(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 664 586**

(51) Int. CI.:

G06Q 10/08 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.06.2010 PCT/EP2010/058454**

(87) Fecha y número de publicación internacional: **10.03.2011 WO11026665**

(96) Fecha de presentación y número de la solicitud europea: **16.06.2010 E 10724092 (1)**

(97) Fecha y número de publicación de la concesión europea: **21.02.2018 EP 2473954**

(54) Título: **Procedimiento para comprobar que una mercancía es una mercancía original de un fabricante de productos a vender**

(30) Prioridad:

02.09.2009 DE 102009039823

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.04.2018

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Werner-von-Siemens-Straße 1
80333 München, DE

(72) Inventor/es:

SCHATTLEITNER, ANGELA y
SEUSCHEK, HERMANN

(74) Agente/Representante:

LOZANO GANDIA, José

PROCEDIMIENTO PARA COMPROBAR QUE UNA MERCANCÍA ES UNA MERCANCÍA ORIGINAL DE UN FABRICANTE DE PRODUCTOS A VENDER

DESCRIPCIÓN

La invención se refiere a un procedimiento y a un sistema para comprobar que una mercancía es una mercancía original de un fabricante de productos a vender, mediante autentificación de al menos un tag o etiqueta RFID (Radio Frequency Identification, identificación de rediofrecuencia) asociada a la mercancía, utilizando un protocolo Challenge-Response (reto-respuesta) asimétrico.

En el control de entrada de mercancías se somete una mercancía que llega por lo general a un control de aceptación, en el que la mercancía suministrada se comprueba en cuanto a cantidad y calidad. Esto se realiza bien mediante muestreo o bien se controla la entrada de la mercancía completa. Lo mismo es válido en principio para controles aduaneros, en los que se realiza un cotejo entre mercancías de entrada o de salida y la declaración de aduana.

En unidades de embalaje equipadas con tags RFID existe la posibilidad de realizar, en lugar del control manual físico, un control automatizado con ayuda de un aparato lector de RFID. De esta manera resulta posible comprobar muchas unidades de embalaje en un corto tiempo (Bulk Reading, lectura masiva).

En el documento EP 2 081 353 A2 se da a conocer un sistema y un procedimiento para la autentificación y firma digital. En el protocolo de autentificación descrito se envía desde la unidad a comprobar una demanda de autentificación a la instancia que ha de confirmar. La unidad a comprobar, por ejemplo un tag RFID, incluye una memoria de sólo lectura, en la que está memorizada una clave pública del tag RFID. Esta demanda de autentificación contiene la clave pública y el certificado del tag RFID que se ha leído desde la memoria de sólo lectura.

El artículo "MULTI-DOMAIN RFID ACCESS CONTROL USING ASYMMETRIC KEY BASED TAG READER MUTUAL AUTHENTICATION" (CONTROL DE ACCESO RFID DE MULTIDOMINIO DE AUTENTIFICACIÓN MUTUA UTILIZANDO LECTORA DE ETIQUETAS BASADA EN CLAVE ASIMÉTRICA), 26º CONGRESO INTERNACIONAL DE LAS CIENCIAS AERONÁUTICAS, 14 Septiembre 2008 (2008-09-14), páginas 1-10, de Mingyan Li y colab. describe uno o varios procedimientos para el control de accesos de un tag RFID mediante un procedimiento de encriptación asimétrico. Al respecto se autentifican mutuamente una unidad lectora de RFID y un Back-end-Server (servidor de soporte).

No obstante, en el marco de un tal control de calidad y de cantidad automatizado no se diferencia entre productos auténticos y falsificados. Pero partiendo de la base de problemas continuamente crecientes con piratería de producto, en particular también debido a la expansión y liberalización continuadas del comercio mundial, sería extremadamente deseable una comprobación automatizada y fiable de la autenticidad de mercancías.

La presente invención tiene así como objetivo básico proporcionar un procedimiento para la comprobación automatizada de mercancías en la recepción o en controles aduaneros, con el que se controle con fiabilidad la autenticidad de las mercancías.

Este objetivo se logra mediante un procedimiento y un sistema con las características de las reivindicaciones 1 y 2. Ventajosos perfeccionamientos de la invención se indican en las reivindicaciones dependientes.

