(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 400 934**

(51) Int. CI.:

G06K 19/077 (2006.01)
G06K 19/07 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.11.2008 E 08874470 (1)**

(97) Fecha y número de publicación de la concesión europea: **09.01.2013 EP 2286373**

(54) Título: **Lector y transpondedor para ocultar las aplicaciones soportadas por un lector y/o transpondedor, y procedimiento correspondiente**

(30) Prioridad:

26.05.2008 EP 08104090

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.04.2013

(73) Titular/es:

NXP B.V. (100.0%)
High Tech Campus 60
5656 AG Eindhoven, NL

(72) Inventor/es:

STERN, SUSANNE;
HUBMER,PAUL;
THUERINGER, PETER;
MURRAY, BRUCE;
NEUMANN, HEIKE y
DE JONG, HANS

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Lector y transpondedor para ocultar las aplicaciones soportadas por un lector y/o un transpondedor, y procedimiento correspondiente

Sector de la invención

La invención se refiere a un transpondedor que tiene almacenada una serie de aplicaciones diferentes, a un lector diseñado para decodificar datos recibidos desde un transpondedor, y a un procedimiento para la ocultación de las aplicaciones soportadas por un lector y/o un transpondedor. Además, la presente invención se refiere a un elemento de programa. Adicionalmente, la invención se refiere a un medio legible por ordenador.

Antecedentes de la invención

Los datos transmitidos entre un lector y un transpondedor (en particular, una tarjeta inteligente o una etiqueta RFID), son codificados de manera que un atacante no puede conseguir los datos y utilizarlos para actos delictivos. Para datos personales, datos de contabilidad, números de tarjetas de crédito, y similares, es muy evidente la utilización de esta codificación. Dado que las nuevas tarjetas inteligentes pueden emular más tarjetas inteligentes, es decir, soportar un número de distintas aplicaciones, también las aplicaciones soportadas deben ser ocultadas. La utilidad de ello no es evidente a priori. No obstante, teniendo en cuenta una tarjeta que soporta aplicaciones de “Visa”, “American Express”, “Wal Mart” y “Subway New York”, la utilidad resulta evidente puesto que es muy probable que esta tarjeta pertenezca a un ciudadano de Estados Unidos. Con este “estigma”, puede pasar a ser blanco de un terrorista.

A continuación, se describirán algunas consideraciones adicionales respecto a sistemas de comunicación convencionales.

La privacidad puede ser relacionada a un individuo y a un grupo de personas que comparten unas ciertas características (por ejemplo, ciudadanos de EE.UU). La protección de la privacidad puede ser deseable.

La privacidad se puede perder de varias formas. Convencionalmente, el UID (Identificador Único) de la tarjeta utilizada en detección de colusión, es legible de modo directo. Por lo tanto, un usuario individual puede ser escaneado en varios lugares.

Una solución existente de modo convencional consiste en utilizar un ID Azar (RID). No obstante, incluso las aplicaciones auténticas en los lectores necesitan conocer cuál es la tarjeta con la que deben comunicar, de manera que existe todavía necesidad de un ID Lógico Único de Tarjeta (UCLID).

Cuando una tarjeta presenta este tipo, marca, etc., parece inocua. No obstante, el conocimiento de que este tipo de tarjeta X de un fabricante Y es utilizada por el metro de Nueva York y no ha sido adquirida por muchas ciudades revela que el portador de esta tarjeta es de manera muy probable un ciudadano de Nueva York.

Puede ser deseable que el descifrado de una clave utilizada para una aplicación no destruya la privacidad para otras aplicaciones.

Además, el documento WO 2006/003562 da a conocer un procedimiento para escoger un juego de datos de múltiples juegos de datos registrados en un dispositivo, de manera que cada juego de datos está asociado a una clave específica, en el que la información a intercambiar es codificada en el dispositivo utilizando una de las claves, la información de intercambio codificada es enviada al dispositivo en situación remota, es decodificada utilizando la clave almacenada en el dispositivo remoto, y entonces se devuelve al dispositivo la información de intercambio decodificada. A continuación, la información de intercambio es comparada con la información de intercambio decodificada. Si las dos son iguales, se ha encontrado el juego apropiado de datos, de otro modo, el ciclo empieza nuevamente con otra clave. Las funciones de dispositivo y dispositivo remoto pueden cambiar, de manera que el ciclo se puede iniciar en un dispositivo remoto. El documento WO 2006/003562 se refiere también a un dispositivo para presentar un juego de datos de múltiples juegos de datos registrados en el dispositivo a un dispositivo remoto.

No obstante, dicho procedimiento utiliza autentificaciones de prueba que requieren mucho tiempo. Además, no soporta lectores de aplicaciones múltiples.

El documento US 2004/0025035 A1 da a conocer un sistema de identificación electrónico sin contacto, en el que un transpondedor almacena datos de aplicación y datos de directorio comprendiendo identificadores de aplicación relativos a las aplicaciones almacenadas. Los datos de directorio son codificados por una unidad de lectura.

El documento US 6.126.078 da a conocer un soporte de identificación que almacena una serie de aplicaciones independientes y que es capaz de codificar los datos de transmisión y decodificar los datos recibidos comunicados con una estación de lectura y escritura.

Objetivo y resumen de la invención

Por lo tanto, es un objetivo de la invención dar a conocer un lector y/o transpondedor que puede funcionar de manera que preserva la privacidad.

El objetivo de la invención se consigue mediante un transpondedor, un lector, un procedimiento, un elemento de programa y un medio legible por ordenador, de acuerdo con las reivindicaciones independientes. De acuerdo con una realización a título de ejemplo, se da a conocer un transpondedor que comprende una unidad de almacenamiento que tiene almacenadas una serie de aplicaciones diferentes, una unidad de proceso que, a petición de un lector, está adaptada para generar una respuesta interpretable utilizando un esquema de codificación conocido tanto por el transpondedor como por el lector, de manera que el lector es capaz de determinar si una aplicación está soportada por el transpondedor al analizar la respuesta utilizando el esquema de codificación, y una unidad de transmisión adaptada para enviar la respuesta a dicho lector.

De manera más específica, de acuerdo con una realización a título de ejemplo, se da a conocer un transpondedor (que puede estar acoplado en comunicación con un lector) que tiene almacenadas una serie de aplicaciones diferentes (por ejemplo, una aplicación de una serie de aplicaciones soportadas por el transpondedor) que, a petición de un lector (por ejemplo, por un mensaje de comunicación transmitido desde el lector al transpondedor), amplía el nombre de la aplicación en un número al azar (por ejemplo, un verdadero número al azar o un seudo-número al azar, que puede ser generado por un generador de números al azar del transpondedor, o que puede ser almacenado en una unidad de almacenamiento del transpondedor), codifica o genera un MAC (es decir, genera un Código de Autentificación de Mensaje, MAC) con el número ampliado con una clave asociada con dicha aplicación (cuya clave puede ser también conocida por el lector) y envía el número codificado a dicho lector. De acuerdo con otra realización a título de ejemplo, se dispone de un lector que comprende una unidad de transmisión adaptada para enviar una petición a un transpondedor, indicativa de un número de aplicaciones soportadas por el lector, una unidad de análisis adaptada para analizar una respuesta recibida desde el transpondedor con un esquema de codificación conocido tanto por el transpondedor como por el lector, y una unidad de determinación adaptada para determinar si una aplicación está soportada por el transpondedor al analizar la respuesta utilizando el esquema de codificación.

De acuerdo con otra realización a título de ejemplo, se dispone de un lector (que puede estar acoplado en comunicación con un transpondedor) diseñado para decodificar datos recibidos desde un transpondedor con una clave (cuya clave puede ser también conocida por el transpondedor) asociada a una aplicación (por ejemplo, una o una serie de aplicaciones soportadas por el transpondedor) y para determinar si dicho número decodificado contiene un nombre de dicha aplicación. De acuerdo con otra realización adicional a título de ejemplo, se prevé un procedimiento para la ocultación de aplicaciones soportadas por un lector y/o un transpondedor, cuyo procedimiento comprende:

el lector envía una orden de petición a dicho transpondedor,
el transpondedor genera una respuesta interpretable utilizando un esquema de decodificación conocido tanto por el transpondedor como por el lector, y que es indicativa de si la aplicación está soportada por el transpondedor,
el transpondedor envía la respuesta a dicho lector, y
el lector determina si una aplicación está soportada por el transpondedor al analizar la respuesta utilizando el esquema de codificación.

De manera más específica, de acuerdo con otra realización a título de ejemplo, se da a conocer un procedimiento para la ocultación de aplicaciones soportadas por un lector y/o un transpondedor, cuyo procedimiento comprende:

el lector envía una orden de petición a dicho transpondedor,
el transpondedor amplía el nombre de una aplicación, que soporta, mediante un número al azar,
el transpondedor codifica o genera un MAC con el número ampliado con una clave asociada con dicha aplicación, enviando al transpondedor el número ampliado codificado o después de la generación de un MAC a dicho lector,
el lector decodifica dicho número ampliado codificado o verifica el MAC en dicho número ampliado codificado, y
el lector determina si dicho número ampliado decodificado o verificado contiene un nombre de una aplicación.

De acuerdo con otra realización a título de ejemplo de la invención, se facilita un elemento de programa (por ejemplo, una rutina de software, código fuente o en código ejecutable), de manera que, cuando está siendo ejecutada por un procesador, es adaptada para controlar o llevar a cabo un procedimiento de proceso de datos que tiene las características antes mencionadas.

De acuerdo con otra realización adicional a título de ejemplo de la invención, un medio legible por ordenador (por ejemplo, un CD, un DVD, un elemento USB, un disquete, o un disco duro) queda dispuesto de manera que almacena un programa de ordenador que, cuando es ejecutado por un procesador, es adaptado para controlar o llevar a cabo un procedimiento de proceso de datos que tiene las características anteriormente mencionadas.

El proceso de datos que se puede llevar a cabo, de acuerdo con realizaciones de la invención, se puede realizar por

un programa de ordenador, es decir, mediante software, o utilizando uno o varios circuitos electrónicos de optimización más especiales que se encuentran en forma de hardware o en forma híbrida, es decir, por medio de componentes de software y componentes de hardware.

