(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 624 298**

(51) Int. CI.:

G06F 21/50 (2013.01)
G06K 7/10 (2006.01)
G06K 7/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **19.11.2013 PCT/EP2013/003493**

(87) Fecha y número de publicación internacional: **30.05.2014 WO14079561**

(96) Fecha de presentación y número de la solicitud europea: **19.11.2013 E 13801984 (9)**

(97) Fecha y número de publicación de la concesión europea: **22.02.2017 EP 2923299**

(54) Título: **Procedimiento para operar un sistema de comunicaciones**

(30) Prioridad:

21.11.2012 DE 102012022735

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.07.2017

(73) Titular/es:

GIESECKE & DEVRIENT GMBH (100.0%)
Prinzregentenstrasse 159
81677 München, DE

(72) Inventor/es:

WACKER, DIRK y
MARTINI, ULLRICH

(74) Agente/Representante:

DURÁN MOYA, Luis Alfonso

DESCRIPCIÓN

Procedimiento para operar un sistema de comunicaciones

La invención se refiere a un procedimiento para operar un sistema de comunicaciones. El sistema de comunicaciones comprende un transpondedor con al menos una antena. El transpondedor puede estar diseñado en particular en la forma de un soporte de datos portátil con forma de tarjeta. Además, el sistema de comunicaciones comprende un dispositivo de lectura con al menos una antena, en el que el dispositivo de lectura está configurado para intercambiar datos con el transpondedor. Dentro de un rango predeterminado es posible un intercambio de datos entre el transpondedor y el dispositivo de lectura. Para asegurar la comunicación ante un ataque de transmisión (*"rely-attack"*) se efectúa una medición y evaluación por el dispositivo de lectura del tiempo de transmisión de un comando desde el dispositivo de lectura al transpondedor y de recepción de una respuesta correspondiente del transpondedor.

Para evitar un ataque de transmisión puede llevarse a cabo una medición del tiempo de propagación de señal. El tiempo total de propagación se compone del tiempo de propagación de una señal (trayecto de transmisión de un comando y trayecto de recepción de una respuesta) junto con el tiempo para procesar y recibir el comando y para emitir la respuesta. El tiempo total de propagación no puede exceder por tanto un determinado valor máximo.

Para la verificación, se conoce también a través del denominado protocolo de limitación de distancia (*"distance bounding protocol"*) verificar un límite máximo de la distancia física entre una unidad de verificación (verificador V) y una unidad de prueba (probador P). El procedimiento se basa en la evaluación del tiempo de retardo entre la emisión de una prueba (*"challenge"*) y la recepción de una respuesta correspondiente a la misma. El tiempo de retardo permite a la unidad de verificación calcular un límite máximo de la distancia de comunicación. El procedimiento se basa en el hecho de que las ondas electromagnéticas se propagan casi a la velocidad de la luz, pero nunca más rápido.

En una variante de este protocolo, la unidad de verificación, por ejemplo un dispositivo de lectura, y la unidad de verificación, por ejemplo un transpondedor, pueden compartir un secreto conjunto para una autentificación de tipo prueba-respuesta. En este caso, el transpondedor no envía la respuesta al dispositivo de lectura. En lugar de ello, el dispositivo de lectura pregunta por una o varias partes de la respuesta de forma aleatoria, a las cuales el transpondedor debe responder dentro de un intervalo de tiempo. Este proceso puede repetirse para incrementar la seguridad. Esta variante se trata en principio de un protocolo criptográfico, en el que unos resultados se deben presentar dentro de intervalos de tiempo específicos. Esto hace que sea más difícil para un atacante llevar a cabo un denominado ataque de transmisión, ya que el atacante no puede proporcionar los resultados de la prueba en el intervalo de tiempo especificado. En este caso se superan forzosamente los intervalos de tiempo específicos.

En soportes de datos portátiles sin contacto de acuerdo con la norma ISO/IEC 14443 no es posible ejecutar el protocolo de limitación de distancia descrito anteriormente, de manera que un sistema de comunicaciones de un soporte de datos y un dispositivo de lectura portátiles no puede llevar a cabo un reconocimiento de si los dos participantes en la comunicación están realmente dispuestos dentro del rango de comunicación de aproximadamente 10 cm o si, debido a un ataque de transmisión, una comunicación del soporte de datos tiene lugar con un dispositivo de lectura remoto, sin contacto, lo que no es deseable para el propietario del soporte de datos. Una realización del protocolo de limitación de distancia resultaría en una extensión de la ISO/IEC 14443 para ser capaz de implementar los requerimientos de tiempo tan precisos del comportamiento de la respuesta del soporte de datos.

La presente invención plantea el objetivo de especificar un procedimiento para operar un sistema de comunicaciones con el que un ataque de transmisión puede reconocerse de forma fiable o bien ser rechazado inmediatamente. En particular, este procedimiento debe estar previsto para que un dispositivo de lectura pueda valorar el procedimiento de tiempo de respuesta de un transpondedor. En este caso, no se requeriría en particular ningún cambio en la norma existente ISO/IEC 14443. Un objetivo adicional consiste en especificar un sistema de comunicaciones correspondiente.

A partir del documento US 2012/249296 A1 se deriva un procedimiento para asegurar una comunicación NFC frente a ataques en el que un intercambio de información entre un dispositivo de lectura y una tarjeta sin contacto tiene lugar con una duración determinada. De acuerdo con el procedimiento, una señal de retroalimentación es encriptada por medio de un pseudoalgoritmo.