El procedimiento de acuerdo con la invención para comprobar una mercancía como mercancía original de un fabricante de productos a vender, autentifica al menos un tag RFID asociado a la mercancía utilizando un protocolo Challenge-Response asimétrico. Primeramente se lee un código de producto a partir del tag RFID y se determina un aviso de expedición electrónico asociado. A continuación se genera un challenge o reto basándose en un número aleatorio y una clave pública y se transmite al tag RFID inalámbricamente. El tag RFID determina una response (respuesta) en base al reto transmitido y a una primera clave secreta, que está asociada al tag RFID. La respuesta determinada se comprueba para determinar un resultado de la autentificación y el resultado de la autentificación se inscribe en el aviso de expedición electrónico.

De acuerdo con la invención se propone en consecuencia dotar tags RFID de una mercancía de una clave privada PKI (Private Key Infrastructure, infraestructura de clave privada) y unirla con la mercancía irreversiblemente. En el aviso de expedición electrónico o la declaración de aduana electrónica está incluido el correspondiente bloque de datos para la autentificación (Public Key clave pública) del tag RFID. De esta manera se verifica ventajosamente con métodos criptográficos clave pública) del tag RFID. De esta manera se verifica ventajosamente con métodos criptográficos la autenticidad de la mercancía.

Ventajosamente se integra además la prueba de protección antiplagio propuesta sin discontinuidades en procesos de negocio ya existentes. Así se realiza simultáneamente en el control de entrada de mercancías también la prueba de protección antiplagio. En el sistema de gestión de mercancías se registra el estado de suministro actual de la mercancía. Estas informaciones pueden apoyar adicionalmente un proceso de gestión de la calidad.

En una variante que no es parte de la invención, está almacenado en el tag RFID un certificado digital que incluye la clave pública. El certificado digital se lee y se comprueba la autenticidad del certificado digital.

En esta variante están memorizados en el tag RFID a comprobar la clave privada y un certificado digital correspondiente. El certificado digital incluye entonces usualmente la clave pública, informaciones adicionales y una firma digital. La lectura de la clave privada se impide mediante medidas de hardware. El certificado digital por el contrario puede leerse. Se lee antes de la prueba de autenticidad mediante un aparato lector de RFID y se transmite a una unidad de comprobación. Allí se comprueba la autenticidad del certificado digital con ayuda de la firma digital. Cuando se ha verificado el certificado digital, se comprueba el tag RFID mediante un protocolo Challenge-Response asimétrico según la invención descrita. Entonces se comprueba con ayuda de la clave pública la presencia de la clave privada, sin que tenga que leerse la misma.

Según la presente invención, puede determinarse la clave pública a partir del aviso de expedición electrónico.

En la presente invención no se almacena el certificado digital en el tag RFID, sino que está registrado en el aviso de expedición electrónico para cada unidad de mercancía. En esta variante de configuración no se lee el certificado digital del tag RFID, sino que se toma del aviso de expedición electrónico. La prueba se realiza a su vez de acuerdo con la invención descrita.

El sistema de acuerdo con la invención para comprobar una mercancía como mercancía original de un fabricante autentifica al menos un tag RFID asociado a la mercancía utilizando un protocolo Challenge-Response asimétrico según el procedimiento reivindicado. El sistema presenta un aparato lector de RFID con un módulo de comunicación para la comunicación inalámbrica con el tag RFID. Además un tag RFID con un módulo de autentificación, que determina para un challenge (reto) recibido una respuesta correspondiente y un segundo módulo de comunicación para la comunicación inalámbrica con el aparato lector de RFID. Además está previsto un segundo módulo de autentificación para generar un reto y comprobar una respuesta. Un middleware (software de intercambio de información entre aplicaciones) de RFID proporciona finalmente avisos de expedición electrónicos.

A continuación se describen formas de realización preferidas del procedimiento de acuerdo con la invención y del sistema de acuerdo con la invención, con referencia a las figuras adjuntas, para describir características esenciales para la invención. Se muestra en:

figura 1 en una representación esquemática, componentes del sistema de una forma de realización posible del sistema de acuerdo con la invención,
figura 2 en una representación esquemática, componentes del sistema de otra forma de realización posible del sistema de acuerdo con la invención,
figura 3 en un esquema de circuitos en bloques, bloques funcionales de un tag RFID según el estado de la técnica,
figura 4 en un esquema de circuitos en bloques, bloques funcionales de un tag RFID adecuado para la invención,
figura 5 un diagrama secuencial de un protocolo Challenge-Response de acuerdo con la invención, para la prueba de autenticidad.