El término “transpondedor” puede indicar especialmente una tarjeta RFID o una tarjeta inteligente (por ejemplo, sin contacto). De modo más general, un transpondedor puede ser un dispositivo (que comprende, por ejemplo, un chip) que puede transmitir automáticamente ciertos datos (por ejemplo, codificados) cuando es activado por una señal especial procedente de un interrogador.

El término “lector” puede indicar, en particular, una estación de base adaptada para enviar un haz de radiación electromagnética para leer un transpondedor y detectar una señal reflejada o emitida. El dispositivo lector puede estar adaptado como uno de un grupo que consiste en un dispositivo de lectura o escritura, un lector RFID, un lector de tarjeta de chip sin contacto, un transpondedor pasivo y un dispositivo de Comunicación en Campo Próximo (“Near Field Comunicatian”).

El término “aplicación” puede indicar en particular un servicio dentro de un sistema de comunicación formado por el lector y el transpondedor a cuyo servicio puede aportar una contribución el transpondedor. La disposición de dicha aportación puede comportar la capacidad del transpondedor en proporcionar datos almacenados o calculados, proporcionar capacidad de proceso, etc. Son ejemplos de dichos servicios el pago de una tarifa para utilizar un transporte público por el usuario del transpondedor, el pago de un precio de compra para un artículo mediante un sistema de pago inalámbrico, un servicio de tarjeta de crédito, etc.

El término “nombre de una aplicación” puede indicar particularmente un identificador o un código indicativo de las aplicaciones que permiten recuperar sin ambigüedades una aplicación específica basada en el identificador. Este nombre puede ser particularmente un código alfanumérico, tal como una secuencia de letras, una secuencia de números, o una combinación de letras y números.

El término “esquema de codificación” puede indicar particularmente cualquier esquema, rutina, o algoritmo aplicado para codificar un bloque de datos como base para un mensaje de comunicación, de manera que la interpretación del contenido del bloque de datos codificados requiere el conocimiento del esquema de codificación, por ejemplo, una o varias claves utilizadas para la codificación. Diferentes tipos de codificación que están comprendidos bajo este término, son una codificación simétrica (en la que las entidades asociadas en la comunicación pueden utilizar la misma clave en ambos lados) y una codificación pública (en la que las entidades asociadas en la comunicación pueden utilizar una clave pública, una clave privada, o similares). Particularmente, también la formación de un MAC (Código de Autenticación de Mensaje) (“Message Authentication Code”) y la formación de un CRC (Cyclic Redundancy Check (Comprobación de Redundancia Cíclica)), que es codificado posteriormente, se pueden considerar como forma de una codificación basada en un esquema de codificación.

El término “Message Authentication Code“ (MAC) (Código de Autenticación de Mensaje) puede indicar, en particular, un fragmento corto de información utilizada para autentificar un mensaje. Un algoritmo MAC puede aceptar como entrada una clave secreta y un mensaje de longitud arbitraria a autentificar, y puede emitir un MAC. El valor MAC puede proteger tanto la integridad de los datos del mensaje como su autenticidad al autorizar verificadores (que también poseen la clave secreta o la correspondiente clave pública).

El término “Cyclic Redundancy Check” (CRC) (Comprobación de Redundancia Cíclica), puede indicar particularmente un tipo de función (o una emisión de la misma), que adopta como entrada un flujo de datos de cualquier longitud, y produce como salida un valor de un determinado espacio, por ejemplo, un entero de un cierto número de bits. Se puede utilizar un CRC como suma de comprobación para detectar alteración de datos durante la transmisión.

Una realización de la invención puede ofrecer la ventaja de que la aplicación, soportada por el transpondedor, puede ser ocultada durante la transmisión de mensajes de comunicación entre un lector y un transpondedor. De acuerdo con ello, un atacante no puede conseguir información alguna de cuáles o cuántas aplicaciones están soportadas por un transpondedor, protegiendo de esta manera la privacidad de los asociados de la comunicación.

En una realización, también los datos procedentes del lector pueden ser ocultados, de manera que el atacante tampoco pueda conseguir información alguna de cuáles o cuántas aplicaciones están soportadas por el lector.

Algunos aspectos a título de ejemplo de realizaciones de la invención se mencionarán a continuación:

El lector puede comunicar un conjunto de aplicaciones que soporta y el transpondedor puede responder al lector si soporta una o varias de estas aplicaciones, y opcionalmente puede trasladar la identidad del transpondedor al lector.

Esta comunicación puede ser realizada de manera que mantenga la confidencialidad (es decir, que un atacante no pueda interpretar si el transpondedor soporta o no la aplicación y la integridad (de manera que el lector puede determinar que el transpondedor soporta la aplicación y, asimismo, que el lector pueda determinar que el

transpondedor soporta la aplicación en este momento, lo cual puede ser designado como “reciente” (“freshness”).

El lector puede seleccionar entonces la aplicación enviando un mensaje al transpondedor, que el transpondedor puede decodificar, pero del que un atacante no puede sacar conclusiones en cuanto al soporte.

La confidencialidad puede indicar que un atacante no puede determinar qué aplicación soporta el transpondedor, ni observando una comunicación en la que, por ejemplo, se puede transportar el nombre de la aplicación. Esta es la razón para codificar la comunicación. Tampoco, observando múltiples mensajes que, por ser idénticos, dan a conocer información, aunque estén codificados. Esta es la razón para incluir un número al azar.

La integridad puede indicar que el lector puede determinar, mediante la respuesta, que esta respuesta ha sido generada por un transpondedor que soporta la aplicación. Esto se puede realizar particularmente por una de las realizaciones siguientes a título de ejemplo, en las que muchas alternativas son posibles:

- Un MAC calculado sobre RND || ApplName (nombre de aplicación). Este traslada el soporte de la aplicación, pero no la identidad del transpondedor. En este caso, RND es un número al azar, y ApplName es una identidad de una aplicación.
- Un CRC calculado sobre una información, por ejemplo, RND || UCLID y a continuación el conjunto codificado (RND || UCLID || CRC). En este caso, UCLID es un identificador del transpondedor. La CRC proporciona integridad.
- Un MAC calculado sobre una información codificada, por ejemplo, sobre Enc(K. RND || UCLID). El MAC proporciona integridad. En este caso, Enc. es una función de codificación y K es una clave.

El carácter reciente o “freshness” se puede tratar de la siguiente manera: El lector puede enviar un número al azar, junto con una lista de aplicaciones que soporta. El transpondedor puede incluir este número al azar en base del cálculo de CRC o MAC. Esto puede impedir la nueva interpretación de respuestas anteriores del transpondedor.

La selección de la aplicación se puede realizar con confidencialidad (por lo tanto, codificación e inclusión de un número al azar), integridad (de manera que el transpondedor puede determinar que el mensaje es genuino), y carácter reciente “freshness” (razón para incluir alguna información al azar que ha proporcionado el transpondedor al lector en el proceso anterior).

En una realización, el soporte de la aplicación puede ser comunicado por el lector y el transpondedor responde de una manera que el lector puede determinar el soporte real, mientras que un atacante no puede determinarlo.

A continuación, se explicarán otras realizaciones a título de ejemplo del transpondedor. No obstante, estas realizaciones son aplicables también al lector, al procedimiento, al elemento de programa y al medio legible por ordenador.

Una unidad de proceso (tal como un circuito integrado del transpondedor, que tiene capacidades de proceso) del transpondedor puede ser adaptado para evaluar, cuando se recibe la petición de un lector indicativo de aplicaciones soportadas por el lector, cuál de la una o varias aplicaciones soportadas por el lector está soportada o están soportadas por el transpondedor, y para llevar a cabo la ampliación y aplicaciones para las solicitudes soportadas por el lector y soportadas por el transpondedor. Por lo tanto, el transpondedor puede reaccionar a la petición del lector generando una lista de aplicaciones que soporta el transpondedor y que soporta también el lector. De este modo, se puede conseguir un acuerdo entre transpondedor y lector con respecto a aplicaciones soportadas por ambas entidades.

La unidad de proceso puede estar adaptada para ampliar el nombre de la aplicación por el número al azar y una suma de comprobación antes de la codificación. Cualquiera de los nombres de las aplicaciones, los números al azar, la suma de comprobación, y las claves pueden tener cualquier secuencia de caracteres numéricos, secuencia de letras, o cualquier código alfanumérico. Si bien, realizaciones específicas pueden permitir añadir simplemente el nombre de la aplicación al número al azar, el sistema puede resultar incluso más seguro y menos sensible a fallos cuando adicionalmente al nombre de la aplicación y el número al azar también se añade una suma de comprobación al bloque de datos antes de ser codificado para la subsiguiente transmisión segura.

En una realización, la unidad de proceso del transpondedor puede ser adaptada para generar, para una aplicación que no está soportada por el transpondedor, asimismo, un número al azar. Una unidad de transmisión (tal como una antena) del transpondedor puede ser adaptada para enviar el número al azar generado a dicho lector. Añadiendo, asimismo, un bloque de datos para una aplicación que no está soportada por el transpondedor a un mensaje de transmisión, tal como un mensaje de comunicación, la longitud del mensaje de comunicación se puede hacer independiente del número de aplicaciones soportadas por el transpondedor. Por lo tanto, un atacante no puede deducir el número de aplicaciones (soportadas) analizando meramente la longitud del mensaje de comunicación. El número al azar generado para una aplicación que no está soportada por el transpondedor puede encontrarse libre de cualquier indicación de un nombre de la aplicación que no está soportada. De manera alternativa, el número al azar generado para una aplicación que no está soportada por el transpondedor puede estar acompañado por una indicación de un nombre de la aplicación que no está soportada y con una indicación del hecho de que esta

aplicación no está soportada.

La ventaja de que un simple análisis de la longitud del mensaje de comunicación enviado desde el transpondedor al lector no permite determinar el número de aplicaciones soportadas por el transpondedor, resulta especialmente apropiado cuando la unidad de proceso está adaptada, para la aplicación que no está soportada por el transpondedor, generando el número azar con una longitud que es la misma que la longitud del número codificado para una aplicación soportada por el transpondedor. Al tomar esta medida, el atacante no será capaz en absoluto de distinguir, basándose en la longitud de la sección de datos transmitida, si una aplicación específica está soportada o no está soportada por una de las entidades de comunicación. Esto puede aumentar adicionalmente la seguridad de los datos y la privacidad cuando funciona el sistema de comunicación.