Este objetivo se logra mediante un procedimiento de acuerdo con las características de la reivindicación 1 así como con un sistema de comunicaciones de acuerdo con las características de la reivindicación 13. A partir de las respectivas reivindicaciones dependientes se desprenden unas realizaciones ventajosas.

La invención sugiere un método para operar un sistema de comunicaciones que comprende un transpondedor con al menos una antena, en particular en la forma de un soporte de datos portátil, así como un dispositivo de lectura con al

menos una antena. El dispositivo de lectura está configurado para intercambiar datos con el transpondedor. Un intercambio de datos entre el transpondedor y el dispositivo de lectura es posible con un alcance predeterminado. Se efectúa una medición y evaluación del periodo de tiempo de un comando transmitido desde el dispositivo de lectura al transpondedor y de recepción de una respuesta correspondiente del transpondedor por el dispositivo de lectura. De este modo, se consigue un procesamiento de un periodo de tiempo específico de tarjeta, en el que el periodo de tiempo específico de tarjeta especifica cuánto tiempo utiliza el transpondedor en recibir y procesar un comando recibido desde el dispositivo de lectura así como en enviar una respuesta correspondiente. El periodo de tiempo medido es evaluado en el dispositivo de lectura utilizado el periodo de tiempo específico de tarjeta.

El procedimiento sugerido hace posible reconocer ataques de transmisión. De este modo, no es necesario efectuar modificaciones en un transpondedor configurado según la norma ISO/IEC 14443. El único condicionante para llevar a cabo el procedimiento es que el dispositivo de lectura pueda efectuar una medición del periodo de tiempo. El procedimiento permite obtener una precisión elevada en el reconocimiento de un ataque de transmisión.

De acuerdo con la invención, el periodo de tiempo específico de tarjeta se transmite con la respuesta del transpondedor al dispositivo de lectura para ser evaluado. La evaluación del periodo de tiempo específico de tarjeta permite al dispositivo de lectura decidir si un ataque de transmisión está llevándose a cabo o no.

De acuerdo con una realización adicional, el dispositivo de lectura mide el periodo de tiempo entre el envío del comando y la recepción de la respuesta del transpondedor, pudiendo inferirse un ataque de transmisión por medio de la diferencia entre el periodo de tiempo medido y el periodo de tiempo específico de tarjeta. Cuando la diferencia es mayor que un valor límite predeterminado entonces puede inferirse un ataque. De acuerdo con esta realización, el periodo de tiempo neto de la señal menos el tiempo de procesamiento en el transpondedor se utiliza en el procedimiento para decidir si un ataque de transmisión tiene lugar o no.

De acuerdo con una realización apropiada adicional, el periodo de tiempo específico de tarjeta se transmite de forma segura desde el transpondedor al dispositivo de lectura. De este modo, es posible una transmisión veraz del periodo de tiempo específico de tarjeta al dispositivo de lectura. La transmisión segura puede tener lugar por medio de un mecanismo de encriptación clásico como por ejemplo claves de sesión (*"sesion keys"*) o un procedimiento de intercambio de clave de tipo Diffie-Hellman o cualquier tipo de autentificación segura. De este modo, un atacante de transmisión no puede simplemente obtener el periodo de tiempo específico de tarjeta y emplearlo para eludir un procedimiento seguro.

En una realización adicional, el comando es una prueba (*"challenge"*) en el contexto de una autentificación de tipo prueba-respuesta. El periodo de tiempo específico de tarjeta es transmitido entonces al dispositivo de lectura junto con la respuesta como contestación.

Alternativa o adicionalmente, la prueba puede resultar en un cambio en el periodo de tiempo determinado por el dispositivo de lectura. De este modo, se consigue ventajosamente que el tiempo de ejecución en el transpondedor pueda ser influenciado de forma controlada por la prueba transmitida. Para ello, se utilizan valores de datos como prueba. De este modo, los ataques de transmisión pueden ser repelidos de forma muy efectiva en el caso de que un canal encriptado no pueda rechazar este tipo de ataque.

En una realización alternativa de la invención, el procedimiento es realizado varias veces. El periodo de tiempo entre la etapa de envío y la etapa de recepción se determina respectivamente y se compara con un periodo de tiempo predeterminado como valor límite. Este periodo de tiempo normalmente es el mínimo periodo de tiempo específico de tarjeta para la orden, más el tiempo requerido para la comunicación. Alternativamente, en vez del periodo de tiempo mínimo, se determina un valor medio de periodos de tiempo medidos y se emplea como periodo de tiempo predeterminado. Como valor medio es adecuado en particular tomar el número medio o la media aritmética o geométrica de los periodos de tiempo medidos.

El periodo de tiempo ideal es en este caso un valor que se obtiene bajo condiciones de ensayo o ideales. El mínimo periodo de tiempo es en cambio el periodo de tiempo medido para el sistema de comunicaciones real, que coherentemente es mayor que el periodo de tiempo ideal.