La integración de la prueba de autenticidad de mercancías en el proceso de negocio general, genera una mejor protección frente a plagios, ya que la prueba se realiza en puntos críticos del flujo de las mercancías. Mediante las medidas propuestas puede realizarse muy eficientemente la prueba antiplagio. Además, pueden detectarse los plagios tempranamente y no ser aceptados en absoluto a priori del suministrador. Así resulta un potencial de ahorro considerable, aumentando a la vez la calidad.

La figura 1 muestra componentes del sistema de una forma de realización posible del sistema de acuerdo con la invención. Las unidades de mercancía 101 representadas se encuentran por ejemplo en un puesto de entrada de mercancías u oficina de aduanas. Para comprobar la autenticidad están dotadas las unidades de mercancía 101 de respectivos tags RFID 102. Los tags RFID 102 pueden comunicar con un aparato lector de RFID 103. Este aparato lector RFID 103 está conectado permanentemente a través de una interfaz adecuada con un middleware de RFID 104. El middleware de RFID 104 está conectado a su vez con una unidad de prueba de protección antiplagio 105. Además tiene el middleware de RFID 104 acceso a un sistema de gestión de mercancías 106, a través del que existe acceso a los avisos de expedición electrónicos 107.

Se supone que el middleware de RFID 104, la unidad de prueba de protección antiplagio 105 y el sistema de gestión de mercancías 106 se encuentran en un entorno asegurado. Puesto que los tags RFID 102 se autentifican frente a la unidad de protección antiplagio 105, no tiene que autentificarse forzosamente el aparato lector de RFID 103 frente al middleware de RFID 104. La autentificación de los tags RFID 102 se realiza con un protocolo de autentificación Challenge-Response. En el sistema de gestión de mercancías 106 se contrastan los datos de los avisos de expedición electrónicos con los datos de RFID. Cuando se presentan plagios o en un suministro defectuoso, puede realizarse una señalización en el aparato lector RFID 103 o en un terminal del sistema de gestión de mercancías 106.

Para algunas aplicaciones no existe la disponibilidad permanente de una conexión online entre el aparato lector de RFID y el middleware de RFID. Un tal escenario se muestra en la figura 2. En este caso se realiza la comprobación de la entrada de mercancías 201 offline. Si existe de nuevo una conexión con el middleware de RFID 204, pueden contrastarse los datos con un retardo.

En este ejemplo de realización están disponibles los avisos de expedición electrónicos antes del suministro de las mercancías. Un aviso de expedición electrónico 207 se suministra al middleware de RFID 204 y allí se almacena temporalmente. Cuando se conecta un aparato lector RFID 203 con el middleware 204, se transmiten los avisos de expedición electrónicos 207 aún no procesados al aparato lector de RFID 203 y allí se memorizan.

La unidad lectora de RFID 203 capta ahora offline la entrada de mercancías 201 y contrasta las posiciones con el aviso de expedición electrónico. La comprobación de la autenticidad de las mercancías se realiza con ayuda de un procedimiento de autentificación con los tags RFID 202. En este ejemplo de realización se encuentra la unidad de prueba de protección antiplagio 205 en el aparato lector de RFID 203. Cuando se ha detectado una unidad de mercancías 201 como auténtica, se firma digitalmente el bloque de datos en el aviso de expedición electrónico con la clave privada del aparato lector de RFID. La firma digital se anexa como atributo adicional al aviso de expedición.

Tras el control de entrada de mercancías, se ha almacenado un aviso de expedición con atributos adicionales para la prueba de autenticidad y para la entrada de mercancías en la unidad lectora de RFID móvil 203. Este aviso de expedición ampliado se retransmite en la siguiente conexión con el middleware de RFID 204 al sistema de gestión de mercancías 206. En el sistema de gestión de mercancías 206 se reserva entonces la mercancía ingresada y se envía por ejemplo una confirmación electrónica de entrada de mercancías.

