o a un grupo de estos, en un primer sistema de autorización de un primer propietario / proveedor en base a los primeros datos del sistema.

50 En otra forma de realización del sistema de autorización, el módulo lógico está configurado para utilizar el dispositivo de almacenamiento de autorización o los datos del dispositivo para asegurar al menos una interacción entre la interacción ejecutada o transmitida por el lector, de modo preferente, al menos la interacción lector – tarjeta. Como alternativa o adicionalmente, el módulo lógico está configurado para utilizar el dispositivo de almacenamiento de autorización o los datos del dispositivo para asegurar la ejecución de la aplicación. Como alternativa, la seguridad se efectúa por el dispositivo de almacenamiento de autorización o por los datos del dispositivo en combinación con al menos unos datos entre los datos del lector y los datos de la tarjeta.

En otra forma de realización del sistema de autorización, el módulo lógico está configurado para utilizar el dispositivo de almacenamiento de autorización o los datos del dispositivo para imponer (establecer) la pertenencia al sistema de

5 autorización de un dispositivo del sistema de autorización, por ejemplo la tarjeta o el lector. Adicionalmente o como alternativa, el módulo lógico está configurado para utilizar los datos del dispositivo para imponer una norma de un sistema de autorización, de modo preferente, un sistema de autorización jerárquico. En otra forma de realización, los datos del dispositivo, conjuntamente (esto es, en combinación) con los datos de la tarjeta y / o con los datos del lector, están configurados en consonancia, o el dispositivo de almacenamiento de autorización es utilizado en solitario. (El establecimiento incluye la respectiva verificación o imposición).

10 En otra forma de realización adicional del sistema de autorización, el lector comprende solo una única interfaz para la interacción lector - tarjeta y la interacción lector - dispositivo. La interfaz del lector sin contacto actúa como (es) la interfaz sin contacto. Esto es posible cuando la interacción lector - tarjeta y la interacción lector - dispositivo están basadas en el mismo protocolo y utilizan la misma frecuencia. Este es básicamente el caso cuando el dispositivo de almacenamiento de autorización se realiza como otra tarjeta del sistema de autorización. Como alternativa, la interfaz del lector está configurada para llevar a cabo tanto la interacción lector - tarjeta como la interacción lector - dispositivo, ya sea de manera subsecuente o al mismo tiempo. La configuración puede llevarse a cabo una vez para diversas interacciones, una vez para todas las interacciones futuras o para cada interacción única.

15 La invención se refiere además a un procedimiento de operación (hacer operable) una interacción en un sistema de autorización de acuerdo con la invención. El procedimiento comprende las etapas de:

- a) Iniciar una interacción lector - tarjeta entre un lector y una tarjeta;
- b) De manera opcional, iniciar una interacción de unidad / lector - anfitrión entre el lector y al menos un elemento entre unidad periférica y un anfitrión;
- 20 c) Iniciar una interacción lector - dispositivo entre el lector y un dispositivo de almacenamiento de autorización;
- d) Utilizar el dispositivo de almacenamiento de autorización, unos datos del dispositivo almacenados en el dispositivo de almacenamiento de autorización o los datos del dispositivo en combinación con al menos unos datos entre unos datos del lector almacenados en el lector y unos datos de la tarjeta almacenados en la tarjeta, o una combinación de estos, para definir unos datos de habilitación;
- 25 e) Utilizar los datos de habilitación para hacer operable al menos una de las interacciones o la ejecución de una aplicación o una combinación de estas, llevadas a cabo por transmitidas por el lector.

30 En particular, la presente invención se refiere a un procedimiento de asignación en un sistema de autorización de un lector y de una tarjeta entre sí, en base a los datos del lector y a los datos de la tarjeta utilizados como datos de autorización del sistema de autorización. El procedimiento comprende las etapas de leer mediante un módulo lógico los datos del dispositivo a partir de un dispositivo de almacenamiento de autorización por medio de una interfaz sin contacto del lector, y utilizar los datos del dispositivo para asignar al lector la tarjeta, haciendo así operable al menos una interacción lector - tarjeta entre el lector y la tarjeta.

El montaje inicial del sistema de autorización comprende las siguientes etapas:

- 35 a) Asignar el dispositivo de almacenamiento de autorización al lector, por ejemplo, esto se efectúa asignando los datos del dispositivo a los datos del lector o definiendo que los datos del dispositivo sustituyan a los datos del lector y que se utilicen en su lugar;
- b) Modificar el software del lector o la aplicación almacenada en el lector, o ambos;
- 40 c) Situar el dispositivo de almacenamiento de autorización dentro de un rango de interacción del lector y separado de la interfaz sin contacto por una distancia esencialmente fija.

45 La invención ampara además un producto de programa informático para su uso en un sistema de autorización. El producto de programa informático comprende un código de programa legible por ordenador en un medio legible por ordenador. El sistema de autorización comprende un lector con unos datos del lector, una tarjeta con unos datos de la tarjeta y un dispositivo de almacenamiento de autorización con los datos del dispositivo. El sistema de autorización comprende además un módulo lógico configurado para asignar al lector y a la tarjeta entre sí y para hacer operable una interacción lector - tarjeta entre el lector y la tarjeta. La interacción lector - tarjeta se basa en los datos del lector y en los datos de la tarjeta, siendo los datos de autorización datos del lector y datos de la tarjeta del sistema de autorización. El producto de programa informático comprende unas instrucciones para hacer que el módulo lógico lea por medio de una interfaz sin contacto del lector de los datos del dispositivo a partir del dispositivo de almacenamiento de autorización, y asignar el lector a la tarjeta en base a los datos del dispositivo y, de esta manera, ser operable la interacción lector - tarjeta.

50 Las demás formas de realización descritas anteriormente con referencia al sistema de autorización son aplicables de la misma forma al procedimiento de operación de la interacción en el sistema de autorización, respectivamente el

procedimiento de asignación en el sistema de autorización entre sí del lector y de la tarjeta, y al producto de programa informático.

El término tarjeta debe entenderse que ampara una pluralidad de tarjetas (una población de tarjetas, un inventario de tarjetas). Pueden almacenarse la misma aplicación o diferentes aplicaciones (tarjetas multiaplicación). Las tarjetas así como las aplicaciones pueden suministrarse por los mismos o diferentes propietarios / proveedores independientes de las tarjetas o propietarios / proveedores de la aplicación, respectivamente. El término tarjeta incluye todas las formas de realización físicas diferentes conocidas para realizar una portadora de datos portátiles así como una tarjeta visualizada, por ejemplo una tarjeta simulada sobre una PDA. Los términos lector y dispositivo de almacenamiento de autorización deben considerarse similares al término tarjeta. El término datos, en particular datos del lector, datos de la tarjeta y datos del dispositivo, ampara todos los diferentes datos utilizados y manejados en el sistema de autorización y no están limitados a los datos de autorización. Los datos también amparan los datos derivados de los datos en un módulo lógico del sistema de autorización. Ejemplos de datos son:

i) Datos de identificación para identificar un dispositivo o la aplicación, efectuada por medio de un número de serie, un número de identificación exclusivo o seguro o un identificador de aplicación;

ii) Datos operacionales utilizados en el sistema de autorización, incluyendo los datos de autorización;

iii) Datos de seguridad. Los datos de seguridad pueden considerarse como un subconjunto de los datos operaciones;

iv) Datos de aplicación.

El término aplicación debe considerarse en sentido amplio e incluye al menos unos datos de aplicación y un código de aplicación. El término aplicación se refiere además a una única aplicación o a múltiples aplicaciones, suministradas o bien por los mismos o diferentes propietarios / proveedores de aplicación. Múltiples aplicaciones pueden ser completamente independientes entre sí o respecto de diferentes propietarios / proveedores de las aplicaciones, respectivamente, o pueden depender o interactuar entre sí.

El término hacer operable (hacer ejecutable) ampara todos los manejos de datos y las interacciones que han sido llevadas a cabo en el sistema de autorización para ofrecer una interacción habilitada, controlada, alterada, corregida o actualizada o para ofrecer una aplicación ejecutada o conseguir una aplicación ejecutable, respectivamente.

El término norma de un sistema de autorización debe entenderse como cualquier tipo de datos utilizados para definir e imponer una relación entre los diferentes dispositivos del sistema de autorización y / o las aplicaciones. Todas las normas definen conjuntamente lo que se autoriza con respecto a la interacción entre los dispositivos o con respecto a la ejecución de la aplicación o ambas. En un sistema de autorización jerárquico las normas están también relacionadas y / o dependen de los niveles jerárquicos. Los niveles jerárquicos son utilizados como barrera adicional de los datos mediante la definición de las posibilidades de interacción entre diferentes niveles jerárquicos.

Breve descripción de los dibujos

La presente invención se analizará con mayor detalle, a modo de ejemplo, con referencia a los dibujos. La descripción y los dibujos no deben considerarse que limitan la invención según las reivindicaciones.

Fig. 1 muestra un sistema de autorización de acuerdo con la invención con una tarjeta, un lector, y un dispositivo de almacenamiento de autorización inalámbrico;

Fig. 2 muestra una secuencia de una etapa de interacción en un sistema de autorización de acuerdo con la invención;

Fig. 3 muestra un sistema de autorización de acuerdo con la invención con un lector móvil;

Fig. 4 muestra un sistema de autorización de acuerdo con la invención con varios dispositivos de almacenamiento de autorización inalámbricos;

Fig. 5 muestra un sistema de autorización de acuerdo con la invención con dos lectores móviles;

Fig. 6 muestra con detalle un sistema de autorización estándar de acuerdo con la técnica anterior;

Fig. 7 muestra con detalle un sistema de autorización de acuerdo con la invención;

Fig. 8 muestra otro detalle de un sistema de autorización de acuerdo con la invención;

Fig. 9 muestra otro detalle de un sistema de autorización de acuerdo con la invención;

Fig. 10 muestra un sistema de autorización de acuerdo con la invención y un testigo de transferencia