Mediante la repetición del procedimiento y la comparación con el periodo de tiempo mínimo o el periodo de tiempo predeterminado, el ruido de la señal desaparece o al menos es reducido considerablemente. Retrasos excepcionales durante la transmisión y/o influencias ambientales excepcionales que llevan a un incremento del periodo de tiempo medido, no estando en principio provocadas por un ataque de transmisión, pueden filtrarse tomando el valor medio entre los periodos de tiempo ya medidos. En otras palabras, el ruido de la señal se reduce al tomar el valor medio. Por tanto, es posible asumir tolerancias de tiempo más pequeñas, cuya superación conlleve el reconocimiento de un ataque de

transmisión. Mediante esta repetición múltiple se hace mucho más difícil llevar a cabo un ataque de transmisión y el procedimiento de comunicación se mejora en gran medida.

El número de repeticiones no está limitado, para reducir significativamente el ruido son adecuadas mil o más repeticiones. También está previsto interrumpir la repetición del procedimiento y reinicializarlo. Esto es razonable cuando los periodos de tiempo actualmente medidos en las repeticiones individuales difieren entre sí considerablemente, por ejemplo se diferencian en un 30% o más.

De acuerdo con la invención, está previsto adicionalmente que el periodo de tiempo medido dependa de la longitud del comando y que, el periodo de tiempo ideal, periodo de tiempo mínimo y/o medio o promedio de los periodos de tiempo medidos esté almacenado en el dispositivo de lectura como valor de referencia. Grandes desviaciones respecto de este valor de referencia indican consecuentemente ataques de transmisión desde un primer momento y aseguran adicionalmente el sistema de comunicaciones.

En una realización de la invención, el procedimiento tiene dos fases, estableciéndose en una primera fase un canal seguro entre el dispositivo de lectura y el transpondedor, y efectuándose en una segunda fase la medición del periodo de tiempo y la evaluación del periodo de tiempo por medio de las etapas de procedimiento descritas anteriormente. Mediante el establecimiento de un canal seguro, el comando de dispositivo de lectura y la respuesta de transpondedor pueden ser transmitidas muy rápido y se evitan desviaciones debidas a autentificaciones que deban anteponerse. De este modo, el procedimiento se hace más seguro en relación con el reconocimiento de ataques de transmisión.

En una realización preferida del procedimiento, rutinas de software (también conocidas como “Applets”) se configuran en el transpondedor para procesar el comando de manera que el tiempo de procesamiento del comando de la misma longitud de datos es siempre constante. De este modo se garantiza que el periodo de tiempo específico de tarjeta es constante.

Adicionalmente, el transpondedor puede realizar una o varias mediciones durante el procesamiento del comando recibido desde el dispositivo de lectura y/o monitorizar uno o varios sensores para determinar si el tiempo de ejecución actual del procesamiento se desvía del periodo de tiempo específico de tarjeta. Para ello puede efectuarse por ejemplo una evaluación por temporizadores, registradores o sensores en el reloj interno, un reloj externo o voltaje, teniendo lugar consecuentemente una comparación de valores objetivo.

Adicionalmente, puede estar previsto que el o los valores se transmitan en la respuesta al dispositivo de lectura adicionalmente al periodo de tiempo específico de tarjeta. Alternativa o adicionalmente, el o los valores medidos pueden incorporarse en el periodo de tiempo específico de tarjeta.

El comando transmitido desde el dispositivo de lectura al transpondedor puede ser un comando APDU, con el que el periodo de tiempo específico de tarjeta es solicitado de forma específica por el dispositivo de lectura. Dicho comando representa entonces un comando de verificación de ataque de transmisión especial. Puede aplicarse de forma flexible a diferentes transpondedores y está estandarizado.

Alternativamente, el comando transmitido desde el dispositivo de lectura al transpondedor puede ser un APDU arbitrario. La utilización de un comando arbitrario hace posible enmascarar una verificación de transmisión. En esta variante, es ventajoso que el dispositivo de lectura y el transpondedor acuerden de antemano en reacción a qué comando APDU el periodo de tiempo específico de tarjeta es transmitido en la respuesta al dispositivo de lectura.

El periodo de tiempo específico de tarjeta puede ser medido o calculado por el transpondedor. Esta medición o cálculo puede llevarse a cabo de una sola vez. El resultado de la medición o el cálculo puede estar guardado entonces en una memoria del transpondedor. Se entiende que la medición o el cálculo del periodo de tiempo específico de tarjeta debe efectuarse de forma segura para poder evitar en el futuro un ataque de transmisión de forma fiable.

Alternativamente, el periodo de tiempo específico de tarjeta puede ser conocido y estar guardado en una memoria del transpondedor. El periodo de tiempo específico de tarjeta puede por ejemplo determinarse en el contexto de una personalización e integrarse de forma segura en el transpondedor. Además, el periodo de tiempo se puede determinar en una fase de prueba durante la fabricación del transpondedor y ser integrado en el módulo de memoria.

La invención sugiere adicionalmente un sistema de comunicaciones que comprende un transpondedor con al menos una antena, en particular en la forma de un soporte de datos portátil, así como un dispositivo de lectura con al menos una antena, en el que el dispositivo de lectura está configurado para intercambiar datos con el transpondedor de manera que sea posible un intercambio de datos entre el transpondedor y el dispositivo de lectura dentro de un alcance predeterminado. Para ello, el dispositivo de lectura está configurado para efectuar una medición y evaluación del tiempo

de transmisión de un comando desde el dispositivo de lectura al transpondedor y de recepción de una respuesta correspondiente del transpondedor. Para ello, el dispositivo de lectura está configurado adicionalmente para procesar un periodo de tiempo específico de tarjeta, especificando el periodo de tiempo específico de tarjeta cuánto tiempo utiliza el transpondedor en recibir y procesar un comando recibido desde el dispositivo de lectura así como en enviar una respuesta correspondiente.

