(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 559 264**

(51) Int. CI.:

G06F 21/44 (2013.01)
G06K 7/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.07.2013 E 13176875 (6)**

(97) Fecha y número de publicación de la concesión europea: **04.11.2015 EP 2827269**

(54) Título: **Procedimiento para autentificar una etiqueta RFID**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.02.2016

(73) Titular/es:

KAPSCH TRAFFICCOM AG (100.0%)
Am Europlatz 2
1120 Wien, AT

(72) Inventor/es:

POVOLNY, ROBERT

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Procedimiento para autentificar una etiqueta RFID

La presente invención se refiere a un procedimiento para autentificar una etiqueta RFID con la ayuda de un lector RFID a través de una interfaz de radiofrecuencia entre ellos, habiendo memorizada en el lector RFID una clave específica de usuario y habiendo memorizadas en la etiqueta RFID una identificación específica de la etiqueta y una contraseña generada a partir de la identificación y la clave, según una función de derivación conocida.

Este tipo de etiquetas RFID (en inglés *radio frequency identification tags* o *transponder*), no solo están ampliamente extendidas en la logística de mercancías para el marcado de los productos, véase por ejemplo, "*Specification for RFID Air Interface EPC(TM) Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz, Version 1.2.0*, 23 de octubre de 2008, XP05509311, sino que se utilizan cada vez más como identificación de vehículos legible por radiofrecuencia o como permiso de conducir legible por radiofrecuencia en sistemas de control de peajes y de tráfico (e*lectronic toll collection, ETC; automatic vehicle identification, AVI).* En este caso lo importante es la seguridad frente a la falsificación de la etiqueta RFID, para que no se falsifiquen la matrícula de un vehículo o una identidad de usuario y alguien acumule a expensas o a costa de un tercero tasas de peaje o infracciones de tráfico.

Ya se han implementado protocolos de autentificación sencillos en los estándares de etiquetas RFID más extendidos, por ejemplo, en los estándares ISO 18000-6C o 18000-63. Estos protocolos de autentificación se basan en la utilización de la contraseña mencionada anteriormente ("*access password*"), que se compone por un lado, por una clave secreta, conocida solo por el usuario que distribuye la etiqueta RFID y por una identificación de etiqueta memorizada individualmente en cada etiqueta. En la correspondiente etiqueta solo se memoriza esta contraseña. Con el mero conocimiento de la contraseña no puede reconstruirse la clave, es decir, la función de derivación (función de composición) de la contraseña es irreversible o no es reversible de manera inequívoca. Cuando un lector RFID quiere verificar la autenticidad de una etiqueta RFID, él o ella lee primeramente la identificación específica de la etiqueta de la etiqueta RFID, configura posteriormente con el conocimiento de la clave específica del usuario la contraseña (*access password*) y la envía a la etiqueta RFID. La etiqueta RFID comprueba la contraseña recibida con la contraseña memorizada y envía en caso de ser iguales una respuesta de confirmación de vuelta al lector RFID, véase por ejemplo, el documento US 2010/0289627 A1 o el documento WO 2008/085135 A1.

La invención tiene como objetivo la configuración más segura de un procedimiento de este tipo para autentificar etiquetas RFID, para reconocer intentos de fraude.

Este objetivo se logra con un procedimiento del tipo mencionado inicialmente, que se caracteriza por los siguientes pasos, que tienen lugar en el lector RFID:

recibir la identificación de una etiqueta RFID a autentificar a través de la interfaz de radiofrecuencia,
generar la contraseña correcta a partir de la identificación recibida y la clave memorizada según la función de derivación conocida, y generar al menos una contraseña falsa distinta de la contraseña correcta,
enviar una secuencia de al menos dos contraseñas, de las cuales al menos una es correcta y al menos una falsa, a la etiqueta RFID a través de la interfaz de radiofrecuencia, y
autentificar la etiqueta RFID, cuando no se recibe ninguna respuesta de confirmación con respecto a ninguna contraseña falsa.