Descripción detallada de las formas de realización preferentes

La **Fig. 1** muestra un sistema 10 de autorización de acuerdo con la presente invención. El sistema 10 de autorización comprende un lector 1, una tarjeta 2, un dispositivo de almacenamiento de autorización (ASD) 5 inalámbrico y un módulo lógico del sistema 10 de autorización (véase la Fig. 7). El lector 1 comprende una interfaz 11 de lector para una interacción 92 lector - tarjeta con la tarjeta 2 y una interfaz 12.1 sin contacto para una interacción 95 lector - dispositivo sin tarjeta entre el lector 1 y el ASD 5, así como los medios requeridos para una interacción, por ejemplo una memoria 14 del lector o una lógica 13 del lector utilizadas como módulo lógico (véase la Fig. 7). La tarjeta 2 y el ASD 5 comprenden una interfaz 21 de la tarjeta o una interfaz 51.1 del dispositivo, respectivamente, para la interacción con el lector 1. La tarjeta 2 puede ser o bien una tarjeta 2.1 sin contacto o bien una tarjeta 2.2 de contacto (véase la Fig. 7). Por consiguiente, la interacción 92 lector - tarjeta es o bien una interacción 92.1 sin contacto (interacción inalámbrica sin contacto) o una interacción 92.2 cableada respectivamente con contacto (véase la Fig. 7). El ASD 5 está dispuesto separado de la interfaz 12.1 sin contacto a una distancia 9 esencialmente fija, al menos durante la interacción 95 lector - dispositivo. La distancia 9 fija define un desplazamiento invariable entre el ASD 5 y la interfaz 12.1 sin contacto, realizado por el montaje espacial del sistema 10 de autorización, en particular la posición del ASD 5 en relación con la interfaz 12.1 sin contacto. Una vez que el ASD 5 ha sido finalmente situado dentro del rango de interacción del lector 1, el ASD 5 es en general inamovible con respecto a la interfaz 12.1 sin contacto. Por consiguiente, el ASD 5 está también dispuesto separado de la interfaz 12.1 sin contacto a la distancia 9 fija durante la interacción 92 lector - tarjeta. Ejemplos de montaje espacial son: el ASD 5 está permanentemente instalado a continuación del lector 1; el ASD 5 está fijado sobre el lector 1 por ejemplo fuera del lector; o el ASD 5 está situado dentro del lector.

En el sistema 10 de autorización, el dispositivo 5 de almacenamiento de autorización está configurado para hacer operable al menos una interacción efectuada o transmitida por el lector 1, en particular la interacción 92 lector - tarjeta. Con mayor detalle, el módulo lógico del sistema 10 de autorización, por ejemplo la lógica 13 del lector, está configurada para ser utilizada o interactuar con el ASD 5, en particular para leer datos por medio de la interfaz 92.1 sin contacto a partir del ASD 5, y para asignar al lector 1 la tarjeta 2 para hacer operable la interacción 92 lector - tarjeta (véase la Fig. 7). El módulo lógico comprende un producto de programa informático (con las instrucciones correspondientes) para controlar una unidad de procesamiento.

Una distancia 9 fija se escoge dentro del rango de interacción inalámbrico de la interfaz 12.1 sin contacto. La distancia 9 fija se efectúa, de modo preferente, de manera segura, al menos en operación normal. De una manera segura significa que la manipulación del ASD 5, o que un acceso al ASD 5 por el usuario de la tarjeta o por el propietario / proveedor del sistema 10 de autorización, no es posible sin modificar el hardware del lector 1 o el montaje espacial del sistema 10 de autorización. Pueden efectuarse otros montajes espaciales del sistema utilizando una antena desplazada que comprenda la interfaz 12.1 sin contacto, disponiéndose la antena desplaza a distancia de un recinto del lector 1 que comprende la interfaz 11 del lector.

Pueden implementarse otros medios o procedimientos para verificar que la distancia 9 fija no ha sido alterada, por ejemplo una verificación de la presencia del ASD 5 o una verificación de la señal de interacción del ASD 5. Dicha verificación de la presencia puede efectuarse mediante una interacción periódica entre el lector 1 y el ASD 5; por ejemplo, el lector 1 lee al menos el número de identificación único (UID) del ASD 5, de forma periódica. La verificación de la señal de interacción puede efectuarse analizando si la señal del ASD 5 satisface determinados valores de umbral, o bien predefinidos tras el montaje o definidos sobre la marcha. Los umbrales pueden estar relacionados con el nivel de salida de la señal de interacción o con las diferencias entre el nivel (pico) de salida de la señal de interacción y con las bandas laterales de interacción.

La **Fig. 2** muestra el sistema 10 de autorización con el lector 1, la tarjeta 2, el dispositivo 5 de almacenamiento de autorización inalámbrico, una unidad 3 periférica y un anfitrión 4. Dentro del sistema 10 de autorización son posibles las siguientes interacciones básicas: la interacción 92 lector - tarjeta entre el lector 1 y la tarjeta 2; la interacción 95 lector - dispositivo entre el lector 1 y el ASD 4; una interacción 94 de unidad / lector - anfitrión entre el lector 1 y el anfitrión 4 y / o la unidad 3 periférica. En un sistema de autorización accionado por el lector, en el que el lector 1 es el dispositivo activo e inicia la interacción con la tarjeta 2 y el ASD 5 y, por tanto, la tarjeta 2 y el ASD 5 son dispositivos pasivos, tienen lugar las siguientes etapas de interacción:

a) Etapa S1: el lector 1, inicia la interacción 92 lector - tarjeta pidiendo una contestación a partir de la tarjeta 2.

b) Etapa S2: el lector 1 verifica mediante la interacción 95 lector - dispositivo la presencia del ASD 5. Si un ASD está presente, el lector 1 interactúa 95 con el ASD 5 para obtener los datos de autorización, en particular, los datos 75 del dispositivo (véase la Fig. 7), que falta en el lector 1 o la tarjeta 2 y que se necesita en el proceso de autorización o autenticación, por ejemplo para en último término operar o hacer operable la interacción 92 de lector - tarjeta. Este es, por ejemplo, el caso cuando la tarjeta 2 está presente y es reconocida por el lector 1 mediante la lectura del UID de la tarjeta, pero el lector 1 no puede seguir interactuando con la tarjeta 2, porque los datos 72 de la tarjeta almacenados en la tarjeta 2 no se corresponden con los datos 71 del lector almacenados en el lector 1 (véase la Fig. 7).

c) Etapa S3: el lector 1 interactúa con la tarjeta 2, por ejemplo para ejecutar una aplicación 80 (véase la Fig. 7).

d) Etapa S4: el lector 1 interactúa con la unidad 3 periférica o con el anfitrión 4 con respecto a la aplicación 80.

Esta secuencia de interacciones abrevia simbólicamente (S1, S3 [S2], S4), porque la Etapa S3 depende de la Etapa S2 o la Etapa S3 resulta operable por la Etapa S2, respectivamente.

5 Con respecto al orden de las etapas de interacción, son posibles otras secuencias:

a) (S1 [S2], S3, S4): Etapas S2 / S1 - Etapa S3 - Etapa S4, de forma que la Etapa S1 depende de la Etapa S2; este significa que el lector 1, en primer término, verifica la presencia de un ASD 4. Si un ASD 5 está presente, el lector 1 intenta iniciar la interacción 92 lector - tarjeta o la tarjeta 2 en base a los datos 75 del dispositivo recibidos del ASD 5.

10 b) (S1, S3, S4 [S3]): etapa S1 - etapa S3 - etapas S2 / S4, de forma que la etapa S4 depende de la etapa S2.

También son posibles combinaciones de estas secuencias, por ejemplo 8S1 [S2], S3 [S3], S4 [S2]), de manera que la Etapa S2 se lleva cabo una vez o varias veces para posibilitar el control o la actualización de las Etapas S1, S2 y S4.

15 La **Fig. 3** muestra el sistema 10 de autorización de acuerdo con la invención con el lector 1, la tarjeta 2 y dos dispositivos 5a, 5b de almacenamiento de autorización. En una primera configuración I el lector 1, interactúa 92 con la tarjeta 2. A continuación, el lector 1 es deslocalizado con una primera deslocalización 19a hasta una segunda configuración II. En la segunda configuración II, el lector 1, respectivamente, la interfaz 12.1 sin contacto (remítase a la Fig. 7), es situada separada del primer ASD 5a por la primera distancia 9a fija durante la interacción 95 lector - dispositivo. En la configuración II el lector 1 puede interactuar 92 con la tarjeta 2 o con otras tarjetas. Mediante una segunda deslocalización 19b, el lector 1 es desplazado hasta una tercera configuración III en la que el lector 1 queda dispuesto separado del segundo ASD 5b por la segunda distancia 9b fija durante una siguiente interacción 95 lector - dispositivo. Esta forma de realización muestra cómo en cada configuración el montaje espacial entre el lector 1y el ASD 5a, 5b, si está presente, se caracteriza por la distancia 9a, 9b fija, o incluso si el lector 1 cambia de posición.

20 Un ejemplo con configuraciones diferentes sería una aplicación de acceso relacionada con un elevador. En la planta baja, un usuario presenta su tarjeta al lector permanentemente montado sobre el ascensor para acceder al ascensor (correspondiente a la configuración I). Dentro del ascensor, solicitaría acceder, por ejemplo, al piso 10°. Una vez alcanzado el 10° piso el lector pide al ASD (correspondiente a la configuración II) en base, por ejemplo, al UID de la tarjeta leído por el lector en la planta baja y temporalmente almacenado en el lector, si el usuario puede efectivamente acceder al 10° piso. La aplicación de acceso o el acceso efectivo por el usuario, efectivamente, está sometido a un doble control: un primer control cuando el lector está leyendo la tarjeta y un segundo control en base a la interacción lector - dispositivo en el piso 10°, habilitándose al lector, respectivamente, para continuar o terminar la aplicación de acceso.

25 Como se muestra en la **Fig. 3**, el dispositivo 5 de almacenamiento de autorización inalámbrico y el lector 1 pueden ser configurados solo temporalmente en la distancia 9 fija, dependiendo del desplazamiento 19 o de la posición real del lector 1 con respecto al ASD 5, respectivamente.

30 La **Fig. 4** muestra el sistema 10 de autorización de acuerdo con la invención, que comprende un lector 1, tres tarjetas 2a, 2b, 2c y dos dispositivos 5a, 5b de almacenamiento de autorización inalámbricos dispuestos en las distancias 9a, 9b fijadas. El primer ASD 5a está relacionado con la primera y la segunda tarjetas 2a, 2b, el segundo ASD 5b está relacionado con la tercera tarjeta 2c.