El sistema de comunicaciones de acuerdo con la invención tiene las mismas ventajas que se han descrito anteriormente en relación con el procedimiento de acuerdo con la invención.

El sistema de comunicaciones puede ser configurado adicionalmente para llevar a cabo las etapas del procedimiento descritas anteriormente.

A continuación, se explicará con mayor detalle la invención, con referencia a un ejemplo de realización mostrado en los dibujos. Los dibujos muestran:

la figura 1 una representación esquemática de un sistema de comunicaciones de acuerdo con la invención, que comprende un transpondedor en la forma de un soporte de datos portátil así como un dispositivo de lectura, cada uno de los cuales comprende una antena,

la figura 2 un diagrama de flujo que ilustra el procedimiento básico para operar el sistema de comunicaciones de la figura 1,

la tabla 1 un extracto de periodos de tiempo promedios, periodos de tiempo específicos de tarjeta y desviaciones en función de la longitud de datos.

La figura 1 muestra una representación esquemática de un sistema de comunicaciones de acuerdo con la invención. El sistema de comunicaciones comprende un dispositivo de lectura -10- así como un transpondedor -12-, preferiblemente en la forma de un soporte de datos portátil con forma de tarjeta. Tal transpondedor puede estar presente por ejemplo como tarjeta inteligente (*"smartcard"*) sin contacto. Tanto el dispositivo de lectura -10- como el transpondedor -12- comprenden cada uno al menos una antena no representada en detalle. El dispositivo de lectura -10- y el transpondedor -12- están configurados preferiblemente de acuerdo con la norma ISO/IEC 14443. Cuando el transpondedor -12- y el dispositivo de lectura -10- están dispuestos dentro de un determinado alcance, puede efectuarse un intercambio de datos entre estos dos componentes. En el caso de la denominada comunicación de campo cercano (*"Near Field Communication"* - NFC) un alcance típico es de aproximadamente 10 cm.

Mediante el procedimiento descrito con mayor detalle a continuación, el dispositivo de lectura -10- y el transpondedor -12- hacen posible evaluar un comportamiento de tiempo de respuesta en el contexto de una comunicación y con ello llevar a cabo la conocida limitación de distancia. El procedimiento puede llevarse a cabo sin realizar cambios en el dispositivo de lectura -10- y/o en el transpondedor -12- y que conduzcan a una variación en la realización de acuerdo con la ISO/EIEC 14443.

En el contexto de este procedimiento, que está representado en su forma básica en la figura 2, se efectúa una medición y evaluación del tiempo de un comando -10- (en general: un mensaje) transmitido desde el dispositivo de lectura -10- al transpondedor -12- y de recepción de una respuesta -34- correspondiente del transpondedor -12- por el dispositivo de lectura -10-. Para la transmisión del comando -10- desde el dispositivo de lectura -10- al transpondedor -12- se requiere un tiempo T_s1, para la transmisión de la respuesta -34- desde el transpondedor -12- al dispositivo de lectura -10- se requiere un tiempo T_s2. Para la recepción del comando, su procesamiento y la emisión de la respuesta correspondiente en el transpondedor -12- (número de referencia -32-) se requiere un periodo de tiempo específico de tarjeta T_icc.

El periodo de tiempo específico de tarjeta T_icc por tanto indica el tiempo que puede utilizar el transpondedor -12- entre la recepción, el procesamiento y el envío del comando -30-. La determinación del periodo de tiempo específico de tarjeta T_icc representa una primera etapa S20 del procedimiento de acuerdo con la invención.

El periodo de tiempo específico de tarjeta T_icc puede integrarse con seguridad en el transpondedor -12-, por ejemplo en el contexto de una personalización del mismo. Asimismo, el periodo de tiempo específico de tarjeta T_icc puede determinarse por sí mismo de forma segura en el transpondedor -12-. La determinación puede efectuarse por ejemplo mediante una medición. La determinación del periodo de tiempo específico de tarjeta T_icc se efectúa preferiblemente solamente una vez de acuerdo con condicionantes de la norma. El periodo de tiempo específico de tarjeta T_icc se incorpora entonces por ejemplo en una memoria interna del transpondedor no representada en detalle.

El periodo de tiempo específico de tarjeta T_icc se transmite (etapa S22) de forma veraz, es decir sin ser alterado, al dispositivo de lectura -10- en la respuesta -34- del transpondedor -12-. Simultáneamente al envío del comando -30-, el dispositivo de lectura -10- mide un periodo de tiempo T_IFD entre el envío del comando -30- y la recepción de la respuesta -34- (etapa S24). El periodo de tiempo T_IFD en este caso se compone de la suma de T_s1, T_s2 y T_icc. Mediante el cálculo de la diferencia entre el periodo de tiempo T_IFD y el periodo de tiempo específico de tarjeta T_icc, el dispositivo de lectura -10- o la aplicación software contenida en el mismo, la cual procesa los datos de la respuesta -34-, puede deducir si el transpondedor -12- se comunica directamente con el dispositivo de lectura -10- o si se está presentando un ataque de transmisión.