La invención se basa en el conocimiento de la solicitante, de que los protocolos de autentificación conocidos podrían quedar comprometidos, cuando la identificación RFID es leída de una etiqueta "correcta" y copiada a otra etiqueta ("falsificada"), la cual reacciona –dado que no tiene conocimiento de la contraseña correcta, que se corresponde con esa identificación de etiqueta – con una respuesta de confirmación a la recepción de cualquier contraseña. Este tipo de etiquetas falsificadas pueden realizarse de una manera muy sencilla mediante los llamados "emuladores de etiquetas", los cuales reproducen el protocolo RFID por ejemplo, mediante un microcontrolador; esto permite una imitación precisa del comportamiento de una etiqueta por parte de un falsificador. La solicitante ha podido reconocer que mediante un envío repetido de varias contraseñas, de las cuales al menos una de ellas es "falsa", puede comprobarse de una manera sorprendentemente sencilla, mediante la reacción de la etiqueta RFID, si se trata de una etiqueta RFID correcta o falsificada. El procedimiento de autentificación explicado no requiere ningún tipo de modificación en la etiqueta RFID misma, de manera que pueden continuar utilizándose etiquetas RFID convencionales conforme al estándar.

Preferiblemente la sucesión de contraseñas correctas y falsas se escoge en la secuencia mencionada de manera arbitraria, de manera que una etiqueta falsificada no puede esperar una secuencia de consulta determinada y responder por ejemplo, con una secuencia de respuesta estandarizada.

Según una variante preferida, la emisión de la frecuencia puede interrumpirse tan pronto como se obtenga una respuesta de confirmación a una contraseña falsa, para minimizar la ocupación de la interfaz de radiofrecuencia. Debido al mismo motivo, también es posible que la emisión de la secuencia sea interrumpida tan pronto como no se

obtenga una respuesta de confirmación a una contraseña correcta, y la etiqueta RFID no se autentifique como consecuencia de ello.

Cuando no se obtiene ninguna respuesta de confirmación a una contraseña correcta, esto no tiene que indicar siempre obligatoriamente una etiqueta RFID falsificada, también podría interrumpirse simplemente la interfaz de radiofrecuencia, debido a que la etiqueta RFID ha abandonado el alcance de radiofrecuencia de la interfaz de radiofrecuencia. Para detectar esto, puede preverse según otra variante de la invención, que la última contraseña de la secuencia sea siempre una contraseña correcta. Si no se obtiene ninguna respuesta de confirmación en un periodo de tiempo predeterminado, la interfaz de radiofrecuencia está interrumpida y posiblemente ya estaba interrumpida antes en el caso de una contraseña falsa, de manera que se desecha la totalidad del proceso de autentificación y no se autentifica la etiqueta RFID.

Alternativamente, la emisión de la secuencia puede continuarse durante tanto tiempo, hasta que la etiqueta RFID se encuentre en el alcance de radiofrecuencia de la interfaz de radiofrecuencia, de manera que puede llevarse a cabo una cantidad máxima de emisiones de contraseñas (correctas y falsas), lo cual minimiza las probabilidades de éxito de un fraude con una etiqueta RFID falsificada. La comprobación de si la etiqueta RFID aún se encuentra en el alcance de radiofrecuencia, puede medirse en este caso mediante consultas de radiofrecuencia que parten del lector RFID; en el momento en el que ya no se reciba ninguna respuesta a una consulta de radiofrecuencia de este tipo, el alcance de radiofrecuencia claramente está interrumpido.

Según otra característica de la invención, la identificación de una etiqueta RFID, la cual ha enviado una vez una respuesta de confirmación a una contraseña falsa, puede memorizarse en una lista negra, para tomar entonces medidas necesarias. Puede comprobarse por ejemplo, tras la recepción de la identificación de una etiqueta RFID a autentificar, si la identificación recibida está memorizada en la lista negra, y si es así, no autentificarse la etiqueta RFID e interrumpirse el procedimiento. Una etiqueta RFID reconocida una vez como falsificada, entonces ya no puede ser utilizada.