El número al azar puede ser un número seudo-azar. En contraste con un número seudo-azar, un número verdadero al azar es un número producido independientemente de su criterio de generación. Para propósitos de codificación, los números basados en mediciones físicas se pueden considerar al azar. Los números seudo-azar pueden ser números, con un modelo lo menos detectable posible, pero no verdaderamente al azar. Los programas de ordenador pueden llevar a cabo números seudo-azar porque no pueden hacer números al azar verdaderos. El generador de números al azar puede formar parte del transpondedor.

La unidad de proceso del transpondedor puede estar adaptada para incluir un identificador indicativo de una identidad del transpondedor en la respuesta. En otras palabras, el transpondedor puede incluir, por ejemplo, un identificador único (UID) o Identificador Único Lógico de Tarjeta (UCLID) en el mensaje de comunicación a efectos de indicar claramente al lector qué transpondedor ha contestado a la respuesta.

La unidad de proceso puede ser adaptada para seleccionar una aplicación de una serie de aplicaciones soportadas por el lector y puede incluir la aplicación seleccionada como respuesta. En una situación, en la que el lector y el transpondedor soportan ambos una serie de aplicaciones idénticas, el transpondedor puede tener la capacidad de seleccionar una de estas posibles aplicaciones para utilización subsiguiente. Esto puede ser simplemente ser indicado por el transpondedor al contestar a la respuesta con el nombre de la aplicación que se utilizará a continuación para comunicación subsiguiente. Por lo tanto, el transpondedor puede llevar a cabo una decisión de qué aplicación será presentada a lector.

La unidad de proceso puede estar adaptada para incluir una serie o la totalidad de aplicaciones soportadas por el transpondedor en la respuesta como base para una selección subsiguiente por el lector de una de las aplicaciones soportadas. En esta realización, el lector puede ser la entidad para decidir cuál de una serie de aplicaciones soportadas por ambos asociados en la comunicación puede ser utilizada a continuación. Por lo tanto, después de que el lector ha recibido la respuesta del transpondedor, incluyendo información de qué aplicación o aplicaciones están soportadas por el transpondedor, el lector puede seleccionar una específica de las aplicaciones soportadas que es preferible, por ejemplo, de acuerdo con un criterio de decisión específico. Esta aplicación seleccionada puede ser utilizada a continuación para cooperación posterior entre lector y transpondedor.

La unidad de proceso del transpondedor puede ser adaptada para generar la respuesta para comprender un Código de Autenticación de Mensaje (MAC). Este Código de Autenticación de Mensaje es un ejemplo de la forma en que se puede utilizar un esquema de codificación entre transpondedor y lector para ocultar nombres de aplicaciones soportadas por ambos. Existen varias posibilidades de formación de dicho Código de Autenticación de Mensaje que cumplen este criterio. Una posibilidad es formar el MAC basándose en una clave asociada con una aplicación en combinación con un número al azar. Una alternativa es la combinación de un nombre de una aplicación y un número al azar. Otra alternativa es una combinación de un nombre de una aplicación y un número al azar y un identificador indicativo de la identidad del transpondedor. Este MAC puede permitir al lector determinar sin ambigüedades si la aplicación está soportada por la etiqueta.

Como alternativa a la transmisión de un código de autentificación de mensaje como respuesta, las realizaciones de la invención pueden utilizar una Comprobación de Redundancia Cíclica (CRC) como respuesta o parte de la misma, y siendo codificada posteriormente. Esta CRC codificada se puede considerar como ejemplo de la forma de aplicar un esquema de codificación. Esta CRC se puede basar en un número al azar y un identificador indicativo de una identidad del transpondedor. También es posible codificar una combinación de la CRC con un identificador único y un número al azar.

La unidad de proceso puede ser adaptada para generar la respuesta, comprendiendo una suma de comprobación o cualquier otro bloque de datos libre de nombre de aplicación pero incluyendo información que permite al lector determinar si una aplicación está soportada por el transpondedor basándose en un análisis de la suma de comprobación. Por ejemplo, el lector no tiene que incluir todas las aplicaciones soportadas en un único mensaje de comunicación. En una realización alternativa, es posible que el lector envíe subsiguientemente una serie de mensajes de comunicación al transpondedor, preguntando cada uno de ellos si una aplicación específica está soportada. Como respuesta a cada uno de los mensajes de comunicación, el transpondedor puede indicar, sin nombrar específicamente la aplicación, si la aplicación incluida en una petición anterior está soportada o no. Esto puede ser indicado con un MAC que permite al lector deducir sin ambigüedades una correlación entre una aplicación

y la información respecto al soporte o falta de soporte.

A continuación, se explicarán otras realizaciones a título de ejemplo del lector. No obstante, estas realizaciones se aplican también al transpondedor, al procedimiento, al elemento de programa y al medio legible por ordenador.

El lector puede comprender una unidad de evaluación (que puede formar parte de un procesador del lector) que puede estar adaptada para evaluar qué transpondedor o transpondedores se encuentran en el momento dentro del radio de alcance del lector. En esta realización, el lector puede detectar, en primer lugar, una serie de transpondedores (tales como etiquetas RFID o tarjetas inteligentes) situadas dentro de un alcance espacial alrededor del lector en el que el alcance del lector es capaz de comunicar con los transpondedores.

Después de haber llevado a cabo esta evaluación, una unidad de selección (que puede formar parte de un procesador del lector) puede seleccionar uno de los transpondedores, que han sido detectados previamente por encontrarse dentro del alcance de radio, para comunicación posterior. Este proceso de detección puede ser llevado a cabo en el contexto de un proceso anticolisión, para asegurar que el lector comunica en cada uno de los casos solamente con uno de los transpondedores para evitar conversaciones cruzadas. Por ejemplo, otros transpondedores (distintos del transpondedor seleccionado) dentro del radio de alcance del lector pueden ser conmutados a situación muda o silenciosa por el lector.

El lector puede comprender, además, una unidad de transmisión adaptada para enviar una petición a un transpondedor, siendo las petición indicativa de una o varias aplicaciones soportadas por el lector. Esta unidad de transmisión puede ser una antena de comunicación. Con esta petición, un lector puede ordenar a un transpondedor acoplado en comunicación para indicar qué aplicaciones están soportadas por el lector. Con esta información, el sistema de comunicación puede continuar entonces la comunicación adicional de forma más significativa, por ejemplo, impidiendo comunicación con respecto a aplicaciones que no pueden ser soportadas por los dispositivos asociados de comunicación, es decir, el transpondedor y/o el lector.

En una realización alternativa, esta petición puede ser enviada también en simple texto, por ejemplo, en situaciones en las que no es relevante para la seguridad cuáles son las aplicaciones ofrecidas por un lector o en situaciones en las que no es relevante desde el punto de vista de la seguridad que un lector pregunte a un transpondedor información respecto a aplicaciones soportadas por el transpondedor.

La unidad de proceso y/o la unidad de transmisión del lector pueden estar adaptadas para enviar la petición con una longitud constante independiente de una serie de aplicaciones soportadas por el lector. De modo general, la inclusión de cada una de las aplicaciones soportadas por el lector en la petición puede requerir una longitud de datos específica, de manera que un bloque de datos que consiste en una simple lista de aplicaciones soportadas dependería del número de aplicaciones soportadas. De este modo, si solamente este bloque de datos fuera enviado al transpondedor, sería posible para un atacante deducir el número de aplicaciones soportadas por un simple análisis de longitud del mensaje de comunicación. No obstante, si la petición es enviada siempre con una longitud constante y se llenan posibles secciones vacías de datos, por ejemplo, con un número al azar, se puede ocultar el número de aplicaciones soportadas por el lector.

La unidad de proceso y/o la unidad de transmisión del lector pueden estar adaptadas para enviar una petición “vacía” a un transpondedor para pedir al transpondedor que indique aplicaciones soportadas por el mismo. En este contexto, el término “vacío” puede indicar un mensaje que no incluye indicación de cuáles son las aplicaciones soportadas por el lector y/o indicación de que una lista de aplicaciones soportadas por el transpondedor haya sido pedida por el lector. En esta realización, la petición puede estar completamente libre de cualquier indicación con respecto a aplicaciones soportadas, pero puede incluir una indicación que permite al transpondedor identificar que la información pedida por el lector es el número de aplicaciones soportadas por el transpondedor.

Una unidad determinante del lector puede ser adaptada para razonar que una aplicación no está soportada por el transpondedor cuando se determina que dicho número ampliado decodificado no contiene el nombre de dicha aplicación. En otras palabras, la ausencia de una aplicación conocida en el mensaje de comunicación transmitido desde el transpondedor al lector puede permitir al lector razonar que en la realización específica no se ofrece por el transpondedor una aplicación correspondiente.

La unidad determinante del lector puede estar adaptada para determinar la identidad del transpondedor al recuperar un identificador indicativo de la identidad del transpondedor a partir de la respuesta. De este modo, de acuerdo con un programa acordado de petición de datos, el lector puede también conseguir la información de la respuesta que el transpondedor ha contestado a la petición. Esto permite operar el sistema también en un entorno de un lector y múltiples transpondedores.

La unidad determinante del lector puede ser adaptada para determinar una aplicación soportada y seleccionada por el lector para uso subsiguiente a partir de la respuesta. Esta realización corresponde a una situación en la que el transpondedor decide con respecto a la aplicación a utilizar.

De manera alternativa, el lector puede tomar la decisión respecto la aplicación a utilizar a continuación durante una comunicación subsiguiente entre lector y transpondedor. En esta situación, la unidad determinante del lector puede estar adaptada para seleccionar una aplicación de una serie de aplicaciones soportadas por el transpondedor para utilización subsiguiente y para comunicar la aplicación seleccionada al transpondedor. Por ejemplo, un lector puede pedir una contestación sobre cuáles de diez aplicaciones están soportadas por un transpondedor. El transpondedor puede contestar con seis de estas diez aplicaciones que soporta. El lector puede seleccionar entonces una de estas seis aplicaciones soportadas de forma común para otra operación del sistema de transpondedor del lector y puede informar al transpondedor de forma correspondiente.