Para ello, se efectúa una comparación de la diferencia con un valor límite SW predeterminado (etapa S26). Si la diferencia es mayor que el valor límite SW ("sí"), entonces la comunicación con el transpondedor -12- sin contacto es interrumpida por el dispositivo de lectura -10-. En este caso, está teniendo lugar un ataque de transmisión (etapa S28). Si la diferencia es menor que el valor límite SW ("no"), la comunicación con el transpondedor -12- sin contacto es mantenida por el dispositivo de lectura -10-, puesto que no está teniendo lugar ningún ataque de transmisión (etapa S30).

Para la transmisión veraz del periodo de tiempo específico de tarjeta T_icc se elige preferiblemente una transmisión segura. Para ello puede utilizarse por ejemplo el denominado canal de mensajería seguro del transpondedor. En el caso de que la transmisión segura esté asegurada por la transmisión (*"rely-secure"*), el transpondedor solo necesita transmitir de forma segura el periodo de tiempo específico de tarjeta T_icc en su respuesta al dispositivo de lectura -10-.

Para solicitar el periodo de tiempo específico de tarjeta en el transpondedor -12-, puede transmitirse un comando especial de verificación de ataque de transmisión como comando -30- por el dispositivo de lectura -10- al transpondedor -12-. Alternativamente, puede utilizarse un comando APDU convencional en el contexto de una solicitud clásica o normalizada al transpondedor para enmascarar la verificación de transmisión. En este último caso, puede utilizarse para ello una selección aleatoria de cualquier comando APDU arbitrario.

El comando APDU arbitrario es acordado por ejemplo tanto por el transpondedor -12- como por el dispositivo de lectura -10- en las etapas anteriores, de manera que el transpondedor -12- reconoce el comando de verificación de transmisión y transmite el periodo de tiempo específico de tarjeta T_icc en su respuesta -34- al dispositivo de lectura -10-. Alternativamente, el comando APDU arbitrario no es acordado de antemano, sino que las estructuras de datos transferidas en el comando APDU o en la respuesta APDU indican que en el comando APDU el periodo de tiempo T_icc es requerido o bien transferido. Para ello, se utiliza por ejemplo un valor de longitud tipo (*"Type Length Value"*) especial, abreviadamente un objeto TLV.

Opcionalmente, mediante el comando -30- puede ser transmitida una prueba al transpondedor -12- que por ejemplo es transmitida de vuelta en la respuesta -34- junto con el periodo de tiempo específico de tarjeta T_icc al dispositivo de lectura -10-. Asimismo, la prueba puede provocar un comportamiento de tiempo definido y alterado del comando -30-.

Una variante adicional del procedimiento consiste en que, durante el procesamiento del comando -30-, el transpondedor -12- efectúa una o varias mediciones y/o monitoriza uno o varios sensores del transpondedor para determinar si el tiempo de ejecución se desvía significativamente del tiempo normalizado, es decir del periodo de tiempo específico de tarjeta. Esto puede efectuarse por ejemplo mediante la evaluación de temporizadores/registradores/sensores en el reloj interno, ciclo externo, voltaje, etc., y su comparación con respectivos valores objetivo. Opcionalmente, el o los valores medidos pueden ser tenidos en cuenta en el cálculo del periodo de tiempo específico de tarjeta T_icc y/o ser devueltos en la respuesta -34- al dispositivo de lectura -10- adicionalmente al periodo de tiempo específico de tarjeta.

En una segunda realización (no representada en las figuras), el procedimiento de las figuras 1 y 2 se repite varias veces. Un número de repeticiones razonable es mil, para poder filtrar errores extraordinarios e influencias ambientales que introducen desviaciones en la medición de tiempo. De este modo, el procedimiento se divide en dos fases, estableciéndose un canal seguro en la primera fase. Al establecer el canal seguro, las respuestas del transpondedor -12- pueden efectuarse muy rápido. En particular, el tiempo T' medido puede predecirse muy bien. Para establecer el canal, se pueden aplicar procedimientos normalizados tales como mensajería segura (*"Secure Messaging"*) o autentificaciones de Diffie-Hellman. El establecimiento del canal seguro puede omitirse cuando se garantice que el procedimiento no sea manipulado por un tercero.

En la segunda fase del procedimiento la medición de tiempo real T' se efectúa para reconocer el ataque de transmisión de acuerdo con los procedimientos descritos en las figuras 1 y 2. De este modo, las mediciones se repiten varias veces y el conjunto de las mediciones resulta en la segunda fase. Se aplica lo siguiente: Si el periodo de tiempo promedio T puede ser predicho con una cierta desviación estándar σ, entonces se cumple, con una probabilidad $p(\varepsilon)$, que el periodo de tiempo medido actualmente T' es:

$$T' = T_0 + \varepsilon$$

siendo el periodo de tiempo ideal T_0 la suma de T_icc, T_s1 y T_s2. Para ello, T_0 o bien se determina por medio de la combinación actual de transpondedor - dispositivo de lectura bajo condiciones de ensayo o bien está contenido en el dispositivo de lectura -20- como un valor de referencia típico.