La invención es adecuada para todos aquellos estándares de comunicación entre etiquetas RFID y lectores RFID, los cuales utilizan el protocolo de autentificación con *access passwords* indicado inicialmente, particularmente para los estándares ISO 18000-6C y 18000-63 o estándares compatibles con ellos, y no requiere ninguna modificación de las etiquetas RFID. Esto es particularmente ventajoso, dado que las etiquetas RFID son un producto en masa económico, que está en amplia circulación en muchas formas de diseño de los productores más diversos y solo ha de cumplir requisitos mínimos de los estándares mencionados, de manera que no es necesaria una modificación de los estándares en lo que se refiere a este requisito mínimo para el procedimiento de autentificación que aquí se indica.

La invención se explica a continuación con mayor detalle mediante ejemplos de realización representados en los dibujos que se adjuntan. En los dibujos muestran:

La Fig. 1 las relaciones de radiocomunicación entre un lector RFID y una etiqueta RFID que pasa por éste en el marco del procedimiento según la invención;
La Fig. 2 un diagrama de bloques y al mismo tiempo un diagrama de flujo del procedimiento de la invención; y
Las Figs. 3 a 5 diagramas de secuencia de la transmisión de datos que se desarrolla en la interfaz de radiofrecuencia entre el lector RFID y la etiqueta RFID en el marco del procedimiento según la invención.

La Fig. 1 muestra una etiqueta RFID (*radio frequency identification tag*) 1, que lleva a cabo en un momento t_1 a través de una interfaz de radiofrecuencia 2 radiocomunicaciones con un lector RFID 3. El alcance de radiofrecuencia de la interfaz de radiofrecuencia 2 alrededor del lector 3 se indica con 4. La etiqueta 1 se mueve pasando por el lector 3 en dirección de la flecha 5. Con líneas discontinuas se indican tres posiciones más de la etiqueta 1 en momentos t_2, t_3, t_4, que se suceden, en los cuales se producen correspondientemente otras comunicaciones de radiofrecuencia a través de la interfaz de radiofrecuencia 2.

El contenido de las comunicaciones de radiofrecuencia o los paquetes de datos que se intercambian a través de la interfaz de radiofrecuencia 2 entre la etiqueta 1 y el lector 3, es de cualquier tipo, y en lo sucesivo solo se describen aquellas partes del protocolo de comunicación a través de la interfaz de radiofrecuencia 2, las cuales se ocupan de la autentificación de la etiqueta 1 frente al lector 3.

Los componentes participantes en el proceso de autentificación y los pasos de procedimiento básicos se explican mediante la Fig. 2, que describe una etiqueta 1 según el estándar ISO 18000-6C o 18000-63. Se entiende, que la etiqueta 1, el protocolo de la interfaz de radiofrecuencia 2 y el lector 3, también pueden estar configurados según otro estándar que ponga a disposición las funcionalidades de autentificación descritas.

Según la Fig. 2, la etiqueta 1 comprende cuatro zonas de memoria 6 – 9 con una protección diferente, y concretamente:

- una primera zona de memoria 6, que puede ser leída y escrita a voluntad por la interfaz de radiofrecuencia 2, por ejemplo, para programas de aplicación que se ejecutan en un lector 3;
- una segunda zona de memoria 7 que puede leerse mediante la interfaz de radiofrecuencia 2, para la grabación de una identificación específica de etiqueta TID, inequívoca; la zona de memoria 7 solo puede ser escrita en el transcurso de la producción de la etiqueta 1 por parte de un proceso de producción 10, el cual adjudica las identificaciones de etiqueta TID, y por lo demás está protegida frente a la escritura;
- una tercera zona de memoria 8, que en el caso de la inicialización de la etiqueta 1 específica del usuario, puede ser escrita por parte de un proceso de inicialización 11, estando protegida después frente a la escritura, y siendo legible después mediante la interfaz de radiofrecuencia 2; el proceso de inicialización 11 puede ser escrito por ejemplo, por un usuario, por ejemplo, operador del sistema, que adquiere un lote de etiquetas 1 con diferentes identificaciones de etiqueta TID, con datos específicos de usuario (específicos de operador), por ejemplo, una identificación del operador o un índice i, que remite a una de varias claves K_i específicas de usuario memorizadas en una tabla de claves 12 del proceso 11; y
- una zona de memoria 9 reservada, que no puede ser leída mediante la interfaz de radiofrecuencia 2, en la que solo puede depositar datos el proceso de inicialización de usuario 11, en este caso, una contraseña PW ("*access password*"), y a la que solo pueden acceder determinados procesos en la etiqueta 1 misma, como se explicará más adelante con mayor detalle.