35 La invención permite el uso de ASD 5a, 5b diferentes, que se añaden posteriormente al sistema 10 de autorización, para hacer operable una interacción llevada a cabo o transmitida por el lector 1, por ejemplo la interacción 92 lector - tarjeta con las diferentes tarjetas 2a, 2b, 2c, y en el que las tarjetas 2a, 2b, 2c son añadidas posteriormente al sistema 10 de autorización. Es posible el uso de diferentes ASD 5a, 5b, siempre que el lector 1 tenga unas capacidades anticollision u otras capacidades para seleccionar un único ASD de una pluralidad de ASDs.

40 La **Fig. 5** muestra el sistema 10 de autorización que comprende dos lectores 1a, 1b, la tarjeta 2 y el dispositivo 5 de almacenamiento de autorización inalámbrico. En primer lugar, el primer lector 1a interactúa 92 con la tarjeta 2. A continuación, después del primer desplazamiento 19a, el primer lector 1a interactúa 95 con el ASD 5 dispuesto a la primera distancia 9a fija. Más tarde, el segundo lector 1b interactúa 92 con la tarjeta 2 o con otra tarjeta. Más tarde aún, después del segundo desplazamiento 19b, el segundo lector 1b interactúa 95 con el mismo ASD 5 dispuesto a la segunda distancia 9b fija. En este sistema 10 de autorización, el ASD 5 es asignado a varios lectores 1a, 1b diferentes.

45 Un ejemplo de dicha configuración sería una aplicación para acceder a una caja de seguridad de un banco. La caja fuerte del banco comprende una pluralidad de cajas de seguridad, cada una de las cuales comprende el lector, y unos emplazamientos de las diversas cajas en los que la caja puede ser abierta, cada una de las cuales comprende el ASD. Con esta tarjeta bancaria, el usuario puede identificarse y retirar su caja de seguridad para sustituirla en el

emplazamiento de la apertura de la caja. Solo después de la verificación satisfactoria del usuario y / o de la caja de seguridad por el ASD, el usuario puede abrir la caja de seguridad.

La **Fig. 6** muestra un sistema 100 de autorización estándar cerrado conocido en la técnica anterior. El sistema 100 estándar comprende un lector 101 de la etiqueta, una etiqueta 102.1 sin contacto y una etiqueta 102.2 con contacto. Así mismo, el sistema 100 estándar puede comprender la unidad 3 periférica y / o el anfitrión 4, ambos conectados al lector 101 de la etiqueta. El lector 101 de la etiqueta comprende la interfaz 11 del lector, la lógica 13 del lector configurada y utilizada como módulo lógico y lógicamente conectada a la interfaz 11 del lector, y la memoria 14 lógicamente conectada a la lógica 13 del lector. La interfaz 11 del lector es, o bien una interfaz 11.1 del lector sin contacto para la interacción 92.1 sin contacto con la etiqueta 102.1 sin contacto o, como alternativa o adicionalmente, una interfaz 11.2 del lector con contacto para la interacción 92.2 con contacto con la etiqueta 102.2 con contacto.

En el lector 101 de la etiqueta, un secreto 171 del lector es almacenado, por ejemplo en la lógica 13 del lector en la interfaz 11.1 del lector o en la memoria 14 del lector. Así mismo, el lector 101 de la etiqueta contiene la aplicación 80, por ejemplo almacenada en la memoria 14 del lector. En la etiqueta 102, son almacenadas un secreto 172 de la etiqueta y la aplicación 80. El secreto 171 del lector y el secreto 172 de la etiqueta se corresponden entre sí y definen un secreto 170 de habilitación, por ejemplo datos de autorización. Ejemplos de secretos 170 de habilitación son claves de acceso, claves de sesión, algoritmos, etc., utilizados para asignar manualmente, por ejemplo, la etiqueta 102 y el lector 101 de la etiqueta o la etiqueta 102 o el lector 101 de la etiqueta, respectivamente, y la aplicación 80. Para iniciar la interacción 92 lector - tarjeta de forma segura (interacción segura), o para obtener un acceso seguro a la aplicación 80, tanto el secreto 171 del lector como el secreto 172 de la etiqueta tienen que ser mantenidos en secreto. Por consiguiente, ambos tienen que ser almacenados en la etiqueta 102 y en el lector 101 de la etiqueta de una manera que no pueda ser alterada, leída, alterada o de cualquier otra forma modificada, salvo con el permiso expreso de, por ejemplo, el propietario / proveedor del sistema estándar o del propietario / proveedor de la aplicación 80, respectivamente. En resumen, el secreto 170 de habilitación puede estar relacionado con el sistema 100 de autorización estándar cerrado propiamente dicho o con la aplicación 80 realizada dentro del sistema 100 estándar, o con ambos. En particular, el secreto 170 de habilitación está configurado para hacer operable la interacción 92 lector - tarjeta entre la etiqueta 102 y el lector 101 de la etiqueta, y / o la ejecución de la aplicación 80. Así mismo, partes del secreto 170, en general, el secreto 171 del lector, o incluso un secreto del anfitrión, pueden ser almacenados en el anfitrión 4 para mejorar la seguridad o para la ejecución especial de la aplicación dependiendo de la presencia del anfitrión.

El lector 101 de la etiqueta puede también comprender una interfaz 112.2 lector - módulo para una interacción 195 lector - módulo con contacto entre la lógica 13 del lector y un módulo 105 seguro, por ejemplo un módulo de identidad de abonado (SIM) o un módulo de aplicación segura (SAM). En general, el módulo 105 seguro es parte integrante del lector 101 de la etiqueta y está permanentemente conectado al lector 101 de la etiqueta cuando el lector 101 de la etiqueta es inicialmente instalado. En el módulo 105 seguro, está almacenado un secreto 175 del módulo que en general es inaccesible e inmodificable. En la mayoría de los casos, el módulo 105 seguro es, por ejemplo, realizado como una tarjeta inteligente insertada de modo permanente en el lector 101 de la etiqueta. El módulo 105 seguro está interactuando con el lector 101 de la etiqueta a través de los contactos. Por tanto, la velocidad de la interacción 195 lector - módulo con contacto es lenta en comparación con una interacción sin contacto. En general, el secreto 175 del módulo completamente sustituye el secreto 101 del lector, y por eso no hay ningún secreto almacenado en el lector 101 de la etiqueta. En este caso, la habilitación 170 del secreto se define por la correspondencia del secreto 171 de la etiqueta y del secreto 175 del módulo.

La **Fig. 7** muestra el sistema 10 de autorización de acuerdo con la invención, que comprende el lector 1, la etiqueta 102.1 sin contacto, la tarjeta 2.1 sin contacto, la tarjeta 2.2 con contacto (del sistema estándar) - en suma, la tarjeta 2, la unidad 3 periférica, el anfitrión 4, y el dispositivo 5 de almacenamiento de autorización inalámbrico. Como se conoce en la técnica anterior, el lector 1 comprende la interfaz 11 del lector, la lógica 13 del lector, y la memoria 14 del lector. La lógica 13 del lector es utilizada como módulo lógico del sistema 10 de autorización. Sin tener en cuenta el ASD 5, el módulo lógico está configurado para asignar entre sí el lector 1 y la tarjeta 2 en base a los correspondientes datos 71 del lector (por ejemplo, el secreto 171 del lector) y los datos 72 de la tarjeta (por ejemplo, el secreto 172 de la tarjeta), haciendo con ello operable la interacción 92 lector - tarjeta entre el lector 1 y la tarjeta 2. Así, la interacción 92 lector - tarjeta se basa en los datos 71 del lector y en los datos 72 de la tarjeta, siendo ambos - o pertenecientes a - datos de autorización del sistema 10 de autorización. Así mismo, el lector 1 comprende la interfaz 12.1 sin contacto para la interacción 95 lector - dispositivo con el ASD 5. La tarjeta 2 y el ASD 5 comprenden la interfaz 21 de la tarjeta y una memoria de la tarjeta y la interfaz 51.1 del dispositivo y una memoria del dispositivo, respectivamente. ambos pueden además comprender una lógica de la tarjeta y una lógica del dispositivo, respectivamente, para manejar los datos. El módulo lógico está configurado para leer los datos 75 del dispositivo a partir del ASD 5, como interacción 95 lector - dispositivo o como parte de dicha interacción. El módulo lógico está también configurado para asignar el lector 1 a la tarjeta 2 para hacer operable la interacción 92 lector - tarjeta en base a los datos 75 del dispositivo, en particular utilizado los datos 75 del dispositivo para sustituir, o actualizar o corregir, los datos 71 del lector. El ASD 5 está dispuesto separado de la interfaz 12.1 sin contacto a la distancia 9 fija. La interfaz 11 del lector puede ser configurada como una interfaz 11.1 del lector sin contacto para la interacción 92.1 lector - tarjeta sin contacto entre el lector 1 y la tarjeta 2.1 sin contacto o la etiqueta 102.1 sin contacto y - alternativa o adicionalmente - como una interfaz 11.2 del lector con contacto para la interacción 92.2 lector - tarjeta