El dispositivo de lectura -10- captura el periodo de tiempo actual T' en cada repetición. Cuando el periodo de tiempo ideal T_0 se utiliza como valor de referencia, se verifica si cada periodo de tiempo actual T' se desvía del periodo de tiempo ideal T_0 en una desviación ε, por ejemplo un 10%. En caso contrario, se asume que hay un ataque de transmisión y la comunicación se interrumpe. En una realización alternativa, no es el periodo de tiempo ideal T_0 el que se usa como referencia, sino el periodo de tiempo mínimo T. Cuando el periodo de tiempo mínimo T es un 10% menor que el periodo de tiempo medido realmente T', entonces el procedimiento es igualmente interrumpido y se asume que hay un ataque de transmisión. El periodo de tiempo mínimo T es reemplazado por el periodo de tiempo medido actualmente T' y es adoptado como el nuevo periodo de tiempo mínimo T, si el periodo de tiempo medido actualmente T' es menor que el periodo de tiempo mínimo T utilizado hasta el momento.

En vez del periodo de tiempo mínimo T también puede determinarse un valor promedio T, por ejemplo un promedio, de entre todos los periodos de tiempo T' capturados hasta el momento y este valor promedio T puede adoptarse como referencia. Este valor promedio puede ser aplicado después de completar todas las repeticiones del procedimiento.

De todo lo anterior se desprende que todas las actuaciones adicionales del atacante de transmisión deben ser efectuadas dentro de la desviación ε, en particular grandes distancias espaciales y equipos adicionales para retransmitir la señal implican una superación de la desviación ε. Debido a las fuertes restricciones temporales se hace imposible un ataque de transmisión en el sistema de comunicaciones.

En la tabla 1 se especifica el resultado de una serie de ensayos. Para ello, un dispositivo portátil (*"notebook"*) que tiene un sistema operativo y un lector de tarjeta -10- conectado al mismo, así como una tarjeta sin contacto como transpondedor -12-, fue analizado con relación a los periodos de tiempo T, T' y ε. De este modo, se variaron las longitudes de datos L de los comandos -30-. El periodo de tiempo específico de tarjeta T_icc fue tomado como constante en esta serie de ensayos. El comando -30- de la respectiva longitud de datos L fue enviado respectivamente 1000 veces y respondido por el transpondedor -12-.

Una implementación del procedimiento en un sistema de comunicaciones prevé que el dispositivo de lectura -10- envíe comandos -30- a la tarjeta hasta que la desviación ε esté dentro de un rango definido. Cuando esto se produce, puede intercambiarse información confidencial ya que se garantiza que la vía de comunicación no está redireccionada y/o intervenida.

De este modo, un ataque de transmisión puede considerarse como reconocido cuando un número de repeticiones predefinido del procedimiento de acuerdo con la invención se mantienen infructuosas. Cuanto mayor sea el número de repeticiones tanto menor puede ser el rango definido de la desviación ε. El rango definido de la desviación ε en los periodos de tiempo representados de acuerdo con la tabla 1 es de 0,1 milisegundos, por ejemplo, donde la distancia entre el dispositivo de lectura y el transpondedor puede limitarse a de 1 km a 10 km.

El procedimiento puede ser mejorado significativamente si se utilizan pequeños sistemas operativos en tiempo real.

En una realización alternativa del procedimiento (tampoco representada en las figuras), un comando es enviado al transpondedor -12-, siendo procesado por el transpondedor. El comando, también denominado como comando de inicio, precisa al transpondedor -12- a iniciar el procesamiento de una cadena de caracteres sinfín. Simultáneamente al comando de inicio, el dispositivo de lectura -20- inicia igualmente el procesamiento de la cadena de caracteres sinfín en el dispositivo de lectura -20-. En un momento arbitrario posterior al inicio de la cadena de caracteres sinfín, el dispositivo de lectura -20- interrumpe la cadena de caracteres sinfín. Simultáneamente a la interrupción de la cadena de caracteres sinfín, el dispositivo de lectura -20- envía un segundo comando al transpondedor -12-, también denominado como comando de interrupción. Después de recibir el comando de interrupción, el transpondedor interrumpe igualmente el procesamiento de la cadena de caracteres sinfín y envía una respuesta al dispositivo de lectura con el valor actual calculado como el último valor en la cadena de caracteres sinfín o un parámetro equiparable que especifique el cronológicamente último estado de procesamiento de la cadena de caracteres. Este parámetro es evaluado en el dispositivo de lectura y comparado con un parámetro de comparación en el dispositivo de lectura -20-. En el caso de que el parámetro/valor se encuentre dentro de ciertos límites se garantiza que no está teniendo lugar un ataque de

transmisión. La cadena de caracteres sinfín es una adición constante de un número aleatorio a sí mismo, por ejemplo. Alternativamente, pueden concebirse cadenas de caracteres sinfín complejas cuya interrupción proporcione un resultado en el momento de la interrupción.

Para detectar un ataque de transmisión, el procedimiento de acuerdo con la invención utiliza por tanto el tiempo de propagación neto de una señal enviada y recibida de nuevo por el dispositivo de lectura -10- menos un tiempo de cálculo conocido del transpondedor.

El procedimiento sugerido puede ser implementado de una manera muy simple. Permite que dispositivos de lectura reconozcan de forma fiable y con gran exactitud ataques de transmisión mediante terminales con capacidad NFC. Para ello, no se requieren modificaciones en la ISO/IEC 14443. El hecho de que el dispositivo de lectura sin contacto deba ser capaz de efectuar una medición de tiempo es solamente un condicionante.