Como estructuras de datos adecuadas para reproducir un aviso de expedición electrónico con los correspondientes campos de datos para las informaciones adicionales por unidad de mercancías, son adecuadas las siguientes normas.

- Un/EDIFACT (United Nations Electronic Data Interchange for Administration, Commerce and Transport, Intercambio de datos electrónico para administración, comercio y transporte de las Naciones Unidas): Aquí podría estar incluido en el aviso de expedición (DESAV) el segmento PIA (Additional Product ID, ID de producto adicional) perteneciente al segmento LIN (Line Item, elemento de línea), la clave pública o bien el certificado digital para la prueba de autenticidad. También en la declaración de aduana electrónica (COSDEC) en el marco del procedimiento Atlas-IT podrían posibilitar los datos criptográficos adicionales una prueba de autenticidad en la introducción.

- OpenTrans: Aquí podría contener en el aviso de suministro (Dispatch Notification) el Remark-Element (elemento de observaciones) relativo a una Dispatch Notification Item el material de clave público necesario o bien el certificado digital.

Para la gestión asimétrica de claves en la comprobación de autenticidad de los tags RFID se proponen dos procedimientos.

Un ejemplo de realización posible, pero no de acuerdo con la invención, se representa en la figura 3, en la que se representa un tag RFID con una memoria 301, un módulo de autentificación 302 que incluye una clave privada 306 y un módulo de comunicación 303. Aquí se memoriza el certificado digital 304 en la memoria 301 del tag RFID. Además de un código de producto 305, están memorizados en consecuencia sobre el tag RFID adicionalmente un correspondiente certificado 304 que incluye la clave pública, informaciones adicionales y una firma digital. La lectura de la clave privada 306 se impide mediante medidas de hardware. El certificado digital puede leerse y se lee antes de la prueba de autenticidad mediante la unidad lectora de RFID y se transmite por ejemplo mediante el middleware de RFID a la unidad de prueba de protección antiplagio. Allí se comprueba la autenticidad del certificado digital en base a la firma digital. Cuando se ha verificado el certificado digital, se comprueba el tag RFID mediante protocolo Challenge-Response asimétrico. Entonces se comprueba con ayuda de la clave pública la presencia de la clave privada, sin que tenga que leerse la misma.

Un ejemplo de realización de acuerdo con la invención se muestra en la figura 4, en la que se representa un tag RFID con una memoria 401, un módulo de autentificación 402 que incluye la clave privada 404 y un módulo de comunicación 404. El código de producto 405 puede bajarse mediante la memoria 401 del tag RFID.

En esta variante no se almacena el certificado digital sobre el tag RFID, sino que se registra en el aviso de expedición electrónico para cada unidad de mercancía. La prueba de autenticidad funciona como en la variante precedente, con la diferencia de que el certificado digital no se lee desde el tag RFID, sino que se toma del aviso de expedición electrónico.

La figura 5 muestra un diagrama secuencial para un protocolo de autentificación entre un aparato lector de RFID 501 y un tag RFID 502. En este ejemplo de realización está memorizado el certificado digital en el tag RFID 502. En la primera etapa 503 lee el aparato lector de RFID 501 el certificado digital desde el tag RFID 502. El certificado digital incluye al menos la clave pública y una firma digital. El aparato lector de RFID 501 verifica con ayuda de una clave de firma pública la firma digital y con ello el certificado digital. Cuando el resultado de la verificación es negativo 504, no se autentifica el tag RFID. Pero si el resultado de la verificación es positivo 505, se genera mediante el aparato lector de RFID 501 un reto en base a la clave pública y se transmite al tag RFID. El tag RFID 502 a su vez genera en base al reto recibido y a la clave secreta una respuesta 506, que es leída por el aparato lector de RFID 501. El aparato lector de RFID 501 verifica la respuesta recibida con ayuda de la clave pública del tag RFID 501. Cuando el resultado de la verificación es negativo, no se autentifica el tag RFID Tag 501; 507. Cuando el resultado de la verificación es positivo, se autentifica el tag RFID 501 mediante el aparato lector de RFID.

El procedimiento propuesto para la prueba de protección antiplagio puede utilizarse también en el marco del despacho de aduanas en el procedimiento electrónico (Atlas= Sistema automatizado de tarifas y despacho local de aduanas). De esta manera puede evitarse selectivamente el paso de plagios a través de la frontera.