con contacto del lector 1 con la tarjeta 2.2 de contacto. La interfaz 11.1 del lector sin contacto para la interacción 92.1 lector - tarjeta sin contacto puede funcionar como interfaz 12.1 sin contacto para la interacción 95 lector - dispositivo. Así mismo, en el lector 1 están almacenados el secreto 171 del lector y, en la etiqueta 102.1 sin contacto, el secreto 172 de la etiqueta, como se conoce en la técnica anterior. En el lector 1 y la etiqueta 102.1 sin contacto, está almacenada la aplicación 80, en particular una primera aplicación 80a relacionada con el sistema 100 de autorización estándar. En la tarjeta 2.1 sin contacto y en la tarjeta 2.2 con contacto, están almacenados los datos 72 de la tarjeta y la aplicación 80, en particular una segunda aplicación 80b relacionada con el sistema 10 de autorización. La segunda aplicación 80b puede también estar almacenada en el lector 1. Los datos 72 de la tarjeta básicamente se corresponden con los datos 71 del lector almacenados en términos amplios dentro del lector 1 del sistema 10 de autorización. Conjuntamente, los datos 72 de la tarjeta y los datos 71 del lector son utilizados para formar o definir los datos 70 de habilitación, en particular utilizando los datos 75 del dispositivo para alterar (sustituir, actualizar, corregir) los datos 71 del lector. Los datos 70 de habilitación son básicamente comparables con el secreto 170 de habilitación y pueden ser utilizados para implementar las mismas funciones, por ejemplo métodos o procedimientos de autorización. Los datos 70 de habilitación son utilizados por el módulo lógico para hacer operable al menos la interacción 92 lector - tarjeta. En el caso de que, en el sistema 10 de autorización, no exista ningún dato 71 del lector almacenado en el lector 1 - que es el caso del lector 1 mostrado en la Fig. 7 -, o en el caso de que los datos 71 del lector no sean asignados a los datos 72 de la tarjeta, los datos 72 de la tarjeta y los datos 75 del dispositivo almacenados en el ASD 5 son asignados entre sí para ser utilizados como datos 70 de habilitación. En el caso de que, en el sistema 10 de autorización, los datos 71 del lector almacenados en el lector 1 sean incompletos, por ejemplo, los datos 71 del lector no proporcionan acceso a una determinada aplicación 80 almacenada en la tarjeta 2 o en el caso de que los datos 71 del lector estén relacionados con una versión más antigua de los datos de autorización que los datos 72 de la tarjeta, los datos 75 del dispositivo son utilizados para alterar los datos 71 del lector. En este caso, los datos 72 de la tarjeta, los datos 71 del lector y los datos 75 del dispositivo almacenados en el ASD 5 son asignados entre sí para ser utilizados como datos 70 de habilitación. En el sistema 10 de autorización, los datos 70 de habilitación están configurados para hacer operable al menos una interacción llevada a cabo o transmitida por el lector 1, por ejemplo la interacción 92 lector - tarjeta, y la interacción 94 de unidad / lector - anfitrión o la interacción 95 lector - dispositivo. Como alternativa o adicionalmente, los datos 70 de habilitación están configurados para hacer ejecutable o ejecutar la segunda aplicación 80b. Básicamente, en el sistema 10 de autorización de acuerdo con la invención, los datos 75 del dispositivo están configurados para alterar (sustituir, actualizar, corregir) los datos 71 del lector. Desde un punto de vista funcional, al menos con respecto a que pueda hacerse operable la interacción 92 lector - tarjeta, los datos 75 del dispositivo, al menos en parte son utilizados para alterar los datos 71 del lector o actúan como datos 71 del lector, respectivamente. El módulo lógico está configurado en la medida correspondiente.

Así mismo, los datos 70 de habilitación pueden ser utilizados por el módulo lógico del sistema 10 de autorización para hacer operable, o bien una interacción que se lleve a cabo y se transmita por el lector 1 y que dependa del ASD 5 o bien los datos 75 de dispositivo, por ejemplo, también una interacción 94-2 de unidad / tarjeta - anfitrión entre la tarjeta 2 y la unidad 3 periférica o el anfitrión 4, respectivamente, una interacción 95 - 2 dispositivo - tarjeta entre al ASD 5 y la tarjeta 2, o una interacción 95.4 unidad / dispositivo - anfitrión entre el ASD 5 y la unidad 3 / anfitrión 4. Como alternativa o adicionalmente, los datos 70 de habilitación pueden ser configurados para asegurar las interacciones. Los datos 70 de habilitación, en particular los datos 75 del dispositivo son utilizados como característica de seguridad o nivel de seguridad adicional. Así mismo, los datos 70 de habilitación pueden ser configurados para acceder de forma segura a la segunda aplicación 80b (acceso seguro) o para ejecutar de forma segura la segunda aplicación 80b (ejecución segura).

Los datos 75 del dispositivo almacenados en el ASD 5, o el ASD 5 en cuanto tal, son asignados al lector 1. Por tanto, el lector 1 puede interactuar con el ASD 5 o viceversa, con respecto a los datos 70 de habilitación que estén o bien relacionados con el sistema 10 de autorización propiamente dichos (sistema relacionado) o bien que esté relacionado con la aplicación 80 realizada dentro del sistema 10 de autorización (aplicación relacionada), o con ambos.

La autorización para que el módulo lógico lleve a cabo la interacción 95 lector - dispositivo de acuerdo con la invención, se implementa básicamente por una modificación del software del lector o por la aplicación 80 ejecutada por el lector. La modificación ampara un cambio parcial o completo (sustitución, actualización, corrección) del software del lector. Por ejemplo, los siguientes pueden ser modificados: el sistema operativo, los datos operacionales, los subprogramas, los ajustes, los parámetros, los algoritmos o funciones. Cuando el ASD 5 es utilizado con respecto a la aplicación 80, entonces también la aplicación 80 tiene que ser modificada en una manera en la que la aplicación 80 pueda ser ejecutada por el lector 1, ya sea por el software original, no modificado del lector o por el software del lector modificado.

El lector 1 puede ser configurado para la interacción 92.1 lector - tarjeta sin contacto por medio de la interfaz 11.1 del lector e utilizando una primera frecuencia y, para la interacción 95 lector - dispositivo sin contacto por medio de la interfaz 12.1 sin contacto utilizando una segunda frecuencia o la primera frecuencia. Utilizando dos interfaces físicas o dos frecuencias, la interacción 92.1 lector - tarjeta la interacción 95 lector - dispositivo puede producirse incluso simultáneamente. La interfaz 11.1 del lector y la interfaz 12.1 sin contacto puede realizarse como una entidad única o incluso como una entidad única, por ejemplo una interfaz con una sola antena, utilizando las mismas o diferentes frecuencias.

El lector 1 puede ser también configurado para utilizar un primer protocolo (para codificación, comunicación) para la interacción 92.1 lector - tarjeta sin contacto por medio de la interfaz 11.1 del lector y para utilizar un segundo protocolo, o el primer protocolo para la interacción 95 lector - dispositivo sin contacto por medio de la interfaz 12.1 sin contacto. Utilizando dos protocolos diferentes, la interacción 92.1 sin tarjeta y la interacción 95 lector - dispositivo pueden producirse simultáneamente. Dependiendo del lector 1 con respecto a los protocolos de interacción, protocolos de los que varias combinaciones respecto de las cuales sean posibles la interacción. Una primera combinación puede ser que el protocolo para la interacción 92.1 lector - tarjeta con la etiqueta 102.1 o la tarjeta 2.1 difiera del protocolo para la interacción 95.1 lector - dispositivo. En una segunda combinación, el protocolo para la interacción 92.1 lector - tarjeta con la tarjeta 2.1 es la misma que el protocolo para la interacción 95 lector - dispositivo, y difiere del protocolo para la interacción 92.1 lector - tarjeta con la etiqueta 102.1.

Utilizando las mismas frecuencias y el mismo protocolo para la interacción 92.1 lector - tarjeta y la interacción 95 lector - dispositivo, básicamente no hay diferencia entre estas dos interacciones. Para el lector 1 - desde el punto de vista de la interacción - el dispositivo 5 de almacenamiento de autorización es simplemente otra tarjeta 2.1 sin contacto u otra etiqueta 102.1 sin contacto.

El sistema que sigue muestra la forma en que el dispositivo 5 de almacenamiento de autorización es utilizado para potenciar, o para ejecutar sistemas de autorización genéricos, en particular para conmutar el primer sistema 100a de autorización cerrado que comprende la etiqueta 102 y el lector 101 de la etiqueta al sistema 10 de autorización el cual comprende así mismo la tarjeta 2. En el primer sistema 100a de autorización cerrado, la pertenencia del sistema se define por el secreto 70 de habilitación, en particular el secreto 171 del lector y el secreto 172 de la etiqueta. Por consiguiente el lector 101 de la etiqueta no puede interactuar 95 con la tarjeta 2 que no contiene el secreto 172 de la etiqueta. La asignación del ASD 5 con los datos 75 del dispositivo al lector 101 de la etiqueta, o viceversa, utilizando los datos 75 del dispositivo como datos 71 del lector para formar los datos 70 de habilitación, el lector 101 de la etiqueta es reconfigurado para convertirse en el lector 1. A continuación, el lector 1 puede interactuar 92 con la tarjeta 2. El ASD 5 es utilizado para transformar el lector 1 de la etiqueta en el lector 1, siendo el lector 1 de un nivel más genérico que el lector 101 de la etiqueta. El primer sistema 100a de autorización cerrado se convierte en una parte del sistema 10 de autorización (potenciado, de calidad mejorada, hecho genérico).

El nivel más genérico del sistema 10 de autorización se materializa en las capacidades de interacción potenciadas que permiten fusionar el primer sistema 100a de autorización cerrado y un segundo sistema 100b de autorización cerrado que comprende la tarjeta 2 en un sistema 10 de autorización único. En particular, el segundo sistema 100b de autorización cerrado comprende una tarjeta 2.1 sin contacto y un segundo lector (lector de la etiqueta) 101b. El segundo lector 101b de la etiqueta comprende la interfaz 11.1 del lector, la lógica 13 del lector en la que los datos 71 del lector están almacenados, y la memoria 14 en la que está almacenada la segunda aplicación 80b. Para el segundo sistema 100b de autorización cerrado, la pertenencia del sistema se define por o se deriva de los datos 70 de habilitación, en particular de los datos 72 de la tarjeta y de los datos 71 del lector.

La transformación del lector 101 de la etiqueta en el lector 1 se realiza sin cambio alguno del hardware del lector 1 de la etiqueta. Todo lo que se necesita es situar el dispositivo 5 de almacenamiento de autorización inalámbrico dentro del rango de interacción del lector 101 de la etiqueta y asignar el ASD 5 al lector 101 de la etiqueta (para convertirse en el lector 1), o viceversa. La asignación del ASD 5 y del lector 1 puede realizarse por la modificación del software del lector 101 de la etiqueta o del software ejecutado por el lector 1, respectivamente. Como alternativa o adicionalmente, la aplicación 80, en particular la segunda aplicación 80b, ejecutada por el lector 1 tiene que ser modificada. Debido a que la aplicación 80 es básicamente también solo una pieza del software, la modificación de la aplicación 80 es tan fácil como adoptar el software del lector.

Es posible almacenar la segunda aplicación 80b como aplicación adicional en la etiqueta 102.1, por ejemplo por medio del secreto 171 del lector y del secreto 172 de la tarjeta, el dispositivo 5 de almacenamiento de autorización puede además ser utilizada para mejorar la calidad del primer sistema 100a de autorización cerrado, que comprende la etiqueta 102.1 y el lector 101 de la etiqueta, para incluir la segunda aplicación 80b, que es básicamente controlada por el secreto 70, en particular por los datos 72 de la tarjeta y por los datos 71 del lector del segundo sistema 100b cerrado. En el primer sistema 100a cerrado de calidad mejorada (que es ahora el sistema de autorización potenciado), el acceso a la segunda aplicación 80b se efectúa utilizando el secreto 171 del lector para acceder a la etiqueta 102.1 con el secreto 172 de la etiqueta, y utilizando los datos 70 de habilitación como simulación o sustitución de los datos 71 del lector para acceder y / o ejecutar la segunda aplicación 80.