Para permitir que un lector funcione de acuerdo con un transpondedor, tal como se ha descrito anteriormente, y generando un CRC y/o un MAC en respuesta o como respuesta, se pueden tomar medidas correspondientes en el lector para interpretar esta CRC y/o un MAC.

También es posible que la unidad determinante del lector esté adaptada para determinar una aplicación soportada por el transpondedor al analizar un MAC u otro bloque de datos, incluido en la respuesta, encontrándose el MAC libre de nombre de una aplicación. En una situación en la que un lector pide el soporte de una aplicación determinada por mensaje de comunicación y, por lo tanto, envía una serie de peticiones una después de otra al transpondedor, cada respuesta a cada petición puede permitir, por análisis del MAC, determinar si el transpondedor, para una aplicación específica consultada, indica soporte o no.

Las realizaciones a título de ejemplo de la invención pueden permitir proporcionar atributos de privacidad con respecto a una identidad seleccionada de aplicación. La arquitectura, de acuerdo con una realización a título de ejemplo de la invención, puede aceptar lectores multi-aplicación. Esta arquitectura puede encontrarse, además, libre de utilización de autentificaciones de prueba. En vez de estas realizaciones, se puede obtener una capacidad única de un transpondedor que, en sí mismo, puede depender de una consulta por un lector (es decir, el transpondedor responde solamente con respecto a aplicaciones soportadas por el lector). De este modo, se puede garantizar un elaborado atributo de privacidad y funcionamiento rápido por realizaciones a título de ejemplo de la invención.

Estos y otros aspectos de la invención quedarán evidentes y podrán ser deducidos con referencia a las realizaciones que se describen a continuación.

Breve descripción de los dibujos

La invención se describirá en mayor detalle a continuación, mediante ejemplos no limitativos, haciendo referencia a las realizaciones mostradas en los dibujos.

La figura 1 muestra el flujo de mensajes entre un lector y una tarjeta inteligente, de acuerdo con una realización a título de ejemplo de la invención.
La figura 2 muestra un sistema de comunicación, de acuerdo con una realización a título de ejemplo de la invención.
Las figuras 3 a 5 muestran flujos de mensajes entre un lector y un transpondedor, de acuerdo con realizaciones a título de ejemplo de la invención.

Descripción de realizaciones

La ilustración en el dibujo es esquemática, en diferentes dibujos, se han representado elementos similares o idénticos con las mismas referencias.

La figura 1 muestra un flujo de un mensaje entre un lector 102 y una tarjeta inteligente 104 que forman un sistema de comunicación 100, de acuerdo con una realización a título de ejemplo de la invención.

Durante una comunicación entre el lector 102 y la tarjeta inteligente 104, se intercambian una serie de mensajes de comunicación, tal como se explicará a continuación de manera más detallada.

En una etapa 1 (ver numeral de referencia 120) del esquema de comunicación de la figura 1, el lector 102 evalúa cuáles tarjetas inteligentes se encuentran en su radio de alcance y finalmente selecciona una de ellas durante un procedimiento anticolisión, cuyo procedimiento es conocido por sí mismo. El transpondedor seleccionado es el transpondedor 104.

En una etapa 2 (ver numeral de referencia 130), el lector 102 envía una instrucción a la tarjeta inteligente 104, cuya instrucción contiene información con respecto a las aplicaciones soportadas por el lector 102. En el presente ejemplo, el lector 102 soporta las aplicaciones A, B, y C.

En una etapa 3, la tarjeta inteligente 104 evalúa cuáles de las aplicaciones soportadas por el lector 102 están soportadas también por la tarjeta 104. A continuación, la tarjeta 104 envía el nombre de una aplicación soportada ampliada en un número al azar y una suma de comprobación en retorno al lector (ver numeral de referencia 1401), en el que el número ampliado está codificado y/o se ha generado un MAC, con una clave asociada con las

aplicaciones anteriormente. En el presente ejemplo, la tarjeta 104 soporta la aplicación A, B, D, X, y Z. La aplicación C no está soportada por la tarjeta inteligente 104. Por lo tanto, el nombre de la aplicación A es ampliado por un número al azar y una suma de comprobación, y, a continuación, es codificado y/o se genera un MAC con una clave asociada con la aplicación A. De la misma manera, es procesado el nombre de la aplicación B. Dado que la aplicación C no está soportada, solamente se genera un número al azar y se transmite al lector 102. Se debe observar que el número al azar tiene la misma longitud que los números resultantes para las aplicaciones A y B.

En una etapa 4, el lector 102 decodifica los datos recibidos y/o comprueba el MAC con las claves para las aplicaciones A, B y C que se utilizaron también por la tarjeta inteligente 102 (de modo estricto, la tarjeta 104 utilizó claves para A y B solamente). Después de la decodificación, los nombres de aplicación para A y B aparecen en simple texto, o bien el MAC en el que se utilizaron los nombres de aplicación A y B concuerda con el MAC recibido. Por lo tanto, el lector 102 sabe que la tarjeta inteligente 104 soporta las aplicaciones A y B y no soporta la aplicación C (en cuanto a C, aparece un número al azar después de la decodificación). A continuación, el lector 102 escoge una de las aplicaciones e indica a la tarjeta inteligente 104 cuál de las aplicaciones será utilizada para continuar el proceso.

En el presente ejemplo, el nombre de la aplicación A es ampliado por un número al azar y suma de comprobación. Entonces, el número resultante es codificado con una clave asociada con la aplicación A, y transmitido a la tarjeta inteligente 104 (ver numeral de referencia 150). En la tarjeta inteligente 104, los datos recibidos son decodificados nuevamente, de manera que el nombre de la aplicación A aparece en texto simple. Tanto el lector 102 como la tarjeta inteligente 104 saben ahora cuál es la aplicación que se utilizará. De manera alternativa, la tarjeta inteligente 104 calcula un MAC y verifica que es idéntico al MAC recibido.

El proceso descrito puede comportar las siguientes ventajas:

El nombre de la aplicación que soporta el transpondedor no es transmitido nunca en texto simple, de manera que se pueda impedir que un atacante tenga información no autorizada respecto a las aplicaciones previstas en el sistema de comunicación.

El nombre codificado no es nunca el mismo dado que contiene una parte al azar, de manera que se hace incluso más difícil un ataque.

La longitud de la respuesta de la tarjeta es siempre la misma, con independencia del número de aplicaciones soportadas por los asociados de comunicación. Esto oculta también el número de aplicaciones soportadas.

De acuerdo con ello, un atacante no puede determinar qué ni cuántas aplicaciones son soportadas por la tarjeta inteligente.

En una realización alternativa, en la etapa 2 de la figura 1, los nombres de aplicación son transmitidos en texto simple porque la tarjeta primaria que se tiene que asegurar es la tarjeta inteligente 104. No obstante, también la comunicación desde el lector 102 a la tarjeta inteligente 104 puede ser codificada. En una realización adicional, no hay información con respecto a las aplicaciones soportadas por el lector 102 en absoluto, de manera que solamente se envía una instrucción vacía a la tarjeta 104 en la etapa 2.

No obstante, dada la longitud de la respuesta, el número de aplicaciones soportadas puede ser determinado por un atacante. Por lo tanto, en otra realización, la instrucción de la etapa 2 tiene una longitud implícita predefinida, por ejemplo, 10 aplicaciones. Los bloques de datos que no son utilizados para aplicaciones son llenados entonces con números al azar. Un atacante no puede determinar entonces qué ni cuántas aplicaciones están soportadas. El atacante no puede determinar qué o cuántas aplicaciones están soportadas por la tarjeta inteligente 104.

La privacidad juega un papel importante para individuos y también para un grupo de personas que comparten una cierta propiedad. No obstante, la privacidad puede perderse de varias maneras. Con sistemas de comunicación con tarjetas convencionales, la detección de colisión puede ser legible de modo directo. De este modo, un usuario individual puede ser escaneado en varios sitios. Incluso cuando se utilizan identificadores al azar, las aplicaciones auténticas en los lectores necesitan conocer con qué tarjeta sea comunican, de manera que existe todavía la necesidad de un ID Único Lógico de Tarjeta (UCLID). Cuando una tarjeta presenta la aplicación que soporta, esto puede ser no dañino. Un atacante puede ser capaz de seguir a individuos basándose en información de canales secundarios que se puede deducir de aplicaciones soportadas.

Asimismo, cuando una tarjeta presenta su tipo, marca, etc. ello no es siempre inocuo. Por ejemplo, el conocimiento de que la tarjeta de tipo X del fabricante Y es utilizado por el metro de Nueva York y que no ha sido adquirida por muchas ciudades, da a conocer que el portador de dicha tarjeta es, con elevadas probabilidades, habitante de Nueva York.

En vista de estas configuraciones, la privacidad es un objetivo final. Puede ser deseable que un sistema de comunicación no revele información con respecto al propietario de la tarjeta, aplicaciones de la tarjeta,

identificadores de la tarjeta, fabricantes de la tarjeta, tipo de la tarjeta, etc. a cualquier identidad que no sea un lector auténtico para una aplicación soportada por aquella tarjeta específica. Por lo tanto, la privacidad no se debe perder por el protocolo, datos, comportamiento ni por propiedades de comportamiento análogas de la tarjeta.

La medida en la que un sistema de comunicación implementa dicho objetivo final, depende en costes a afrontar, tiempo, compatibilidad con la base instalada, etc. La violación de una clave utilizada para una aplicación, no viola la privacidad de otras aplicaciones.

No obstante, puede haber un riesgo residual para la privacidad en una situación final de privacidad. Si una clave de aplicación se viola, la privacidad de todos los usuarios de dicha aplicación queda comprometida. El UCLID puede ser leído y entonces el usuario puede ser localizado de este modo.

A continuación, haciendo referencia a la figura 2, se explicará un sistema de comunicación 100, de acuerdo con una realización a título de ejemplo de la invención que puede ser capaz de mantener la privacidad.

El sistema de comunicación 100 puede ser similar al mostrado en la figura 1 y comprende el lector 102 y el transpondedor 104, que están acoplados entre sí para comunicación inalámbrica.