La contraseña PW es configurada en la inicialización de la etiqueta 1 por parte del proceso 11, por un lado, partir de la identificación de etiqueta TID, y por otro lado, a partir de la clave K_i específica de usuario, por ejemplo, según un algoritmo de Hash de forma:

$$\mathbf{PW = truncate\ (SHA\text{-}1(concatinate\ (K_i+TID)))}$$

Basándose en esta estructura de memoria, configuración e inicialización, una etiqueta 1 puede autentificarse frente a un lector 3, el cual dispone de la o las claves K_i específicas de usuario, de la siguiente manera.

En un primer paso (a), un proceso 13 en el lector 3 lee la identificación de etiqueta TID desde la zona de memoria 7 protegida frente a la escritura, pero accesible públicamente, a través de la interfaz de radiofrecuencia 2. A continuación, se lee en el paso (b) también el índice de claves i de la zona de memoria 8 protegida frente a la escritura, pero accesible públicamente, a través de la interfaz de radiofrecuencia 2, y se saca la correspondiente clave K_i de una tabla de claves 14 del lector 3, que se corresponde con la tabla de claves 12 del usuario o del proceso de inicialización 11. En caso de que solo deba utilizarse una única clave K, ya no es necesaria la memorización y la consulta del índice de claves i, suprimiéndose de esta manera el paso (b).

En el proceso 13, se forma a continuación, el valor Hash

$$SHA\text{-}1(concatinate\ (K_i+TID))$$

y se genera mediante truncado en el paso 15, la contraseña *access* PW para la etiqueta 1.

La contraseña PW se envía a continuación, en el paso (c), a un proceso de comprobación 16 en la etiqueta 1, que compara la contraseña PW recibida, con la contraseña PW memorizada en la zona de memoria 9 protegida, accesible solo para el proceso 16. Solo en caso de ser iguales se envía de vuelta en el paso (d) una respuesta de confirmación ("*handle*") hdl a través de la interfaz de radiofrecuencia 2 al lector 3 consultante; la recepción de una respuesta de confirmación de este tipo en el lector 3, autentifica la etiqueta 1 como correcta (auténtica).

Las siguientes ampliaciones del procedimiento descrito, sirven para evitar intentos de fraude mediante etiquetas 1 falsificadas, que responden no obstante, al recibir cualquier contraseña PW en el paso (c), también falsas (es decir, que no son iguales a la contraseña PW memorizada en la zona 9), siempre con una respuesta de confirmación hdl en el paso (d).

Además de la contraseña PW "correcta", que se configura de la manera descrita basándose en la clave específica de usuario K_i y a la identificación específica de etiqueta TID según una instrucción de derivación conocida, por ejemplo, el procedimiento Hash mencionado, el lector 3 genera algunas contraseñas $PW_{f,j}$ "falsas" adicionales, como se ilustra mediante el bloque 18 en la Fig. 2, controladas por ejemplo, por un generador aleatorio 19. El lector 3 envía ahora no solo la contraseña PW "correcta", indicada en lo sucesivo como PW_r, a la etiqueta 1, sino también al menos una contraseña $PW_{f,j}$ "falsa".