En base a la **Fig. 7**, se describirá con mayor detalle la secuencia (S1, S3 [S2], S4) de la **Fig. 2**: en primer lugar, el lector 1 envía una señal de autenticación y lleva a cabo una anticollisión hasta el punto en que se solicite para conseguir la respuesta de la tarjeta 2, por ejemplo, el UID de la tarjeta, para identificar la tarjeta 2 (Etapa S1). En base a dicha identificación, el lector 1 conoce qué tipo de interacción 92 se establecerá, por ejemplo una interacción 92 segura lector - tarjeta sin contacto de acuerdo con el protocolo ISO / IEC 14443 o un protocolo de propietario. En el caso de que el lector 1 tenga todos los datos 70 de habilitación necesarios para establecer la interacción segura, por ejemplo porque los datos 71 del lector están almacenados en el lector 1, el lector 1 inicia la interacción segura. Este escenario se corresponde con la secuencia conocida en la técnica anterior (Etapa S3). En el caso de que el lector 1 carezca de determinados o de todos los datos 70 de habilitación, los datos 70 de habilitación que faltan son recuperados - por medio del módulo lógico configurado paralelamente - del dispositivo 5 de almacenamiento de

autorización. Por tanto, el lector 1 interactúa 95 con el ASD 5. La interacción 95 puede incluir la lectura de los datos 75 del dispositivo y la asignación de los datos 75 del dispositivo y de los datos 72 de la tarjeta hasta la lógica 13 del lector para hacer operable la interacción 92 lector - tarjeta, o para la ejecución de la aplicación 80. La interacción 95 puede también incluir el traspaso de los datos 72 de la tarjeta al ASD 5. La lógica del dispositivo actúa ahora como módulo lógico para manejar los datos 72 de la tarjeta junto con los datos 75 del dispositivo para posibilitar la interacción 92 lector - tarjeta, o para ejecutar la aplicación 80. En el caso de que la lógica del dispositivo esté manejando los datos 70 de habilitación, básicamente se establece una interacción 95-2 dispositivo - tarjeta. El lector 1 está básicamente actuando como un transmisor de interacción y solo es utilizado para transmitir (para tunelizar) la interacción entre el ASD 5 y la tarjeta 2. Por ejemplo, el ASD 5 codifica los comandos individuales de la interacción 92 lector - tarjeta (los comandos serán enviados por el lector 1 a la tarjeta 2) y envía estos comandos al lector 1 utilizando la primera codificación, por ejemplo un protocolo de propietario o instrucciones atómicas. En base a los comandos recibidos del ASD 5, el lector 1 interactúa 92 con la tarjeta 2, ya sea utilizando también la primera codificación o, después de la traslación hasta el lector 1, utilizando una segunda codificación, por ejemplo un protocolo estandarizado como el ISO / IEC 14443 o el NFC. De manera análoga, el lector 1 envía (tuneliza) al ASD 5, con o sin traslación de la codificación, las respuestas enviadas desde la tarjeta 2 hasta el lector 1, para una gestión adicional de los datos por el ASD 5 y la posterior interacción 95-2 dispositivo - tarjeta, si es que debe efectuarse.

Desde el punto de vista del usuario de la tarjeta, solo la interacción 92 lector - tarjeta está en marcha, de modo similar a la Etapa S3 de la técnica anterior, aunque la interacción 92 lector - tarjeta se hace operable por el ASD 5, o por los datos 75 del dispositivo y, por tanto, depende de la Etapa S2 (Etapa S3 [S2]).

Si es oportuno, por ejemplo, ejecutar la aplicación 80 sobre la unidad 3 periférica mediante la lectura de los datos de aplicación a partir de la unidad 3 periférica o escribiendo los datos de aplicación en la unidad 3 periférica, la interacción 94 de unidad / lector - anfitrión tiene lugar durante o después de la interacción 95-2 dispositivo - tarjeta o de la interacción 92 lector - tarjeta (Etapa S4).

Dependiendo de si la lógica 13 del lector, la lógica de la tarjeta o la lógica del dispositivo o incluso una lógica de la unidad 3 periférica y / o del anfitrión 4 es utilizada como módulo lógico del sistema 10 de autorización para gestionar los datos 70 de habilitación en particular los datos 75 del dispositivo, son posibles otros diversos escenarios de secuencias. Por ejemplo, el ASD 5 puede ser utilizado para hacer operable la interacción 95-2 dispositivo - tarjeta o la interacción 95-4 de unidad / dispositivo - anfitrión.

El dispositivo 5 de almacenamiento de autorización inalámbrico permite realizar un sistema 10 de autorización de un nivel más genérico. Desde el punto de vista del usuario de la tarjeta o de la aplicación 80 almacenada en la tarjeta 2, en el sistema 10 de autorización, el usuario de la tarjeta tiene siempre la impresión de que la tarjeta 2 está interactuando 92 solo con el lector 1 y, en particular, que todos los datos 71 del lector son almacenados en el lector 1. Para el usuario de la tarjeta, en particular el usuario de la tarjeta 2.1 sin contacto (con los datos 72 de la tarjeta), no hay diferencia entre el segundo sistema 100b de autorización cerrado, que comprende la tarjeta 2.1 y el segundo lector 101b de la etiqueta (con los datos 71 del lector), y el sistema 10 de autorización, en base al primer sistema 100b de autorización cerrado y que comprende la etiqueta 102.1 (con el secreto 172 de la etiqueta) y el lector 101 de la etiqueta (con el secreto 171 del lector) y potenciándose de acuerdo con la invención.

La **Fig. 8** muestra la forma en que el sistema 10 de autorización el dispositivo 5 de almacenamiento de autorización inalámbrico es utilizado para actualizar el lector 1 con respecto a los datos 70 de habilitación que faltan. Los datos 70 de habilitación que faltan pueden ser datos que no han sido almacenados en el lector 1 cuando no fueron originalmente instalados o introducidos en el sistema de autorización, pero que se necesitan cuando más adelante son añadidas al sistema de autorización nuevas tarjetas (con nuevas aplicaciones) o nuevas aplicaciones (almacenadas en la tarjeta existente).

El lector 1 comprende un solo componente que integra la interfaz 11.1 del lector sin contacto, la interfaz 12.1 sin contacto, la lógica 13 y la memoria 14. La interfaz 11.1 del lector y la interfaz 12.1 sin contacto se realizan como una sola unidad funcional (componente electrónico), o como un subgrupo del componente. Almacenados en la tarjeta 2 se encuentran los primeros datos 72a.i. de la tarjeta, la primera aplicación 80a asociada con los segundos datos 72b.ii de la tarjeta, y la segunda aplicación 80b asociados con los terceros datos 72c.ii de la tarjeta. Los primeros datos 72a.i de la tarjeta están relacionados con el sistema 10 de autorización (sistema relacionado). Los segundos y tercer datos 72b.ii, 72c.ii están relacionados con las aplicaciones 80a, 80b (aplicación relacionada). Pueden ser utilizados ya sea o bien uno o ambos datos relacionados con el sistema o datos relacionados con la aplicación, para implementar las normas de un sistema de autorización. En el lector 1 son almacenados los segundos datos 71b.ii del lector. Los primeros datos 71a.i del lector faltan y, en su lugar, se realizan por medio del ASD 5 como primeros datos 75a.i del dispositivo. Por consiguiente, desde un punto de vista funcional relacionado con la autorización, los primeros datos 71a.i del lector y los primeros datos 75a.i del dispositivo son idénticos. Así mismo, en el ASD 5 son almacenados los segundos datos 75b.ii del dispositivo. Los primeros datos 71a.i del lector o los primeros datos 75a.i del dispositivo, respectivamente, están relacionados con el sistema. Los segundos datos 71b.ii del lector y los segundos datos 75b.ii del dispositivo están ambos relacionados con la aplicación. Debido a que los primeros datos 71a.i del lector faltan, la interacción 92 lector - tarjeta puede solo tener lugar cuando el ASD 5 está presente. Para ejecutar la primera aplicación 80a almacenada en la tarjeta 2, los primeros datos 75a.i del

dispositivo almacenados en el ASD 5, son necesarios para acceder a la tarjeta 2, y los segundos datos 75b.ii del lector almacenados en el lector 1 son necesarios para acceder a la segunda aplicación 80b. Para ejecutar la segunda aplicación 80b, de nuevo se necesitan los primeros datos 75a.i del dispositivo para acceder a la tarjeta 2, y los segundos datos 75b.ii del lector almacenados en el ASD 5 se necesitan para acceder a la primera aplicación 80b.

La **Fig. 9** muestra la tarjeta 2 con los primeros datos 72a.i de la tarjeta que están relacionados con el sistema, estando los segundo y tercer datos 72b.ii y 75c.iii relacionados con la primera o la segunda aplicación 80a, 80b, respectivamente. Así mismo, el sistema 10 de autorización comprende una etiqueta 102 con el secreto 172 de la etiqueta y la tercera aplicación 80c. El lector 1 comprende los datos 71.i del lector, que están relacionados con el sistema, y el ASD 5, fijado al exterior del lector 1. En el ASD 5 están almacenados los primero, segundo y tercero datos 75a.i, 75b.ii, 75c.ii del dispositivo. Los primeros datos 75a.i del dispositivo están relacionados con el sistema y, básicamente, se corresponden con el secreto 171 de la etiqueta que falta en el lector 1 y están relacionados con el secreto 172 de la etiqueta. Los segundo y tercer datos 75b.ii, 75c.ii del dispositivo están relacionados con la aplicación. Los primeros datos 75a.i del dispositivo del ASD 5 permite que el lector 1 interactúe 92 con la etiqueta 102 y ejecute la tercera aplicación 80c. Los segundo y tercer datos 75b.ii, 75c.ii del dispositivo que están relacionados con los segundo y tercer datos 72b.ii, 72c.ii de la tarjeta de las primera y segunda aplicaciones 80a, 80b, permiten que el lector 1 acceda a y ejecute dichas aplicaciones 80a, 80b.