El lector 102 comprende un procesador 112 (tal como un microprocesador o una unidad central de proceso) que está acoplado con una antena emisora 114 y una antena receptora 116. La antena emisora 114 es capaz de transmitir un mensaje de comunicación 118 al transpondedor 104. La antena receptora 116 es capaz de recibir un mensaje de comunicación 122 del transpondedor 104. Aunque la antena de transmisión 114 y la antena receptora 116 se han mostrado como dos antenas distintas en la figura 2, realizaciones alternativas pueden utilizar también una única antena común compartida de transceptor. Los mensajes de comunicación 118, 122 pueden ser intercambiados de forma inalámbrica entre las entidades 102, 104.

Las antenas 114, 116 están acopladas eléctricamente con el procesador 112, de manera que los datos que pueden ser transmitidos desde el procesador 112 a la antena de transmisión 114 para transmisión como mensajes de comunicación 118, 122 recibidos por la antena receptora 116 pueden ser también analizados y procesados por el procesador 112.

Una unidad de almacenamiento 124, tal como una memoria de semiconductor está acoplada con el procesador 112 para transferencia bidireccional de datos a efectos de almacenar datos accesibles por el procesador 112. Además, una unidad de entrada/salida 126 permite al usuario utilizar y controlar el dispositivo lector 102.

Tal como se puede observar además de la figura 2, el transpondedor 104 comprende una antena de transmisión y recepción 110, un procesador 108 tal como un microprocesador, y una memoria 106. En una realización, la memoria 106 y el procesador 108 pueden estar monolíticamente integrados en el circuito integrado (IC) que puede estar conectado a la antena 110 y acoplado a un soporte 128, tal como un trozo de tela.

Durante el funcionamiento, el procesador 112 del lector 102 puede servir como unidad de evaluación par avaluar qué transpondedores 104 se encuentran dentro del radio de acción del lector 102. En la presente situación, solamente el transpondedor 104 se encuentra en el radio de acción del lector 102, es decir, suficientemente cerca para permitir una comunicación suficientemente precisa. Durante un proceso anticolisión, en el caso de que múltiples transpondedores se encuentren dentro del radio de acción del lector 102, el procesador 112 puede servir como unidad de selección para seleccionar uno de los transpondedores. En la presente situación, el transpondedor 104 se encuentra dentro del radio de alcance para subsiguiente comunicación.

El lector 102 puede enviar además, mediante la antena de emisión 114, una petición tal como un mensaje de comunicación 118 al transpondedor 104 indicativo de las aplicaciones soportadas por el lector 102. Esta petición puede ser enviada de manera codificada o en simple texto. En otra realización, la petición 118 puede encontrarse libre de cualquier indicación de aplicaciones soportadas por el lector 102.

No obstante, en una realización preferente, la antena de transmisión 114 envía la petición 118 con una longitud constante independiente del número de aplicaciones soportadas por el lector 102, pero indicando, no obstante, las aplicaciones soportadas de manera codificada. Esto impide que un atacante pueda identificar la información proporcionada por el lector 102 al analizar la longitud del mensaje de comunicación 118. Las partes vacías de un paquete de datos correspondiente pueden ser llenadas con números al azar para ocultar el número de aplicaciones soportadas a un atacante.

El transpondedor 104 puede almacenar en su unidad de almacenamiento 106 datos necesarios para soportar una serie de diferentes aplicaciones que están soportadas por el transpondedor 104. Al recibir la petición 118 del lector 102, el procesador 108 puede generar un mensaje de comunicación 122 para informar al lector 102 con respecto a las aplicaciones soportadas por el transpondedor 104. Con este objetivo, es posible que un nombre de una aplicación indicada en la figura 2 de forma esquemática con el numeral de referencia 202, se pueda ampliar mediante un número al azar 204 y una suma de comprobación 206. El número al azar puede ser generado por el

procesador 108. La suma de comprobación 206, así como el nombre de la aplicación 202 se pueden almacenar en la memoria 106. Además, el paquete de datos 202, 206, 204 puede ser codificado utilizando una clave 208 que se puede almacenar también en la memoria 106. Esta clave 208 puede ser asociada o asignada a la aplicación indicada con el nombre 202. Un mensaje de datos codificado de manera correspondiente 210 puede ser enviado, entonces, por la antena de transmisión 110 al dispositivo lector 102, tal como se ha indicado con el mensaje de comunicación 122 de la figura 2.

Si una aplicación no está soportada por el transpondedor 104, el transpondedor 104 puede enviar simplemente un mensaje de comunicación al lector 102 que consiste en un número al azar. Este puede tener la misma longitud que el mensaje de comunicación 210 a efectos de dificultar que un atacante pueda deducir información con respecto al número de aplicaciones soportado por el transpondedor 104.

Al recibir el mensaje de comunicación 122 por la antena receptora 116, el procesador 112 funcionará como unidad de decodificación para decodificar datos recibidos utilizando la clave 208 asociada a la aplicación soportada por el transpondedor 104. Al tomar esta medida, el número decodificado, es decir, el paquete de datos 202, 206, 204 puede ser deducido por el procesador 112. A partir de este paquete de datos 202, 206, 204 es posible que el procesador 112 identifique el nombre 202 de una aplicación que permite al dispositivo lector 102 determinar que el transpondedor 104 soporta la correspondiente aplicación. Para la comunicación adicional entre el dispositivo lector 102 y el transpondedor 104, ambas entidades saben que la aplicación indicada por el nombre de una aplicación 202 puede ser facilitada por ambas entidades. Al mismo tiempo, se mantiene la privacidad.

Los técnicos en la materia deben observar que el transpondedor de la invención, el lector de la invención y el procedimiento de la invención, así como el software de la invención, no están limitados a la transmisión de datos inalámbrica, sino que en principio se aplican también a la comunicación por cable.

A continuación, haciendo referencia a la figura 3, se explicará un esquema de comunicación 300 entre un lector 102 y un transpondedor 104, de acuerdo con una realización a título de ejemplo de la invención.

En la realización descrita, se envía un mensaje de comunicación 302 desde el lector 102 al transpondedor 104, incluyendo una serie de nombres de aplicación 202 (A, B, C) a los que el lector 102 desea conocer, si estas aplicaciones están soportadas por el transpondedor 104.

Como respuesta a esta petición 302, el transpondedor 104 genera un mensaje de comunicación 304 que incluye, entre otros, un MAC calculado 306 que está formado en base al nombre de una aplicación 202 (es decir, la aplicación soportada A) combinado con un número al azar 204 para ocultar el nombre de la aplicación soportada A. En este contexto, se debe observar que el campo 310 proporciona integridad del criptograma.

Tanto el mensaje de comunicación 302 como la respuesta 304 pueden incluir otro número al azar 308 indicado como RndQ, que es opcional y puede servir para determinar el carácter reciente (“freshness”).

El mensaje de comunicación 304 no solamente incluye los bloques 204, 202, 308 relativos a la aplicación A, sino que puede comprender también bloques correspondientes indicativos de soporte para las aplicaciones B y C, en caso de que sea aplicable. Tal como se ha indicado por los numerales de referencia 204’ y 204’, también para las aplicaciones B y C se puede calcular un número al azar correspondiente. Tal como se ha indicado por los numerales de referencia 310’ y 310’’, también para las aplicaciones B y C se puede calcular un bloque de integridad. Los bloques de integridad 310’ y 310’’ son calculados de la misma manera que el bloque de datos 310 para una aplicación A: MAC con respecto a situación, RndF ó RndH, nombre de aplicación y RndQ, y utilizando una clave KB ó KC en vez de una clave KA.

Después de transmisión de la respuesta 304, desde el transpondedor 104 al lector 102, el análisis del mensaje 304 en el lado del lector 102 permite al lector 102 extraer la información de qué aplicación o aplicaciones están soportadas por el transpondedor 104.

Dado que en la presente realización tres aplicaciones A, B, C están soportadas por el transpondedor 104, el lector 102 puede llevar a cabo un proceso de selección indicado con el numeral de referencia 320. Con este objetivo, el lector 102 calcula un MAC 322 utilizando la clave KA, KB ó KC dependiendo de si la aplicación A, aplicación B ó aplicación C ha sido la escogida. El MAC 322 comprende el número al azar 308, un bloque 324 indicativo de la aplicación A, aplicación B o aplicación C, así como un número al azar correspondiente RndD 204, RndF 204’ ó RndH 204’’.

Después de recibir el mensaje de comunicación 320, el transpondedor puede enviar en retorno un mensaje 330.

En el caso que el transpondedor 104 lleve a cabo una selección con respecto a la aplicación soportada A, B, C a utilizar para una operación siguiente, es posible que el transpondedor 104 facilite solamente una respuesta en retorno para la aplicación A, B ó C. Entonces, la instrucción de selección 320 no es necesaria, puesto que el transpondedor 104 ya ha realizado la selección.

La realización de la figura 3 no incluye un identificador (CLUID) del transpondedor 104 en el MAC 306.

En la realización de la figura 4, que muestra la secuencia de comunicación 400, se genera un MAC 412 que incluye dicho identificador único.

En la realización de la figura 4, después de haber recibido la petición 302, el transpondedor 104 genera una contestación 410. Esta contestación 410 incluye un MAC calculado 412 que está formado por un bloque de carga útil 414 y un bloque 416 indicativo de un nombre de una aplicación. El bloque de carga útil 414 es calculado como función de una clave KA relativa a las aplicaciones A, pudiendo incluir también otros datos. Asimismo, el número al azar RndD puede ser utilizado para esta finalidad. El bloque de carga útil 414 incluye un sub-bloque 418 indicativo de la identidad del transpondedor 104 e incluye un bloque de número al azar 420. Otros bloques correspondientes pueden ser generados asimismo para las aplicaciones B y C, en caso de que sea aplicable, tal como se ha indicado en la figura 4.

Las condiciones de la figura 4 de formación de la contestación 410 se refieren a una situación en la que las aplicaciones A, B y C están soportadas en realidad por el transpondedor 104. En condiciones alternativas en las que una aplicación no está soportada, el transpondedor 104, en vez del mensaje de comunicación 410, puede enviar simplemente un número al azar al lector 102. Esto oculta la “presencia” o “ausencia” de cualquier soporte.