La Fig. 3 muestra la reacción de una etiqueta 1 verdadera (TAG_1), es decir, auténtica, a una secuencia 20 de este tipo, de transmisiones de contraseñas (c). Las Figs. 4 y 5 muestran frente a ello, la reacción de una etiqueta 1 falsificada (TAG_2) a la misma secuencia 20. La secuencia 20 mostrada aquí a modo de ejemplo, es correcta (R) – falsa (F) – falsa (F) – correcta (R), es decir, PW_r - $PW_{f,1}$ - $PW_{f,2}$ - PW_r. Como puede verse, la etiqueta RFID TAG_1 verdadera, solo responde a contraseñas PW_r correctas con una respuesta de confirmación hdl (d), respondiendo una etiqueta RFID falsificada o falsa TAG_2, TAG_3, por el contrario siempre con una respuesta de confirmación hdl (d), también en el caso de contraseñas $PW_{f,1}$, $PW_{f,2}$ falsas.

El lector 3 (RD) comprueba ahora, tras – o durante – el desarrollo de la secuencia 20, si se obtuvo para ella también la secuencia correcta de respuestas (d), es decir, en la secuencia 20 “R – F – F - R” a modo de ejemplo, una secuencia de respuestas igual “hdl – ninguna respuesta – ninguna respuesta – hdl”. En caso de no obtenerse ninguna respuesta de confirmación hdl para ninguna contraseña falsa $PW_{f,j}$, se autentifica (21) la etiqueta 1, de lo contrario no (22).

Como se muestra en el ejemplo de la Fig. 4, el proceso ya puede interrumpirse, y detectarse la etiqueta 1 como no auténtica, tan pronto como se obtenga (23) por primera vez una respuesta de confirmación hdl a una contraseña falsa $PW_{f,j}$.

También puede interrumpirse el procedimiento y detectarse la etiqueta 1 como no auténtica, cuando para una contraseña correcta PW_r no se obtiene ninguna respuesta de confirmación hdl – preferiblemente en un periodo de tiempo T-, véase el paso 24 en la Fig. 5.

No solo puede generarse de manera aleatoria el contenido de las contraseñas falsas $PW_{f,j}$, sino que la sucesión de contraseñas correctas y falsas en la secuencia 20 también puede ser determinada por el generador aleatorio 19. La cantidad de contraseñas correctas y falsas PW_r, $PW_{f,j}$, en la secuencia 20 puede elegirse tan grande como se quiera, cuantas más, más seguro será el procedimiento de autentificación. Son necesarias al menos, una contraseña correcta PW_r y una contraseña falsa PW_f en la secuencia 20. Pueden enviarse por ejemplo, consultas de contraseña (c) durante tanto tiempo por parte del lector 3 a una etiqueta 1, para que pueda continuarse la secuencia 20 y puedan evaluarse (d) las respuestas, como la etiqueta 1 se encuentre en el alcance de la radiofrecuencia 4 del lector 3.

Para comprobar si una etiqueta 1 aún se encuentra en el alcance de la radiofrecuencia 4 de un lector 3, es decir, si realmente podría responder a una contraseña correcta PW_r, la secuencia 20 también podría establecerse tan corta, que la cantidad de consultas (c) ocurriese en todo caso en el periodo de tiempo $t_3 – t_1$, en el que una etiqueta 1 se mueve con la velocidad 5 a través de la zona 4 cubierta por la radiofrecuencia del lector 3. Al mismo tiempo puede determinarse que la última contraseña PW de la secuencia 20 siempre sea en todo caso una contraseña correcta PW_r, de la que puede esperarse una respuesta de confirmación hdl. Alternativa o adicionalmente puede determinarse con la ayuda de otras medidas, si una etiqueta 1 se encuentra dentro del alcance de la radiofrecuencia 4, por ejemplo, mediante consultas de radiofrecuencia adicionales, que parten del lector 3, a través de la interfaz de radiofrecuencia 2.

Tan pronto como se ha reconocido una etiqueta 1 como falsa (pasos 22, 23, 24), puede memorizarse la identificación de etiqueta TID de esa etiqueta 1 en una lista negra 25 en el lector o en una unidad conectada a éste. La lista negra 25 puede ser consultada ya en el paso (a), cuando se consulta la identificación de etiqueta TID de una etiqueta 1 a autentificar.