Esta forma de realización muestra la forma en que el dispositivo 5 de almacenamiento de autorización inalámbrico es utilizado para hacer genérico el lector 1 con respecto a las tarjetas y / o las aplicaciones. Mediante el ASD, el lector 1 es habilitado para interactuar con la tarjeta y para acceder a la tarjeta (en cuanto tal) o para acceder a la tarjeta para ejecutar una aplicación. Así mismo, muestra la forma en que los datos 75.ii del dispositivo relacionado con la aplicación puede ser utilizado para incrementar la seguridad global del sistema 10 de autorización con respecto a las aplicaciones que pueden ser ejecutadas, o para acceder a la aplicación. Además de los datos 71 del lector, los datos 75 distantes pueden ser utilizados como un nivel de seguridad adicional con respecto a las aplicaciones 80 almacenadas en la tarjeta 2.

El lector 1 comprende un solo componente que integra la interfaz 11.1 del lector sin contacto, la interfaz 12.1 sin contacto, la lógica 13, y la memoria 14. La interfaz 11.1 del lector y la interfaz 12.1 sin contacto son realizadas o materializadas como dos unidades funcionales o como subgrupos del componente.

La **Fig. 10** muestra el uso de un testigo 6 de transferencia para transferir o cargar, o almacenar, respectivamente, los datos 75 del dispositivo o unos datos 79 de actualización en el dispositivo 5 de almacenamiento de autorización inalámbrico o en el lector 1. El testigo 6 de transferencia puede ser utilizado para almacenar secretos de la etiqueta, por ejemplo, el secreto 171 de la etiqueta, y datos del lector, por ejemplo los datos 71 del lector, en el lector 1 (véase la flecha de color gris de triple cabeza). El testigo de transferencia puede ser utilizado para almacenar los datos del dispositivo, por ejemplo los segundos datos 75b del dispositivo (véase la flecha de color gris de triple cabeza), y actualizar los datos, por ejemplo los primero y segundo datos 79a, 79b de actualización (véase la flecha de color gris de cabeza doble), en el ASD 5. Los primeros datos 79a de actualización están relacionados con el secreto 171 de la etiqueta y están configurados para corregir o actualizar los datos 79a del primer testigo 6a de transferencia. Los segundos datos 79b de actualización están relacionados con los primeros datos 75a del dispositivo y están configurados para corregir o actualizar dichos primeros datos 75a del dispositivo. Los primeros datos 75a del dispositivo han sido almacenados en el ASD 5, antes de la transferencia de los segundo datos 79b de actualización desde el segundo testigo 6b de transferencia. Los segundos datos 75b del dispositivo son básicamente idénticos a los primeros datos 71a del lector que faltan en el lector 1. En el ejemplo ofrecido, los segundos datos 75b del dispositivo son almacenados en los primero y segundo testigos 6a, 6b de transferencia y pueden ser transferidos desde uno cualquiera de estos dos testigos de transferencia (véase la flecha de color gris de triple cabeza). Cada testigo 6 de transferencia comprende una interfaz 61.1 del testigo (no mostrado) para una interacción sin contacto entre el testigo 6 y el lector 1, o bien utilizando la interfaz 11.1 del lector o la interfaz 12.1 sin contacto. Utilizando la interfaz 11.1 del lector, el testigo 6 es manejado por el lector 1 como otra tarjeta (y una interacción 92.1 lector - tarjeta) utilizando la interfaz 12.1 como otro ASD 5 (y una interacción 95 lector - dispositivo). La **Fig. 10** muestra la forma en que el testigo 6 de transferencia puede ser utilizado para corregir o actualizar el ASD 5, en particular los datos 75 del dispositivo (o incluso los datos 79 de actualización) almacenados en el ASD 5. El testigo 6 de transferencia puede ser utilizado para omitir la sustitución (el cambio) del ASD 5 o para omitir la adición de dispositivos de almacenamiento de autorización inalámbricos adicionales asignados al lector 1, en el caso de que el ASD 5 tenga que ser corregido o actualizado.

Referencias numerales

10	sistema de autorización	94	interacción de unidad / lector - anfitrión
1	lector	94-2	interacción de unidad / tarjeta - anfitrión
2	tarjeta	95	interacción lector - dispositivo
3	unidad periférica	95-2	interacción dispositivo - tarjeta
4	anfitrión	95-4	interacción de unidad / dispositivo - anfitrión
5	dispositivo de almacenamiento de autorización, asd		
6	testigo de transferencia	100	sistema de autorización cerrado
9	distancia fija	101	lector de etiqueta
11	interfaz de lector	102	etiqueta
12.1	interfaz sin contacto	105	módulo seguro
13	lógica de lector	112.1	interfaz módulo - lector
14	memoria de lector	170	secreto de habilitación
19	deslocalización	171	secreto de lector
21	interfaz de tarjeta	172	secreto de etiqueta
51.1	interfaz del dispositivo	175	secreto de módulo
61.1	interfaz de testigo	195	interacción lector - módulo
70	datos de habilitación		
71	datos de lector	...1	sin contacto
72	datos de tarjeta	...2	con contacto
75	datos de dispositivo	...a., ...b., ...c, ...	primeros, segundos, terceros, ...
79	datos de actualización	...i	relacionados con el sistema
80	aplicación	...ii	relacionados con la aplicación
90	interacción	S1, S2, S3, S4	etapas
92	interacción lector - tarjeta		

REIVINDICACIONES

- 1.- Un sistema (10) de autorización que comprende:
- Un lector (1) para una interacción (92) lector - tarjeta con una tarjeta (2);
- 5 Un módulo lógico configurado para asignar el lector (1) y la tarjeta (2) entre sí para hacer operable la interacción (92) lector - tarjeta en base a los datos (71) de lector del lector (1) y los datos (72) de tarjeta de la tarjeta (2), siendo los datos (71) del lector y los datos (72) de la tarjeta datos de autorización del sistema (10) de autorización;
- 10 el módulo lógico está además configurado para leer, por medio de una interfaz (12.1) sin contacto los datos (75) del dispositivo a partir de un dispositivo (5) de almacenamiento de autorización, y para asignar el lector (1) a la tarjeta (2) y para hacer operable la interacción (92) lector - tarjeta en base a los datos (75) del dispositivo mientras el dispositivo (5) de almacenamiento de autorización está presente dentro de un rango de interacción de la interfaz (12.1) sin contacto, **caracterizado porque** el dispositivo (5) de almacenamiento de autorización está dispuesto separado de la interfaz (12.1) sin contacto a una distancia (9) fija, y el módulo lógico está configurado para verificar que la distancia (9) fija no ha sido alterada.
- 15 2.- El sistema (10) de autorización de acuerdo con la reivindicación 1, **caracterizado porque** el módulo lógico está configurado para utilizar los datos (75) del dispositivo para alterar los datos (71) del lector para hacer operable la interacción (92) lector - tarjeta.
- 20 3.- El sistema (10) de autorización de acuerdo con la reivindicación 1 o 2, **caracterizado porque** el módulo lógico está configurado para hacer operable una de las siguientes interacciones: una interacción (95) lector - dispositivo entre el lector (1) y el dispositivo (5) de almacenamiento de autorización, y una interacción (95-2) tarjeta - dispositivo entre la tarjeta (2) y el dispositivo (5) de almacenamiento de autorización transmitido por el lector (1).
- 4.- El sistema (10) de autorización de acuerdo con una de las reivindicaciones 1 a 3, **caracterizado porque** el módulo lógico está dispuesto en el lector (1).
- 5.- El sistema (10) de autorización de acuerdo con una de las reivindicaciones 1 a 4, **caracterizado porque** el módulo lógico está configurado para ejecutar una aplicación (80).
- 25 6.- El sistema (10) de autorización de acuerdo con una de las reivindicaciones 1 a 5, **caracterizado porque** el módulo lógico está configurado para utilizar los datos (75) del dispositivo para asegurar una acción entre la interacción (92) lector - tarjeta y una ejecución de una aplicación (80).
- 30 7.- El sistema (10) de autorización de acuerdo con una de las reivindicaciones 1 a 6, **caracterizado porque** el módulo lógico está configurado para usar los datos (75) del dispositivo para imponer una entre una pertenencia al sistema de autorización del lector (1) y una norma del sistema (10) de autorización, de modo preferente un sistema de autorización jerárquico.
- 35 8.- El sistema (10) de autorización de acuerdo con una de las reivindicaciones 1 a 7, **caracterizado porque** el dispositivo (5) de almacenamiento de autorización está configurado para que resulte inoperable o para borrar los datos (75) del dispositivo cuando son suprimidos a partir de una distancia (9) fija, entre el dispositivo (5) de almacenamiento de autorización y la interfaz (12.1) sin contacto o un rango de interacción del lector.
- 9.- El sistema (10) de autorización de acuerdo con una de las reivindicaciones 1 a 8, **caracterizado porque** el lector (1) comprende un medio para una de las siguientes verificaciones: una verificación de presencia del dispositivo (5) de almacenamiento de autorización y una verificación de la señal de interacción del dispositivo (5) de almacenamiento de autorización.
- 40 10.- El sistema (10) de autorización de acuerdo con una de las reivindicaciones 1 a 9, **caracterizado porque** el sistema (10) de autorización comprende al menos uno entre una unidad (3) periférica y un anfitrión (4) conectado al lector (1) y el módulo lógico está configurado para asignar el lector (1) a la unidad (3) periférica o al anfitrión (4) para hacer operable al menos una interacción (94) de unidad / lector - anfitrión entre el lector (1) y la unidad (3) periférica o el anfitrión (4), una interacción (94-2) de unidad / tarjeta - anfitrión entre la tarjeta (2) y la unidad (3) periférica o el anfitrión (4) y una interacción (95-4) de unidad / dispositivo - anfitrión entre el dispositivo (5) de almacenamiento de autorización y la unidad (3) periférica o el anfitrión (4).
- 45 11.- El sistema (10) de autorización de acuerdo con una de las reivindicaciones 1 a 11, **caracterizado porque** una interfaz (11) de lector del lector (1) utilizada para la interacción (92) lector - tarjeta está configurada para actuar como interfaz (12.1) sin contacto.
- 50 12.- Un procedimiento de asignación en un sistema (10) de autorización de un lector (1) y de una tarjeta (2) entre sí en base a los datos (71) del lector y a los datos (72) de la tarjeta utilizados como datos de autorización del sistema (10) de autorización, que comprende las etapas de:

- a) Leer por un módulo lógico, unos datos (75) del dispositivo a partir de un dispositivo (5) de almacenamiento de autorización por medio de una interfaz (12.1) sin contacto del lector (1);
- b) Utilizar los datos (75) del dispositivo para asignar el lector (1) a la tarjeta (2) y para hacer operable una interacción (92) lector - tarjeta entre el lector (1) y la tarjeta (2) mientras el dispositivo (5) de almacenamiento de autorización está presente dentro de un rango de interacción de la interfaz (12.1) sin contacto, en el que el dispositivo (5) de almacenamiento de autorización está dispuesto separado de la interfaz (12.1) sin contacto a una distancia (9) esencialmente fija; y
- c) Verificar que la distancia (9) fija no ha sido alterada.
- 13.- Un producto de programa informático para su uso en un sistema (10) de autorización, presentando el sistema (10) de autorización un lector (1) con unos datos (71) del lector; una tarjeta (2) con unos datos (72) de la tarjeta; un módulo lógico configurado para asignar el lector (1) y la tarjeta (2) entre sí y para hacer operable una interacción (92) lector - tarjeta entre el lector (1) y la tarjeta (2) en base a los datos (71) del lector y a los datos (72) de la tarjeta, siendo los datos (71) del lector y los datos (72) de la tarjeta datos del sistema (10) de autorización; y un dispositivo (75) de almacenamiento de autorización con unos datos (75) del dispositivo; en el que
- el producto de programa informático comprende unas instrucciones para hacer que el módulo lógico lea, por medio de una interfaz (12.1) sin contacto del lector (1), los datos (75) del dispositivo a partir del dispositivo (5) de almacenamiento de autorización, para asignar el lector (1) al dispositivo (5) de almacenamiento si está presente dentro de un rango de interacción de la interfaz (12.1) sin contacto, **caracterizado porque** el dispositivo (5) de almacenamiento de autorización está dispuesto separado de la interfaz (12.1) sin contacto a una distancia (9) esencialmente fija, y para verificar que la distancia (9) fija no ha sido alterada.

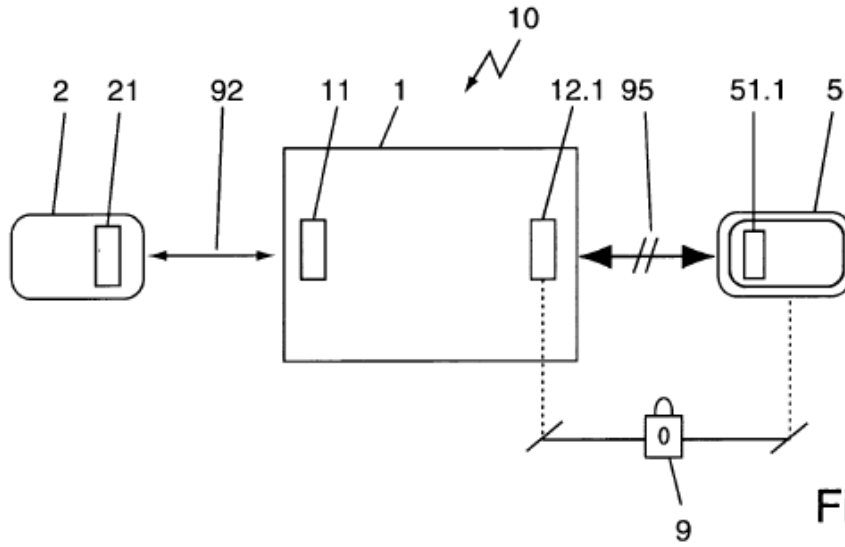


Fig. 1

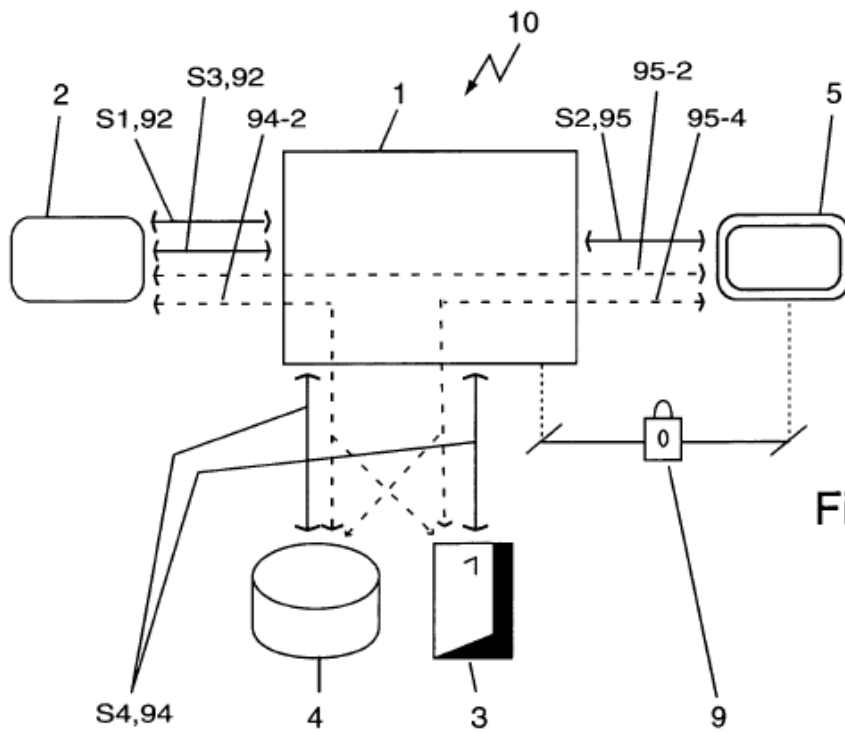
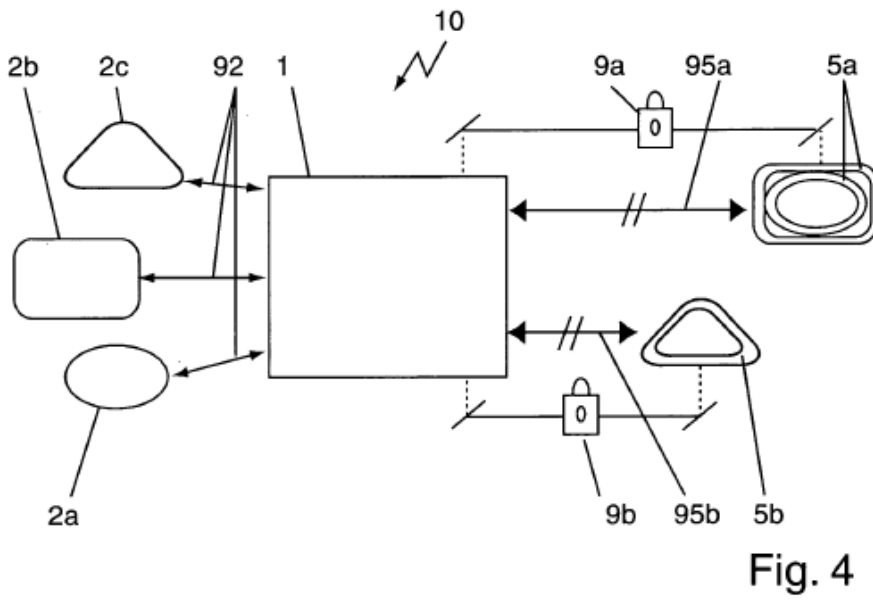
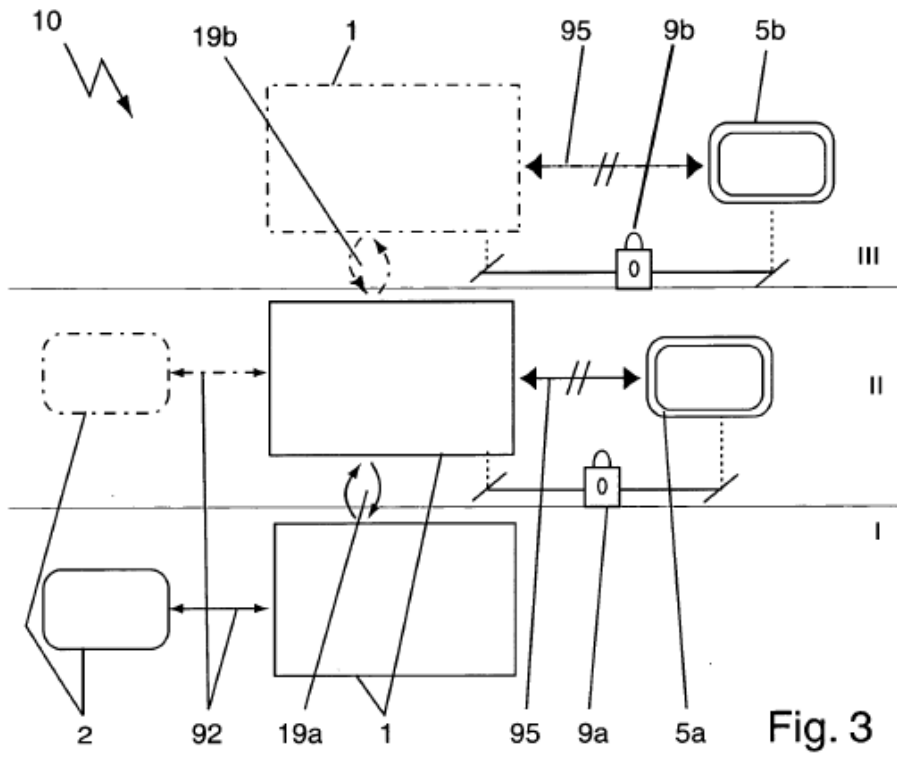