El bloque de carga útil 430 se refiere a la aplicación A, mientras que un bloque de carga útil 430’ se refiere a la aplicación B y un bloque de carga útil 430’’ se refiere a una aplicación C. De manera similar, los bloques de integridad 310’ y 310’’ están formados para las aplicaciones B y C correspondientes al bloque 310. Los bloques de carga útil 430’, 430’’ son calculados de la misma manera que el bloque de carga útil 430 para la aplicación A por codificación del identificador único CLUID y el número al azar RndX, pero utilizando la clave KB ó KC en vez de K_A.

También en este caso se puede generar un mensaje de selección 440 para el lector 102 en situaciones en las que el lector 102 selecciona una de las aplicaciones soportadas A, B, C para utilización subsiguiente. Para este objetivo se puede calcular un MAC 442 para el dispositivo lector 102 que incluye un número al azar 444, un bloque indicativo de una identidad del transpondedor 446 comprendiendo también los campos 324 y 308.

El ejemplo de la figura 4 se refiere a una situación en la que el lector 102 soporta las aplicaciones A, B y C. Con respecto al MAC 442, el número al azar RndY puede ser enviado si el lector 102 no se refiere a ninguna de las aplicaciones A, B ó C. Una clave utilizada para calcular el MAC 442 es KA, KB ó KC, dependiendo de cuál de las aplicaciones A, B, C es la escogida.

Tal como la figura 3, se puede utilizar o no el RndQ 308. O bien una respuesta es utilizada para cada una de las aplicaciones o el transpondedor 104 facilita solamente una respuesta en retorno para A, B ó C. La instrucción de selección 440 no es necesaria.

En la realización de la figura 5, los mensajes de comunicación 302 y 330 son como en las figuras 3 y 4.

No obstante, para el cálculo del mensaje de comunicación 510, se puede calcular un bloque de carga útil 512 como codificación (E) de una clave (K_A) indicativa de la aplicación A y de otros datos. También se puede utilizar un número al azar RndD para calcular ese bloque 512. Tal como se puede deducir de la figura 5, igualmente el bloque 512 comprende una identidad de un transpondedor 418, un número al azar RndX 420, un nombre de una aplicación A 202, un número al azar opcional RndQ 308 y una Comprobación de Redundancia Cíclica (CRC) 514. La CRC 514 asegura la integridad del criptograma. Se pueden calcular bloques correspondientes para las aplicaciones B y C de manera correspondiente, ver los numerales de referencia 512’ y 512’’. Por ejemplo, el campo 512’ se calcula de forma correspondiente a la aplicación A: codificar CLUID, RndX, RndQ y CRC pero utilizando la KB en vez de la KA.

Para un mensaje de selección 350, se puede calcular un MAC 552. Se puede enviar RndY si el lector 102 no selecciona ninguna de las aplicaciones A, B ó C. Para calcular el MAC 552, la clave utilizada es KA, KB ó KC, dependiendo de cuál de las aplicaciones A, B ó C se ha escogido.

De acuerdo con una realización a título de ejemplo de la invención, la funcionalidad completa del lector y del transpondedor se puede invertir de manera que el flujo de protocolo tiene lugar en la otra dirección. Esto es una solución equivalente a los sistemas que se han dado a conocer de manera explícita y se cubre también con el alcance de las reivindicaciones. Por ejemplo, los nombres de la aplicación de lectura pueden ser protestados invirtiendo el lado lector y el transpondedor.

Finalmente, se debe observar que las realizaciones anteriormente mencionadas muestran la invención en vez de limitarla, y los técnicos en la materia podrán diseñar muchas realizaciones alternativas sin salir del alcance de la invención, tal como se refiere en las reivindicaciones adjuntas. En las reivindicaciones, cualesquiera signos de referencia dispuestos dentro del paréntesis no se considerarán como limitadores de las reivindicaciones. Las palabras “comprendiendo” y “comprende” y similares, no excluyen la presencia de otros elementos o etapas de los relacionados en cualquier reivindicación o en la descripción como conjunto. La referencia singular de un elemento no

excluye la referencia plural de dichos elementos y viceversa. En una reivindicación de dispositivo que enumera varios dispositivos, varios de estos dispositivos pueden estar materializados por uno de igual elemento de software o hardware. El mero hecho de que algunas medidas sean expresadas en reivindicaciones distintas dependientes entre sí no indica que no se pueda utilizar de manera ventajosa una combinación de estas medidas.

El alcance de la invención queda definido por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Transpondedor (104) que comprende
una unidad de almacenamiento (106) que tiene almacenada una serie de aplicaciones diferentes; y
una unidad de proceso (108) que está adaptada para generar,
a petición de un lector (102) una respuesta; y
una unidad de transmisión (110) adaptada para enviar la respuesta a dicho lector (102),
caracterizándose el transpondedor (104) por el hecho de que la respuesta es interpretable utilizando un esquema de codificación conocido tanto por el transpondedor (104) como por el lector (102); y porque la unidad de proceso (108) está adaptada para ampliar un nombre de una aplicación por un número al azar y para codificar el número ampliado con una clave asociada con dicha aplicación para generar la respuesta.

2. Transpondedor (104), según la reivindicación 1, en el que la unidad de proceso (108) está adaptada para evaluar, al recibo de la petición indicativa de un lector (102) de aplicaciones soportadas por el lector (102), cuáles de las aplicaciones soportadas por el lector (102) están también soportadas por el transpondedor (104) y para llevar a cabo la ampliación y codificación para las aplicaciones soportadas por el lector (102) y soportadas por el transpondedor (104).

3. Transpondedor (104), según la reivindicación 1, en el que la unidad de proceso (108) está adaptada para ampliar el nombre de la aplicación por el número al azar y una suma de comprobación antes de la codificación.

4. Transpondedor (104), según la reivindicación 1,
en el que la unidad de proceso (108) está adaptada para una aplicación que no está soportada por el transpondedor (104), generar un número al azar;
en el que la unidad de transmisión (110) está adaptada para enviar el número al azar generado a dicho lector (102).

5. Transpondedor (104), según la reivindicación 1, en el que la unidad de proceso (108) está adaptada para la aplicación que no está soportada por el transpondedor (104), para generar el número al azar con una longitud que es la misma que la longitud del número codificado para una aplicación que está soportada por el transpondedor (104).

6. Transpondedor (104), según la reivindicación 1, en el que la unidad de proceso (108) está adaptada para incluir un identificador (418) indicativo de la identidad del transpondedor (104) en la respuesta.

7. Transpondedor (104), según la reivindicación 1, en el que la unidad de proceso (108) está adaptada para seleccionar una de una serie de aplicaciones soportadas por el lector (102) y para incluir la aplicación seleccionada en la respuesta.

8. Transpondedor (104), según la reivindicación 1, en el que la unidad de proceso (108) está adaptada para incluir una serie o la totalidad de aplicaciones soportadas por el transpondedor (102) en la respuesta como base para una selección subsiguiente por el lector (102) de una de las aplicaciones soportadas.

9. Transpondedor (104), según la reivindicación 1, en el que la unidad de proceso (108) está adaptada para generar la respuesta para comprender un Código de Autentificación de Mensaje (306, 412).

10. Transpondedor (104), según la reivindicación 9, en el que la unidad de proceso (108) está adaptada para generar la respuesta que comprende el Código de Autentificación de Mensaje (306, 412) basado en una combinación del grupo que consiste en una clave asociada con una aplicación y un número al azar, un nombre de una aplicación y número al azar y un nombre de una aplicación y un número al azar y un identificador indicativo de la identidad del transpondedor (104).

11. Transpondedor (104), según la reivindicación 1, en el que la unidad de proceso (108) está adaptada para generar la respuesta para comprender una Comprobación de Redundancia Cíclica (514).

12. Transpondedor (104), según la reivindicación 11, en el que la unidad de proceso (108) está adaptada para generar la respuesta que comprende la Comprobación de Redundancia Cíclica (514) basada en un número al azar y un identificador indicativo de la identidad del transpondedor (104).

13. Transpondedor (104), según la reivindicación 1, en el que la unidad de proceso (108) está adaptada para generar la respuesta para comprender una suma de comprobación codificada pero siendo libre de un nombre una aplicación, de manera que el lector (102) está capacitado para determinar si una aplicación está soportada por el transpondedor (104) basándose en la suma de comprobación.

14. Lector (102) que comprende
una unidad de transmisión (114) adaptada para enviar una petición a un transpondedor (104), siendo indicativa la petición de una serie de aplicaciones soportadas por el lector (102); y

una unidad de análisis (112) adaptada para analizar una respuesta recibida desde el transpondedor (104) con un esquema de codificación conocido tanto por el transpondedor (104) como por el lector (102); y
una unidad de determinación (112) adaptada para determinar si una aplicación está soportada por el transpondedor (104) basándose en dicho análisis de la respuesta utilizando el esquema de codificación,
en el que la unidad de análisis (112) es una unidad de decodificación (112) adaptada para decodificar la respuesta recibida desde el transpondedor (104) con una clave asociada con una aplicación para deducir de esta manera un número ampliado decodificado; y
en el que la unidad de determinación (112) está adaptada para determinar si dicho número ampliado decodificado contiene un nombre de dicha aplicación.

15. Lector (102), según la reivindicación 14, en el que la unidad de transmisión (114) está adaptada para enviar la petición de forma codificada o está adaptada para enviar la petición en simple texto.

16. Lector (102), según la reivindicación 14, en el que la unidad de transmisión (114) está adaptada para enviar la petición con una longitud constante que es independiente del número de aplicaciones soportadas por el lector (102).

17 Lector (102), según la reivindicación 14, en el que la unidad de determinación (112) está adaptada para razonar que una aplicación no está soportada por el transpondedor (104) cuando determina que dicho número decodificado no contiene un nombre de dicha aplicación.

18. Lector (102), según la reivindicación 14, en el que la unidad de determinación (112) está adaptada para determinar la identidad del transpondedor (104) recuperando un identificador (418) indicativo de la identidad del transpondedor (104) a partir de la respuesta.