REIVINDICACIONES

1. Procedimiento para comprobar que una mercancía es una mercancía original de un fabricante de productos a vender, mediante autentificación de al menos un tag o etiqueta de Radio Frequency Identification (identificación de rediofrecuencia) RFID asociada a la mercancía, utilizando un protocolo Challenge-Response (reto-respuesta) asimétrico, con las etapas:
   - Lectura de un código de producto a partir del tag RFID mediante una unidad lectora de RFID,
   - determinación de un aviso de expedición electrónico asociado al código de producto leído,
   - generación de un challenge o reto basándose en un número aleatorio mediante un middleware acoplado con la unidad lectora de RFID,
   - transmisión inalámbrica del reto generado al tag RFID mediante la unidad lectora de RFID,
   - determinación de una response (respuesta) mediante el tag RFID en base al reto transmitido y a una primera clave criptográfica secreta, que está asociada al tag RFID,
   - comprobación de la respuesta determinada para determinar un resultado de la autentificación mediante el middelware del RFID, basándose en una clave pública,
   - inscripción del resultado de la autentificación en el aviso de expedición electrónico determinado,

   tomándose la clave pública asociada al tag RFID del aviso de expedición electrónico.

2. Sistema para comprobar que una mercancía es una mercancía original de un fabricante de productos a vender, mediante autentificación de al menos un tag o etiqueta de Radio Frequency Identification (identificación de rediofrecuencia) RFID asociada a la mercancía, utilizando un protocolo Challenge-Response (reto-respuesta) asimétrico según un procedimiento de acuerdo con la reivindicación 1, que presenta:
   - una unidad lectora de RFID con un primer módulo de comunicación para la comunicación inalámbrica con el tag RFID,
   - el tag RFID con un primer módulo de autentificación, que determina para un challenge (reto) recibido una respuesta correspondiente y un segundo módulo de comunicación para la comunicación inalámbrica con la unidad lectora de RFID,
   - un segundo módulo de autentificación para generar un reto y comprobar la respuesta determinada y
   - un middleware de RFID, para proporcionar avisos de expedición electrónicos,

   estando asociado el segundo módulo de autentificación al middleware del RFID.

3. Sistema de acuerdo con la reivindicación 2,
   en el que la unidad lectora de RFID está conectada permanentemente con el middleware del RFID y los avisos de expedición electrónicos se aportan a la unidad lectora de RFID cuando se solicita.

4. Sistema de acuerdo con la reivindicación 2,
   en el que la unidad lectora de RFID puede conectarse con el middleware del RFID y cuando existe una conexión, se aportan avisos de expedición electrónicos a la unidad lectora de RFID.