Fig. 2



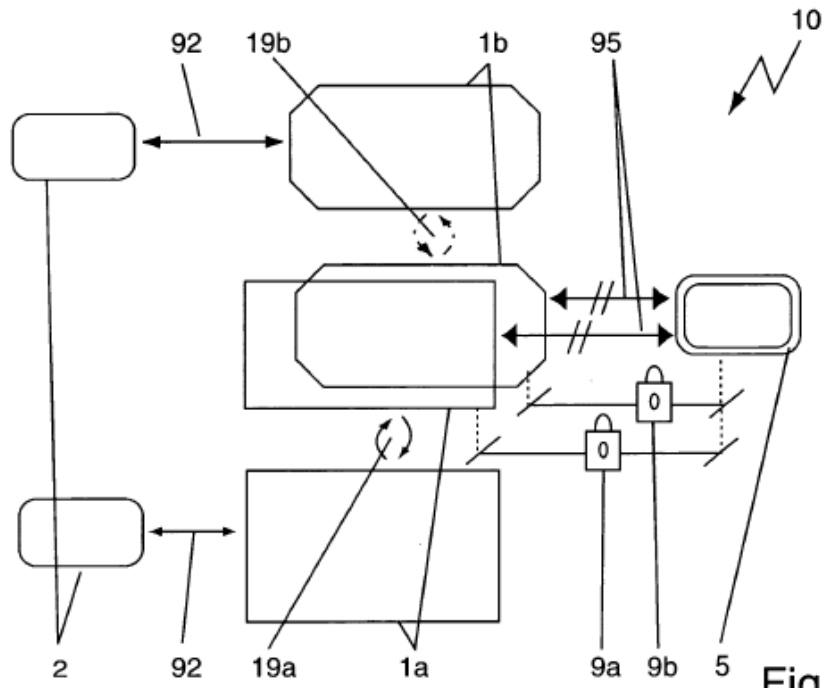


Fig. 5

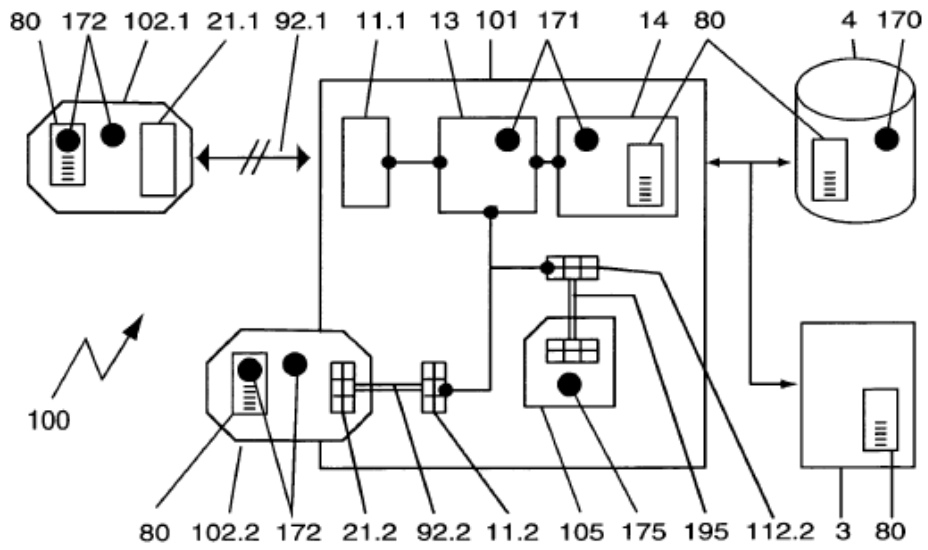


Fig. 6

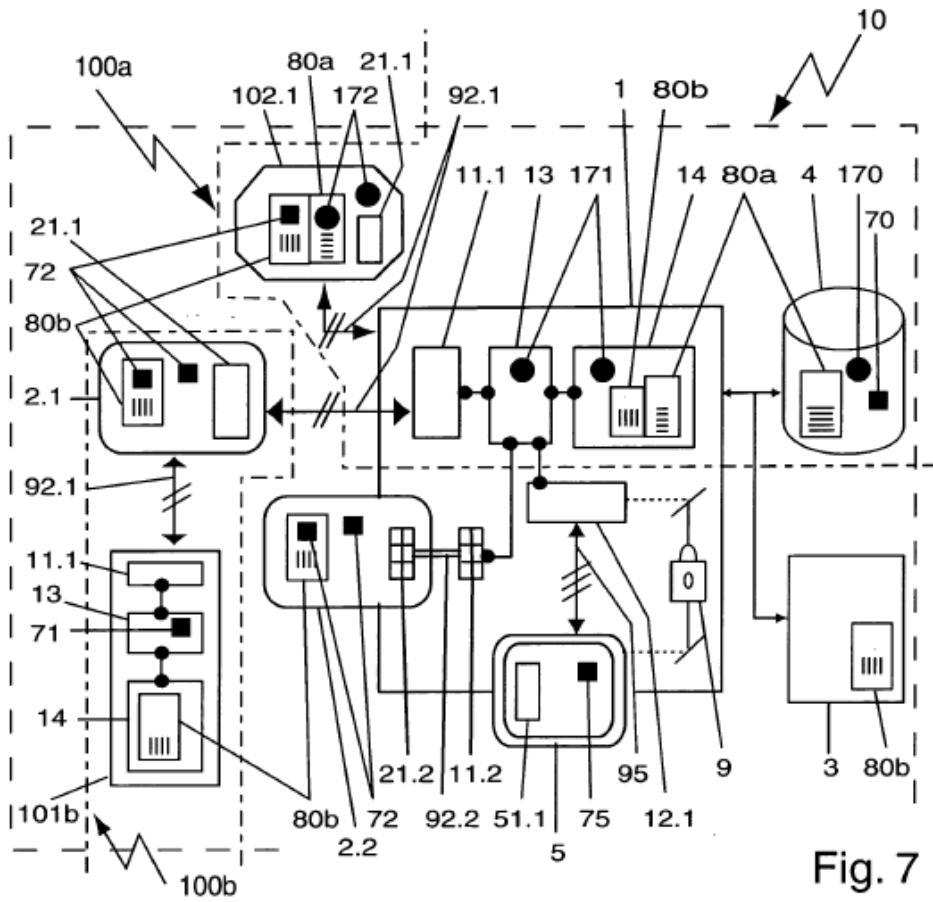


Fig. 7

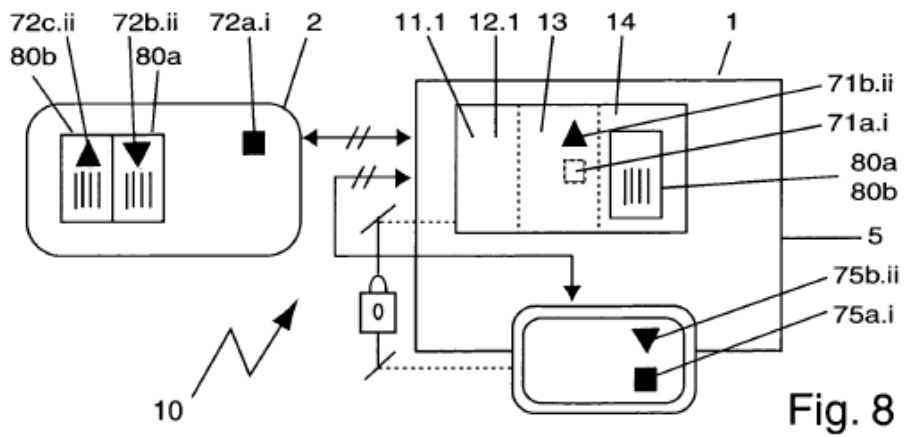


Fig. 8

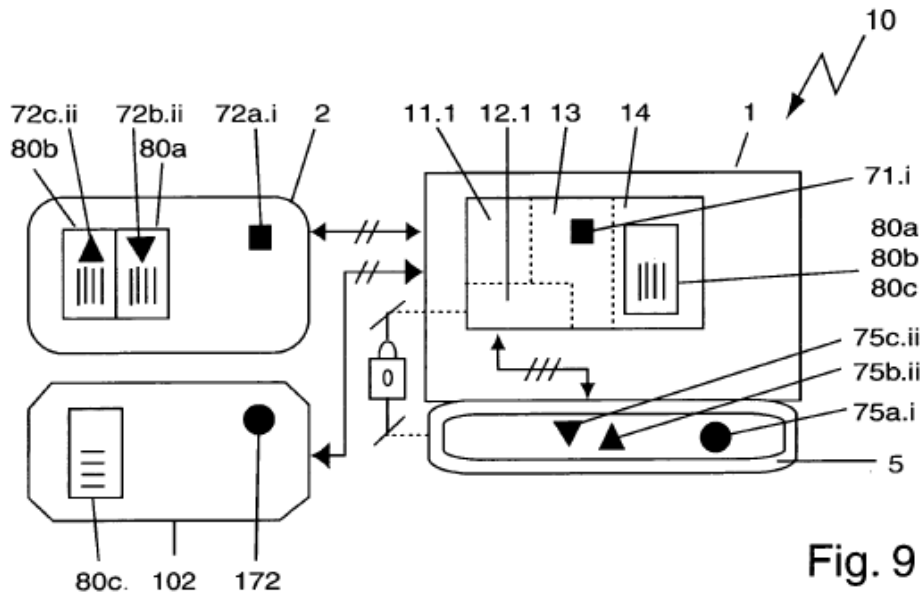


Fig. 9

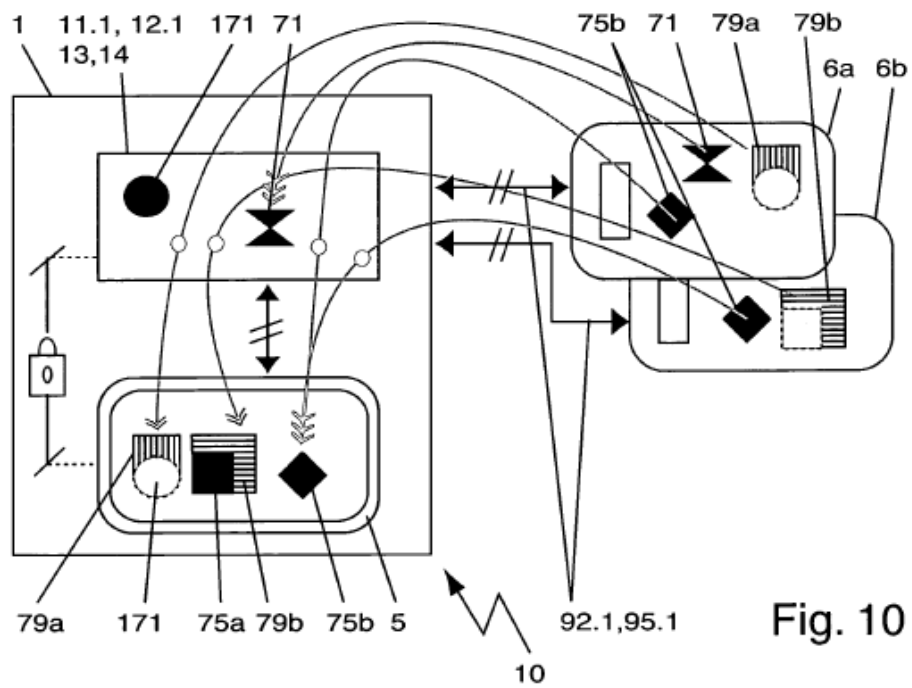


Fig. 10