19. Lector (102), según la reivindicación 14, en el que la unidad de determinación (112) está adaptada para determinar, a partir de la respuesta, una aplicación soportada y seleccionada por el lector (112) para utilización subsiguiente.

20. Lector (102), según la reivindicación 14, en el que la unidad de determinación (112) está adaptada para seleccionar una de una serie de aplicaciones soportadas por el transpondedor (102) y para utilización subsiguiente y para comunicar la aplicación seleccionada al transpondedor (102).

21. Lector (102), según la reivindicación 14, en el que la unidad de determinación (112) está adaptada para determinar una aplicación soportada por el transpondedor (104) por un Código de Autentificación de Mensaje incluido en la respuesta.

22. Lector (102), según la reivindicación 14, en el que la unidad de determinación (112) está adaptada para determinar una aplicación soportada por el transpondedor (104) por análisis de la Comprobación de Redundancia Cíclica incluida en la respuesta.

23. Lector (102), según la reivindicación 14, en el que la unidad de determinación (112) está adaptada para determinar una aplicación soportada por el transpondedor (104) al analizar una suma de comprobación incluida en la respuesta, incluyendo la suma de comprobación información que permite al lector determinar si una aplicación está soportada por el transpondedor basándose en un análisis de la suma de comprobación.

24. Procedimiento para la ocultación de aplicaciones soportadas por un lector (102) y un transpondedor (104), cuyo procedimiento comprende que:
el lector (102) envíe una instrucción de petición a dicho transpondedor (104),
el transpondedor (104) genere una respuesta interpretable utilizando un esquema de codificación conocido tanto por el transpondedor (104) como por el lector (102) y siendo indicativa de si una aplicación está soportada por el transpondedor (104), enviando el transpondedor (104) la respuesta a dicho lector (102),
determinando el lector (102) si una aplicación está soportada por el transpondedor (104) al analizar la respuesta utilizando el esquema de codificación,
ampliando el transpondedor (104) el nombre de una aplicación que soporta el transpondedor (104) por un número al azar; y
codificando el transpondedor (104) el número ampliado con una clave asociada con dicha aplicación para generar la respuesta.

25. Soporte legible por ordenador, en el que está almacenado un programa de ordenador para la ocultación de aplicaciones soportadas por un lector (102) y transpondedor (104), cuyo programa de ordenador, cuando es ejecutado por un procesador (112, 108) está adaptado para llevar a cabo o para controlar un procedimiento según la reivindicación 24.

26. Elemento de programa para la ocultación de aplicaciones soportadas por el lector (102) y el transpondedor (104), cuyo elemento de programa, cuando es ejecutado por un procesador (112, 108) está adaptado para llevar a cabo o para controlar un procedimiento según la reivindicación (104).

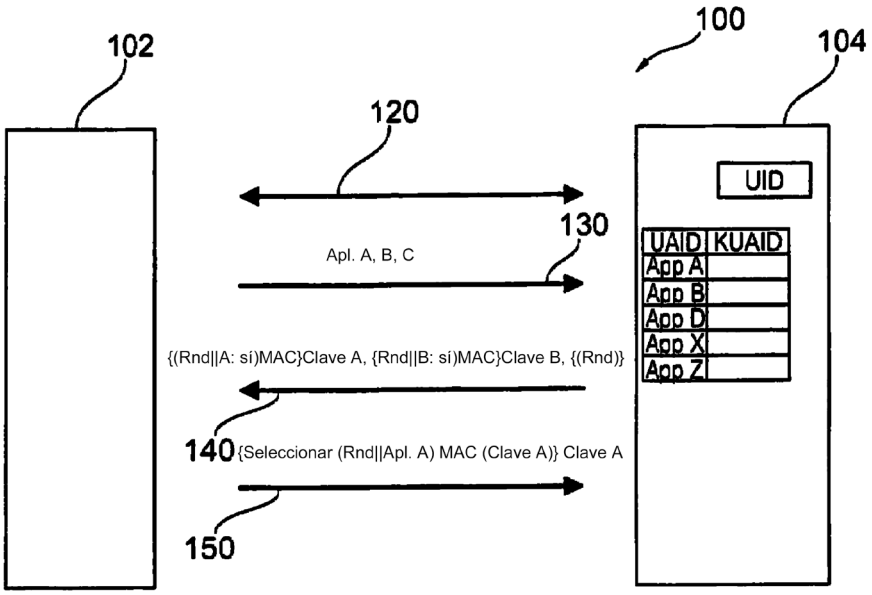
102
100
104
120
UID
130
Apl. A, B, C
UAID KUAID
App A
App B
App D
App X
App Z
{(Rnd||A: sí)MAC}Clave A, {Rnd||B: sí)MAC}Clave B, {(Rnd)}
140
{Seleccionar (Rnd||Apl. A) MAC (Clave A)} Clave A
150

Fig. 1

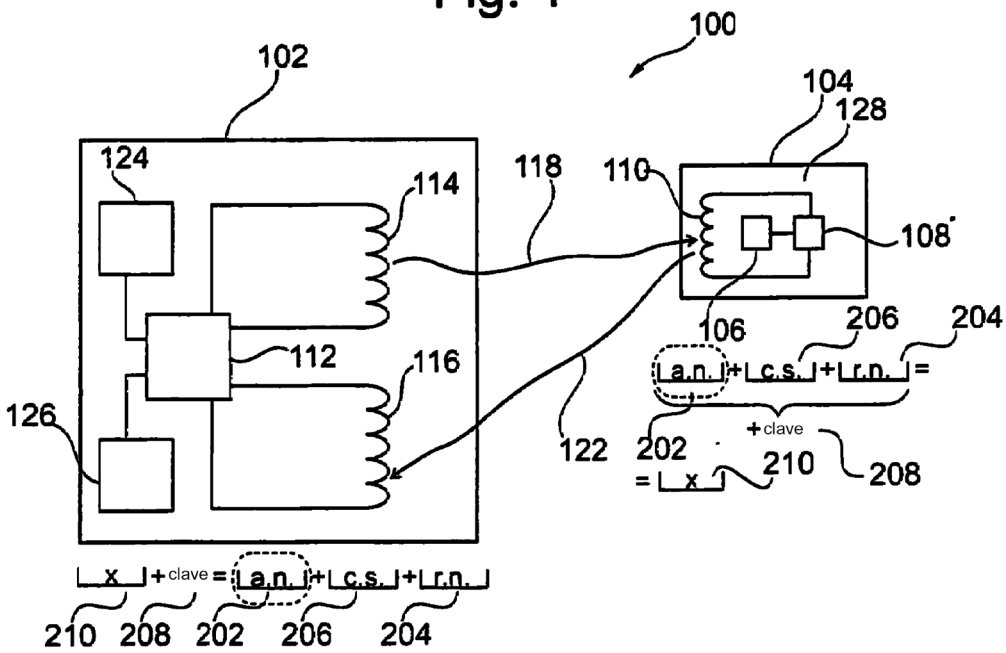
100
102
104
128
124
114
118
110
108
112
116
106
206
204
126
i.a.n. i + c.s. + r.n. =
+ clave
122
202
210
208
= x
x + clave = i.a.n. i + c.s. + r.n.
210
208
202
206
204

Fig. 2

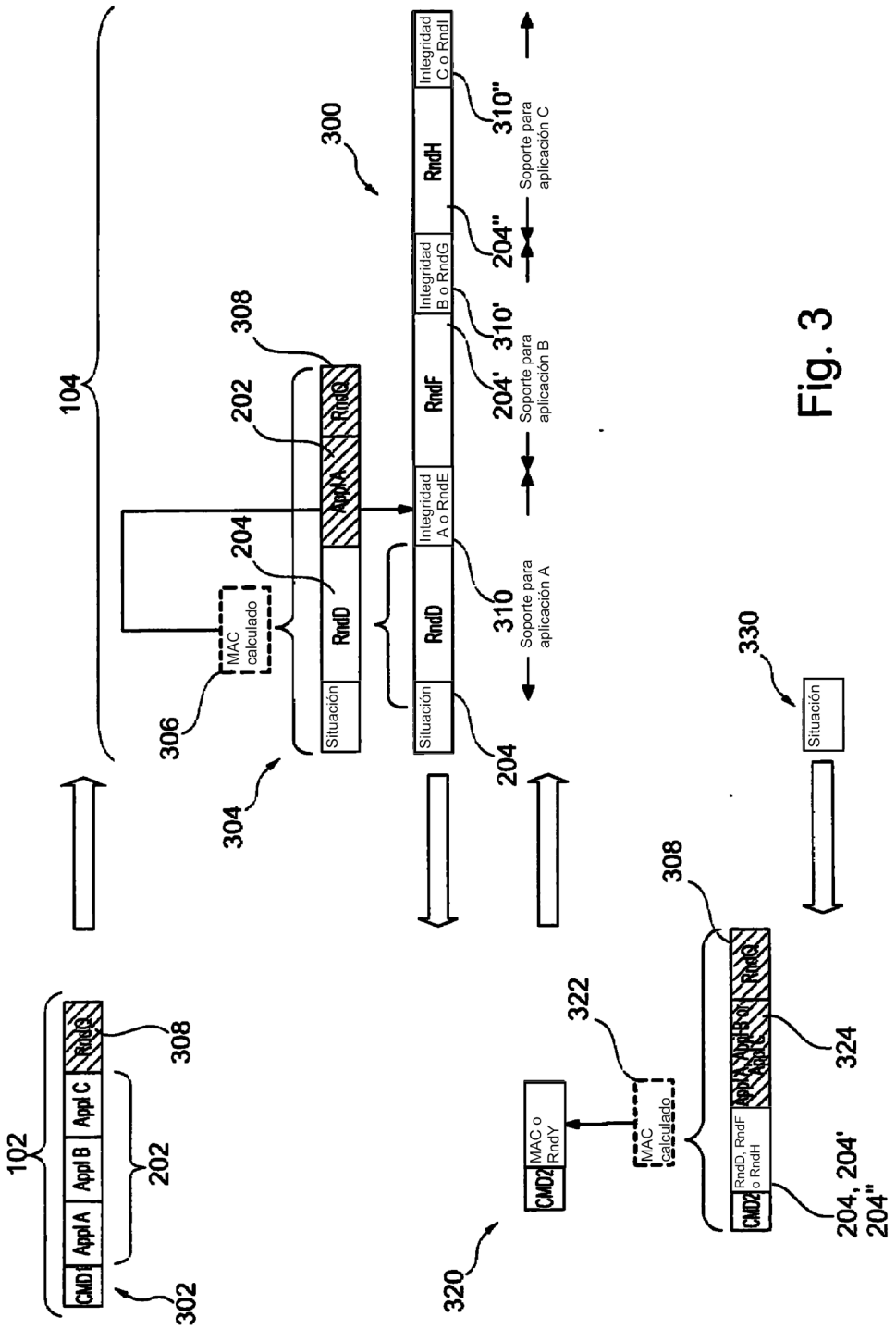
102
CMD1
Appl A
Appl B
Appl C
RndG
202
308
302
104
306
MAC calculado
204
RndD
Situación
304
202
308
300
Integridad A o RndE
RndF
Integridad B o RndG
RndH
Integridad C o RndI
310
310'
310"
204
204'
204"
Soporte para aplicación A
Soporte para aplicación B
Soporte para aplicación C
330
Situación
308
322
MAC o RndY
CMD2
MAC calculado
RndD, RndF o RndH
CMD2
RndG
324
320
204, 204', 204"