La invención no está limitada a las formas de realización representadas, sino que comprende todas las variantes y modificaciones, las cuales quedan en el marco de las reivindicaciones que acompañan.

REIVINDICACIONES

1. Procedimiento para autentificar una etiqueta RFID (1) con la ayuda de un lector RFID (3) a través de una interfaz de radiofrecuencia (2) entre ellos, estando memorizada en el lector RFID (3) una clave específica de usuario (K_i) y estando memorizadas en la etiqueta RFID una identificación específica de la etiqueta y una contraseña (PW) generada a partir de la identificación (TID) y la clave (K_i), según una función de derivación conocida, y reenviando, a través de la interfaz de radiofrecuencia (2), una etiqueta RFID (1) auténtica una respuesta de confirmación (hdl) solo al recibir la contraseña correcta (PW_r), por el contrario, una etiqueta RFID (1) no auténtica, al recibir una contraseña cualquiera (PW_f), comprendiendo los siguientes pasos que tienen lugar en el lector RFID (3):

recibir (a) la identificación (TID) de una etiqueta RFID (1) a autentificar a través de la interfaz de radiofrecuencia (2),
generar (13 – 15) la contraseña correcta (PW_r) a partir de la identificación (TID) recibida y la clave (K_i) memorizada según la función de derivación conocida, y generar (18 – 19) al menos una contraseña falsa (PW_f) distinta de la contraseña correcta (PW_r),
enviar una secuencia (20) de al menos dos contraseñas (PW_r, $PW_{f,j}$), de las cuales al menos una es correcta y al menos una falsa, a la etiqueta RFID (1) a través de la interfaz de radiofrecuencia (2), y
autentificar la etiqueta RFID, cuando no se recibe ninguna respuesta de confirmación (hdl) con respecto a ninguna contraseña falsa ($PW_{f,j}$).

2. Procedimiento según la reivindicación 1, caracterizado por que la secuencia (20) de contraseñas correctas y falsas (PW_r, $PW_{f,j}$) se elige aleatoriamente en la secuencia (20) mencionada.

3. Procedimiento según las reivindicaciones 1 o 2, caracterizado por que la emisión (d) de la secuencia (20) se interrumpe tan pronto como se recibe una respuesta de confirmación (hdl) a una contraseña falsa ($PW_{f,j}$).

4. Procedimiento según una de las reivindicaciones 1 a 3, caracterizado por que la emisión (d) de la secuencia (20) se interrumpe tan pronto como no se recibe ninguna respuesta de confirmación (hdl) a una contraseña correcta (PW_r), y debido a ello la etiqueta RFID (1) no se autentifica.

5. Procedimiento según una de las reivindicaciones 1 a 4, caracterizado por que la última contraseña de la secuencia (20) es una contraseña correcta (PW_r).

6. Procedimiento según una de las reivindicaciones 1 a 4, caracterizado por que la emisión (d) de la secuencia (20) se continúa durante todo el tiempo en que la etiqueta RFID (1) se encuentra en el alcance de la radiofrecuencia (4) de la interfaz de radiofrecuencia (2).

7. Procedimiento según la reivindicación 6, caracterizado por que el alcance de la radiofrecuencia (4) se mide mediante consultas de radiofrecuencia de la etiqueta RFID (1) que parten del lector RFID (3).

8. Procedimiento según una de las reivindicaciones 1 a 7, caracterizado por que la identificación (TID) de una etiqueta RFID (1), que ha enviado una respuesta de confirmación (hdl) a una contraseña falsa ($PW_{f,j}$), se memoriza en una lista negra (25).

9. Procedimiento según la reivindicación 8, caracterizado por que tras la recepción (a) de la identificación (TID) de una etiqueta RFID (1) que hay que autentificar se comprueba si la identificación (TID) recibida está memorizada en la lista negra (25), y en caso de ser así, no se autentifica la etiqueta RFID (1) y se interrumpe el procedimiento.