FIG 1

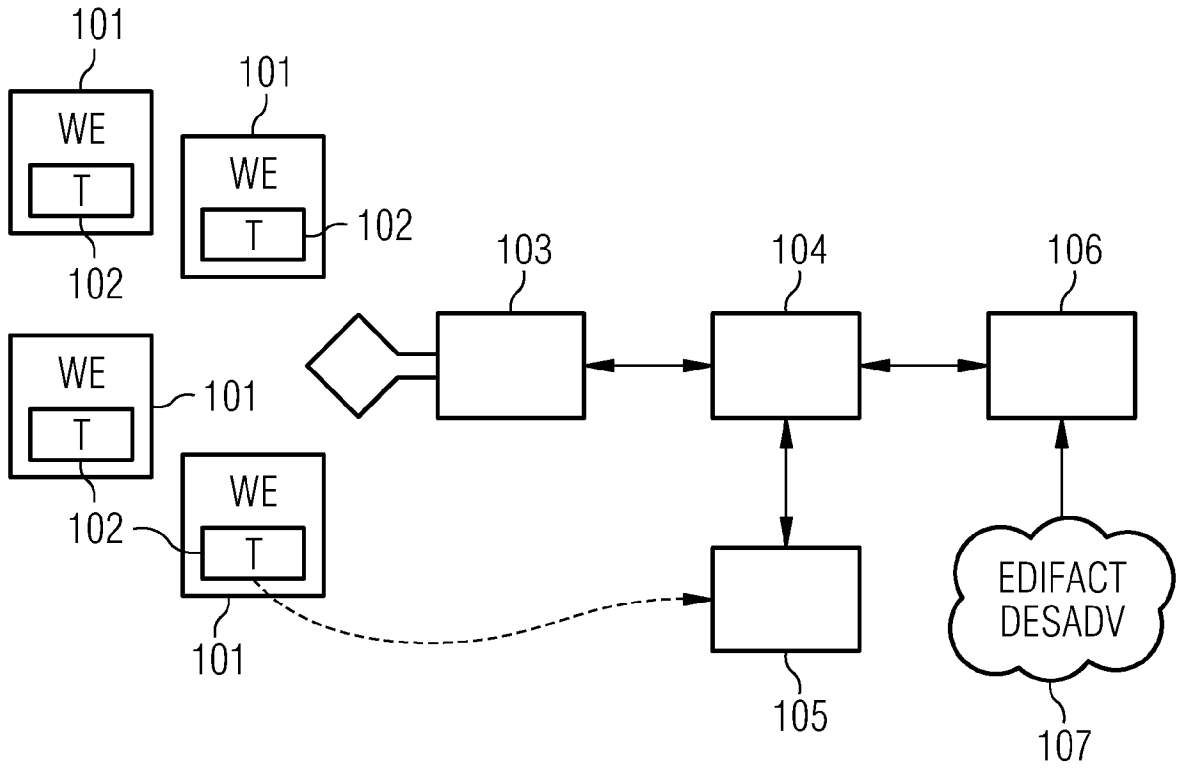

101
WE
T
102
103
104
106
105
EDIFACT
DESADV
107

FIG 2

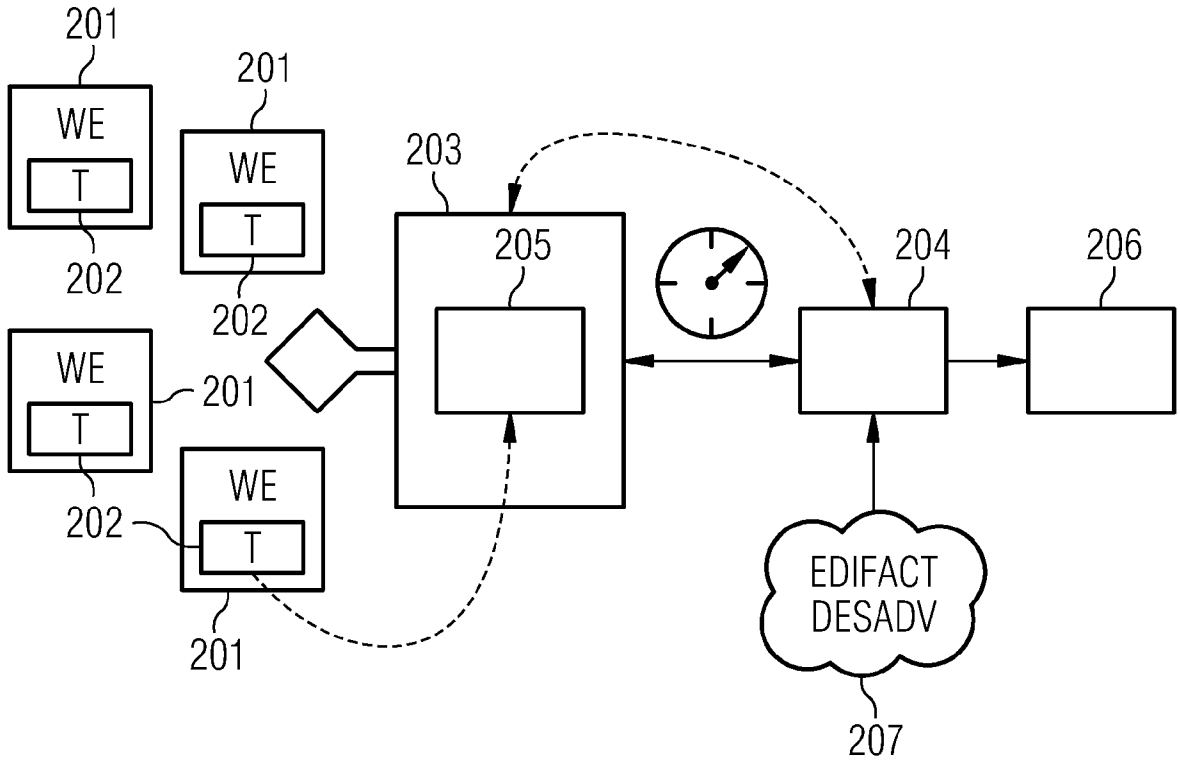

201
WE
T
202
203
205
204
206
EDIFACT
DESADV
207

FIG 3