Lista de números de referencia

10	Dispositivo de lectura
12	Transpondedor
30	Comando
32	Recepción, procesamiento y envío de una respuesta
34	Respuesta
S20	Etapa de procedimiento
S22	Etapa de procedimiento
S24	Etapa de procedimiento
S26	Etapa de procedimiento
S28	Etapa de procedimiento
S30	Etapa de procedimiento
T_icc	Periodo de tiempo específico de tarjeta
T_s1	Tiempo para el procesamiento y transmisión del mensaje -30-
T_s2	Tiempo para la transmisión y evaluación de la respuesta -34-
T’	Periodo de tiempo medido actualmente
T	Periodo de tiempo promedio y/o mínimo
T_0	Periodo de tiempo ideal
ε	Diferencia temporal entre T’ y T_0
L	Longitud de datos del comando

REIVINDICACIONES

1. Procedimiento para operar un sistema de comunicaciones que comprende un transpondedor (12), con al menos una antena, en particular en la forma de un soporte de datos portátil, así como un dispositivo de lectura (10), con al menos una antena, en el que el dispositivo de lectura (10) está configurado para intercambiar datos con el transpondedor (12), en el que un intercambio de datos entre el transpondedor (12) y el dispositivo de lectura (10) es posible dentro de un radio de alcance predeterminado, comprendiendo las siguientes etapas de procedimiento:

- enviar un comando (30) desde el dispositivo de lectura (10) al transpondedor (12);
- procesar el comando (30) en el transpondedor (12), generando una respuesta (34) al comando (30) por el transpondedor (12);
- recibir la respuesta (34) del transpondedor (12) en el dispositivo de lectura (10);
- medir el periodo de tiempo (T') entre la etapa de enviar y la etapa de recibir en el dispositivo de lectura (10), en el que la etapa de procesar se efectúa en un periodo de tiempo específico de tarjeta (T_icc) y el periodo de tiempo específico de tarjeta (T_icc) especifica cuánto tiempo utiliza el transpondedor (12) en recibir y procesar un comando (30) recibido desde el dispositivo de lectura (10) así como en enviar una respuesta correspondiente (34);

caracterizado por que:

el periodo de tiempo específico de tarjeta (T_icc) es transmitido en la respuesta (34) del transpondedor (12) al dispositivo de lectura (10) y

- el periodo de tiempo medido (T') es evaluado en el dispositivo de lectura (10), en el que para evaluar el tiempo medido (T') se utiliza el periodo de tiempo específico de tarjeta (T_icc).

2. Procedimiento según la reivindicación 1, en el que un ataque de transmisión puede inferirse por medio de la diferencia (ε) entre el periodo de tiempo medido (T') y el periodo de tiempo específico de tarjeta (T_icc).

3. Procedimiento según la reivindicación 1 ó 2, en el que el periodo de tiempo específico de tarjeta (T_icc) es transmitido de forma segura desde el transpondedor (12) al dispositivo de lectura (10).

4. Procedimiento según una de las reivindicaciones anteriores, en el que el comando (30) es una prueba y el periodo de tiempo específico de tarjeta (T_icc) es transmitido al dispositivo de lectura (10) junto con la respuesta como contestación (20).

5. Procedimiento según la reivindicación 4, en el que la prueba resulta en una modificación del periodo de tiempo determinado por el dispositivo de lectura (10).

6. Procedimiento según una de las reivindicaciones anteriores, en el que el procedimiento es realizado varias veces y el periodo de tiempo actualmente medido (T') es comparado con un periodo de tiempo predeterminado (T), en particular un periodo de tiempo mínimo, como valor límite.

7. Procedimiento según una de las reivindicaciones anteriores, en el que el periodo de tiempo medido (T') depende de la longitud de datos (L) del comando (30), y el periodo de tiempo predeterminado (T) para la longitud del comando (30), en particular un periodo de tiempo mínimo (T), es guardado en el dispositivo de lectura (10) como un valor de referencia.

8. Procedimiento según una de las reivindicaciones anteriores, en el que el transpondedor (12) efectúa una o varias mediciones durante el procesamiento del comando (30) recibido desde el dispositivo de lectura (10) y/o monitoriza uno o varios sensores del transpondedor (12) para determinar si el tiempo de ejecución del procesamiento se desvía del periodo de tiempo específico de tarjeta (T_icc).

9. Procedimiento según la reivindicación 8, en el que el o los valores medidos se transmiten al dispositivo de lectura (10) en la respuesta (34) adicionalmente al periodo de tiempo específico de tarjeta (T_icc).

10. Procedimiento según la reivindicación 8 ó 9, en el que el o los valores medidos se incorporan en el periodo de tiempo específico de tarjeta (T_icc).

11. Procedimiento según una de las reivindicaciones 1 a 10, en el que el transpondedor (12) mide o calcula el periodo de tiempo específico de tarjeta (T_icc).

12. Procedimiento según una de las reivindicaciones 1 a 10, en el que el periodo de tiempo específico de tarjeta (T_icc) es conocido y guardado en una memoria del transpondedor (12).

13. Sistema de comunicaciones que comprende un transpondedor (12) con al menos una antena, en particular en la forma de un soporte de datos portátil, así como un dispositivo de lectura (10), con al menos una antena, en el que el dispositivo de lectura (10) está configurado para intercambiar datos con el transpondedor (12) de manera que un intercambio de datos entre el transpondedor (12) y el dispositivo de lectura (10) es posible dentro de un radio de alcance predeterminado, en el que el dispositivo de lectura (10) está configurado para

- efectuar una medición y evaluación del tiempo de un comando (30) transmitido desde el dispositivo de lectura (10) al transpondedor (12) y el envío de una respuesta correspondiente (34) del transpondedor (12), **caracterizado por que** el periodo de tiempo específico de tarjeta (T_icc) es transmitido en la respuesta (34) del transpondedor (12) al dispositivo de lectura (10) para ser evaluado

- y el periodo de tiempo específico de tarjeta (T_icc) es procesado especificando el periodo de tiempo específico de tarjeta (T_icc) cuánto tiempo utiliza el transpondedor (12) en recibir y procesar un comando (30) recibido desde el dispositivo de lectura (10) así como en enviar una respuesta correspondiente (34).