10. Procedimiento según una de las reivindicaciones 1 a 9, caracterizado por que la etiqueta RFID (1) y el lector RFID (3) trabajan según el estándar ISO 18000-6C, ISO 18000-63 o un estándar compatible con ellos.

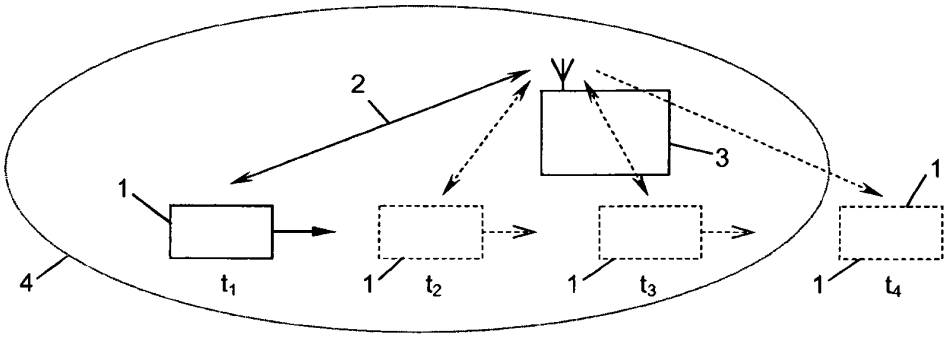
2
3
1
1
1
1
1
4
t1
t2
t3
t4

Fig. 1

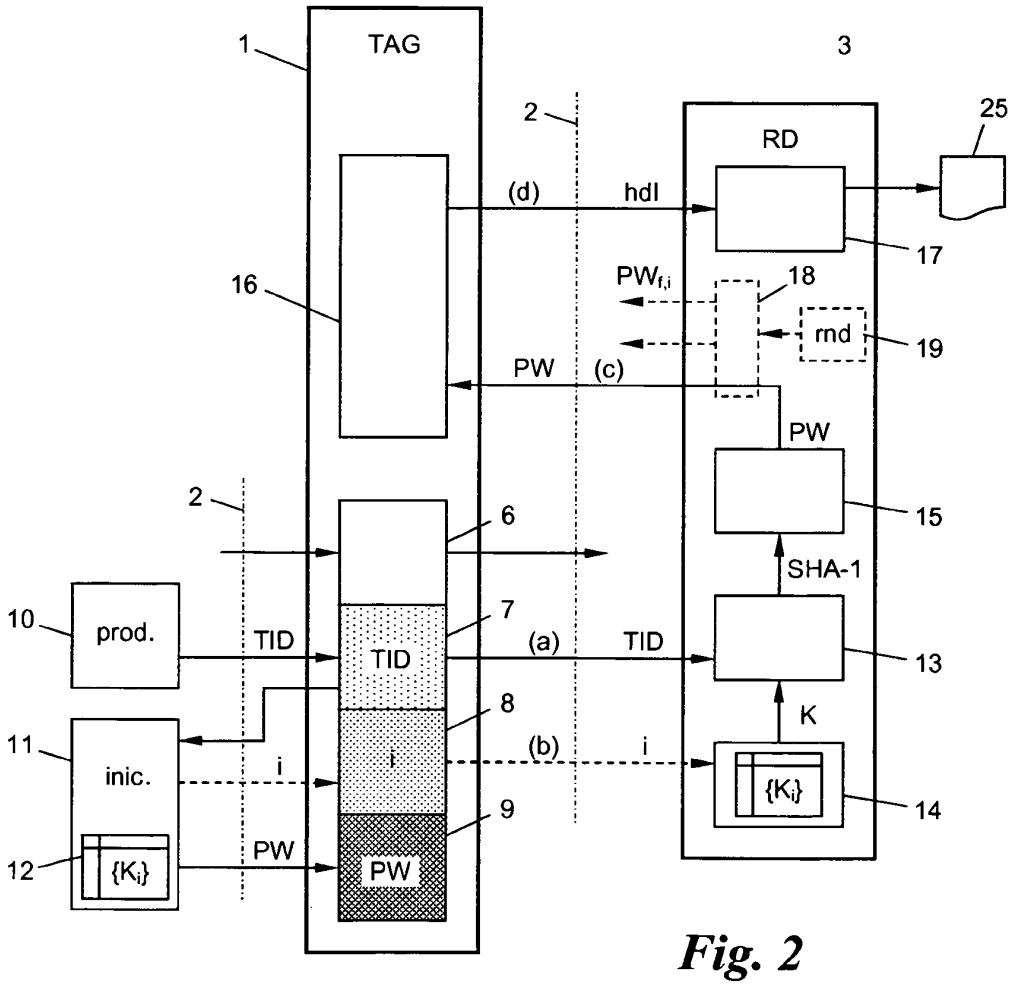
1
TAG
3
2
RD
25
(d)
hdl
17
16
PWf,i
18
rnd
19
PW
(c)
PW
2
6
15
SHA-1
10
prod.
TID
TID
7
(a)
TID
13
8
K
11
inic.
i
(b)
i
{Ki}
14
9
12
{Ki}
PW
PW