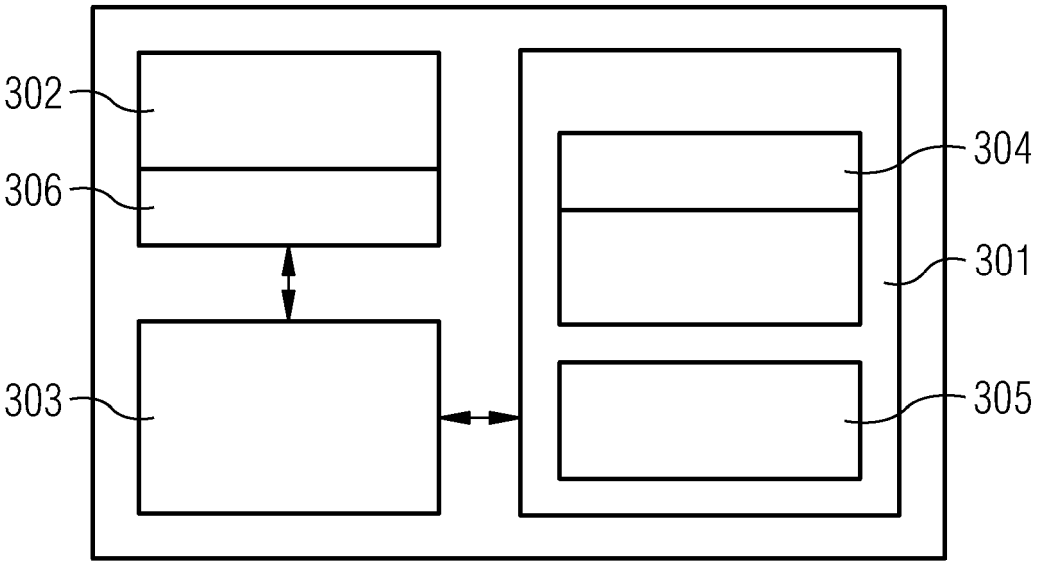


FIG 4

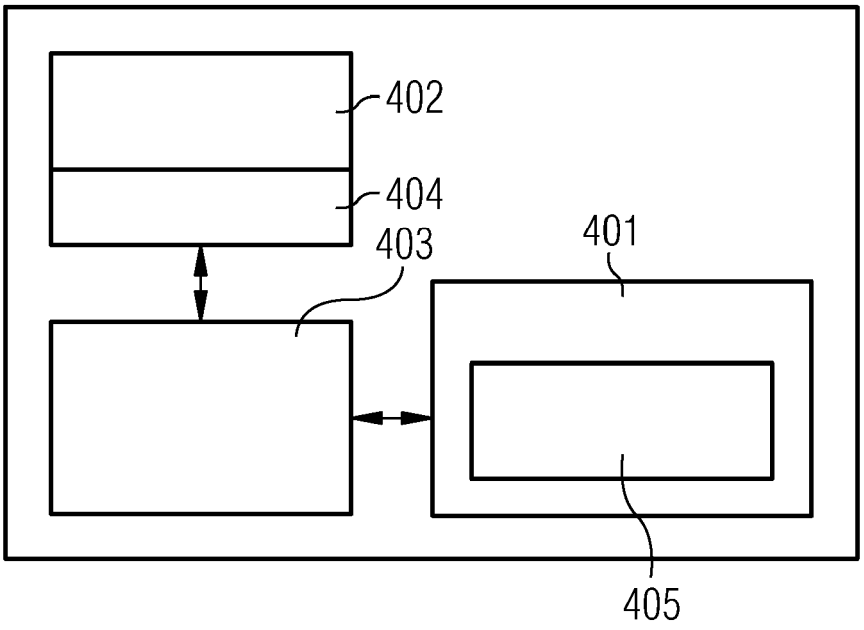
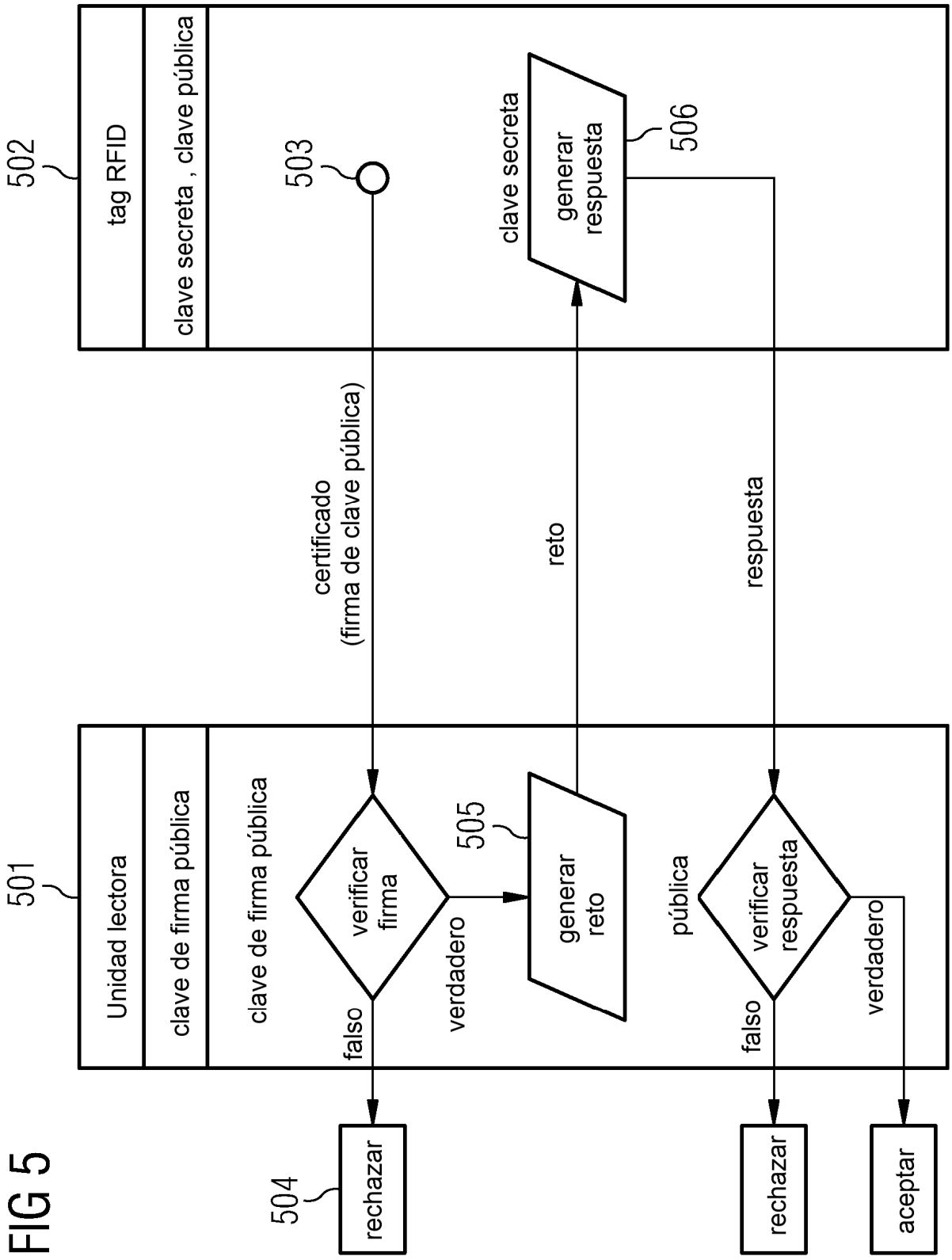


FIG 5


502
tag RFID
clave secreta , clave pública
503
clave secreta
generar respuesta
506
certificado (firma de clave pública)
reto
respuesta
501
Unidad lectora
clave de firma pública
clave de firma pública
verificar firma
falso
verdadero
505
generar reto
pública
verificar respuesta
falso
verdadero
504
rechazar
rechazar
aceptar