14. Sistema de comunicaciones según la reivindicación 13, que está configurado adicionalmente para ejecutar las etapas del procedimiento según una de las reivindicaciones 2 a 12.

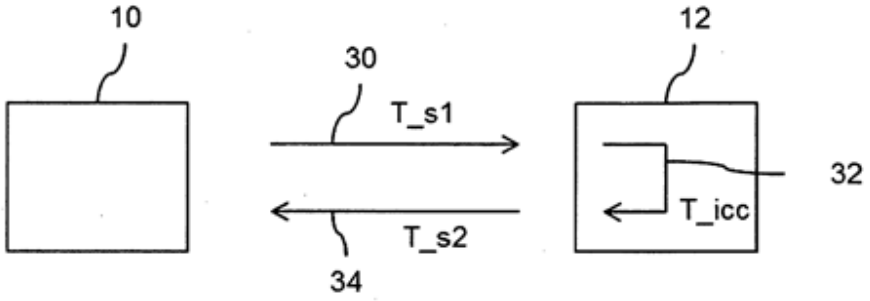
10
12
30
T_s1
32
T_icc
T_s2
34

Fig. 1

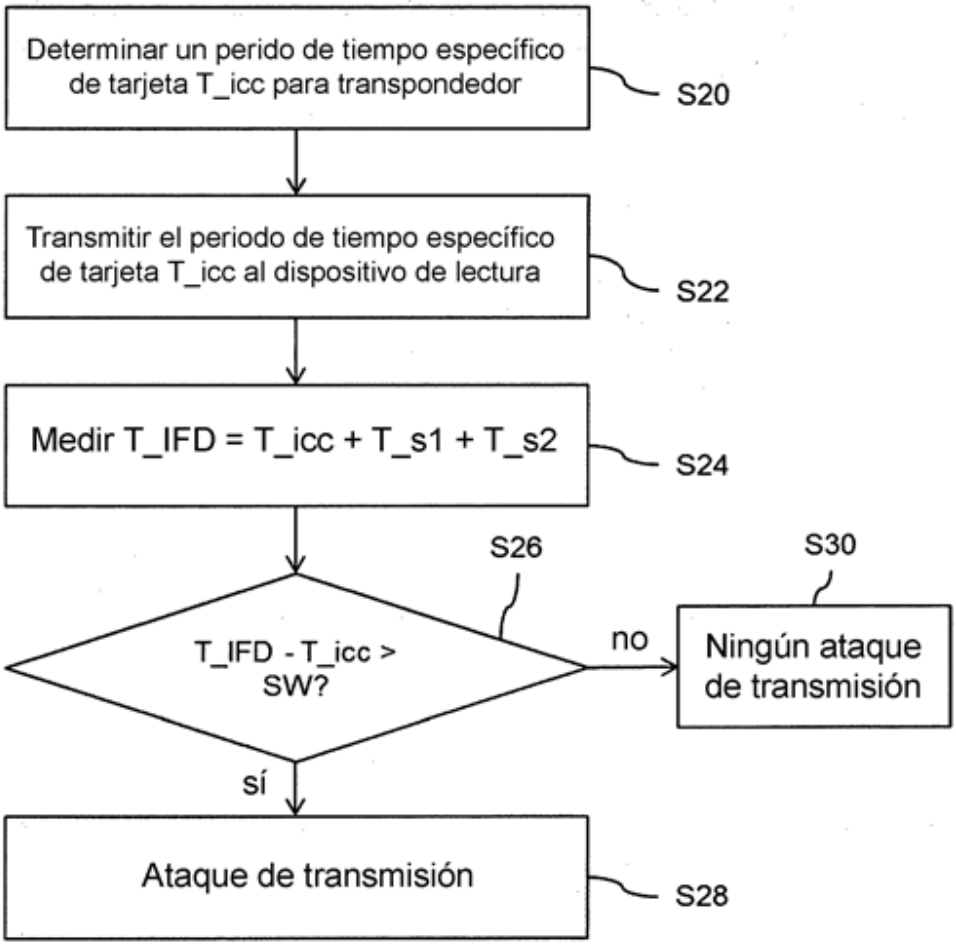
Determinar un perido de tiempo específico de tarjeta T_icc para transpondedor
S20
Transmitir el periodo de tiempo específico de tarjeta T_icc al dispositivo de lectura
S22
Medir T_IFD = T_icc + T_s1 + T_s2
S24
S26
S30
T_IFD - T_icc > SW?
no
Ningún ataque de transmisión
sí
Ataque de transmisión
S28

Fig. 2

Longitud de datos	T [s]	Desviación ε [s]	T_0 [s]
8 Bytes	0,008588	0,000269	0,008276
20 Bytes	0,011449	0,000448	0,011080
64 Bytes	0,02126	0,000422	0,020917
220 Bytes	0,058041	0,000615	0,057600

Tab. 1