Fig. 2

Fig. 3

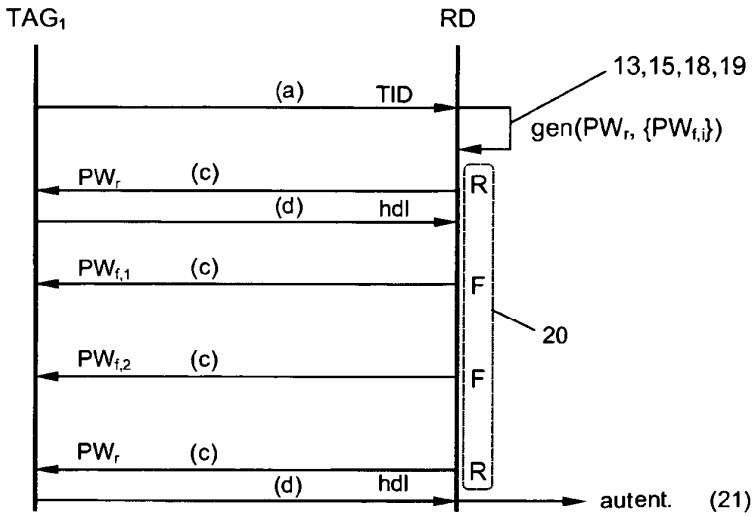

Fig. 4

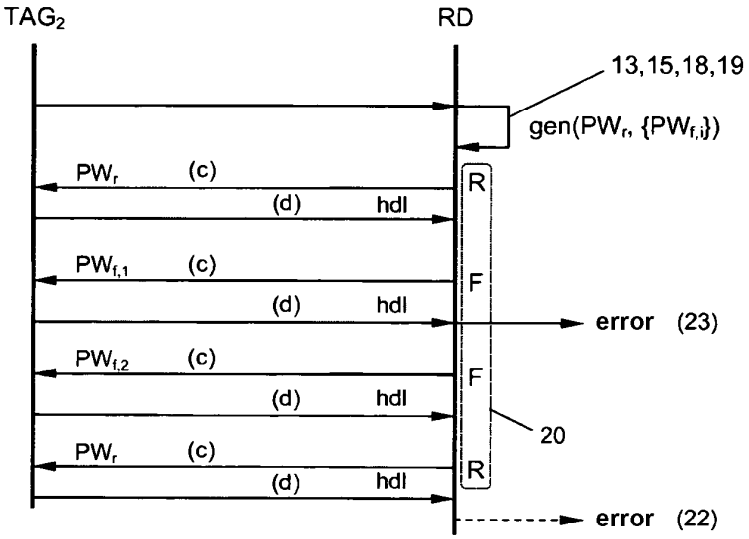

Fig. 5