Fig. 3

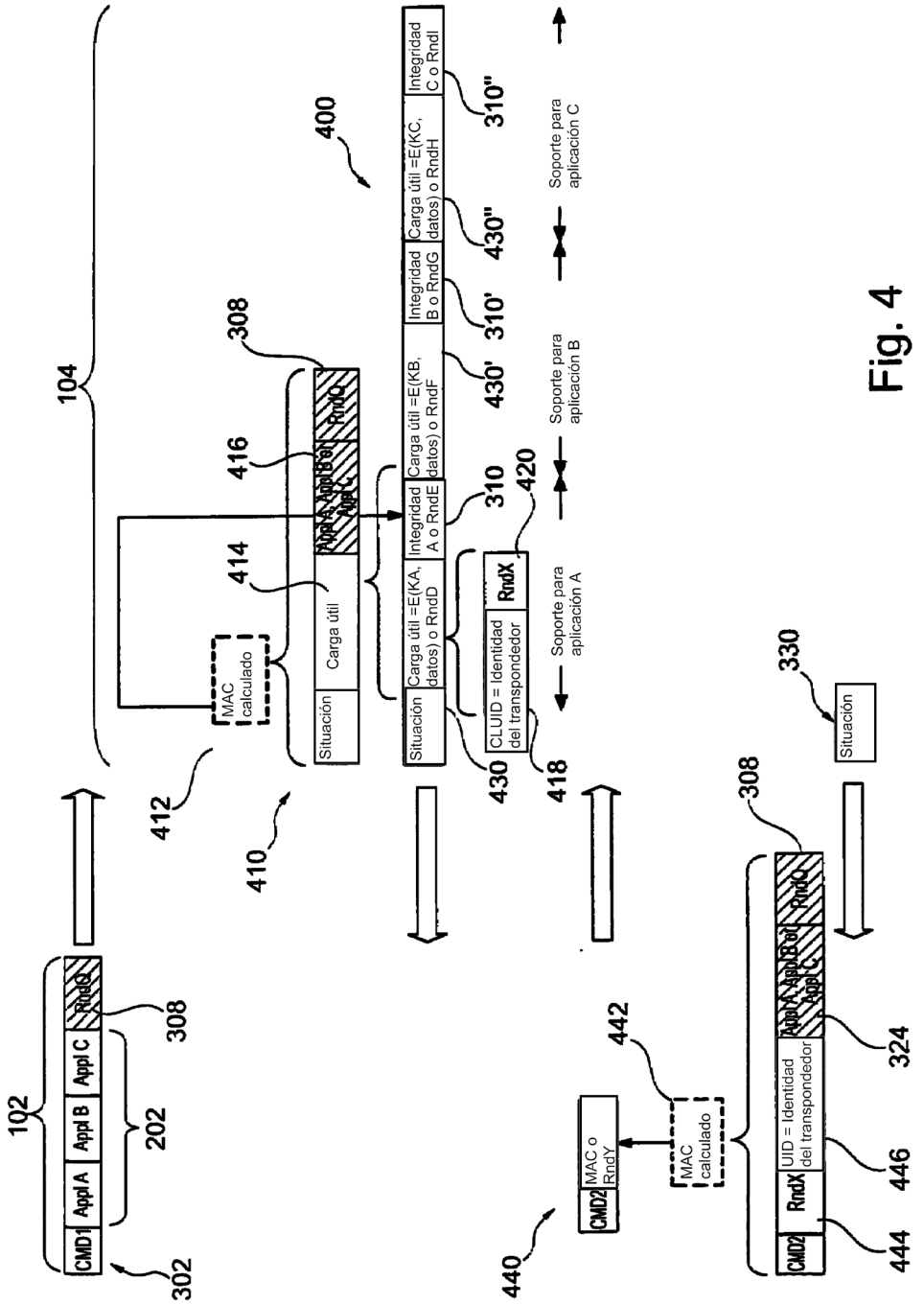
102
CMD1
Appl A
Appl B
Appl C
RndG
202
308
302
104
412
MAC calculado
410
Situación
Carga útil
414
416
308
400
Situación
Carga útil =E(KA, datos) o RndD
Integridad A o RndE
Carga útil =E(KB, datos) o RndF
Integridad B o RndG
Carga útil =E(KC, datos) o RndH
Integridad C o RndI
310
310'
310"
430
430'
430"
CLUID = Identidad del transpondedor
RndX
420
418
Soporte para aplicación A
Soporte para aplicación B
Soporte para aplicación C
330
Situación
308
440
CMD2
MAC o RndY
442
MAC calculado
CMD2
RndX
UID = Identidad del transpondedor
Appl A
Appl B
Appl C
RndG
324
444
446

Fig. 4

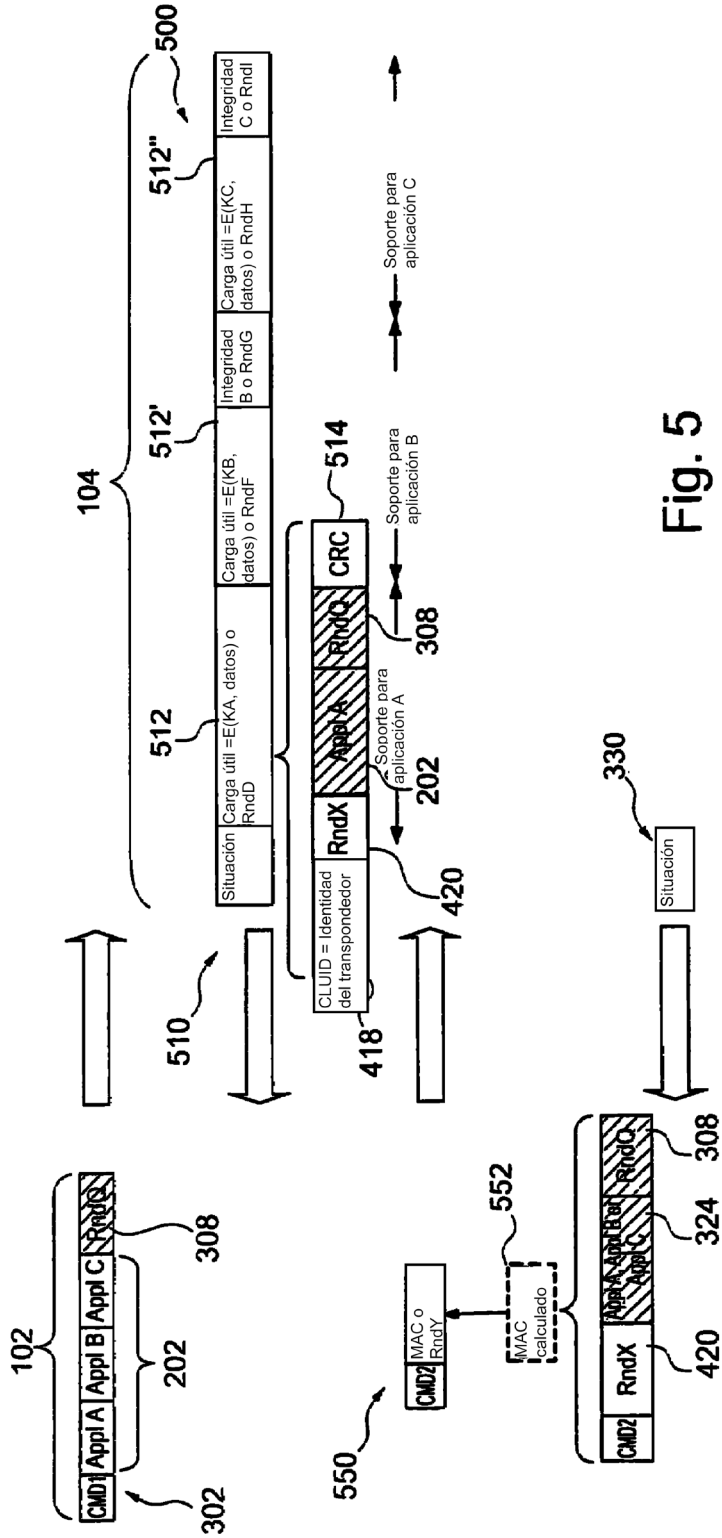
102
CMD1
Appl A
Appl B
Appl C
RndQ
308
202
302
104
500
512
512'
512"
Situación
Carga útil =E(KA, datos) o RndD
Carga útil =E(KB, datos) o RndF
Carga útil =E(KC, datos) o RndH
Integridad B o RndG
Integridad C o RndI
510
CLUID = Identidad del transpondedor
RndX
Appl A
RndQ
CRC
514
418
420
Soporte para aplicación A
Soporte para aplicación B
Soporte para aplicación C
202
308
330
Situación
550
CMD2
MAC o RndY
552
MAC calculado
CMD2
RndX
Appl A
Appl B
Appl C
RndQ
420
324
308

Fig. 5