(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 615 750**

(51) Int. CI.:

H04W 4/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.08.2012 PCT/KR2012/006518**

(87) Fecha y número de publicación internacional: **21.02.2013 WO2013025060**

(96) Fecha de presentación y número de la solicitud europea: **16.08.2012 E 12824527 (1)**

(97) Fecha y número de publicación de la concesión europea: **11.01.2017 EP 2747335**

(54) Título: **Dispositivo y método para autenticación de seguridad entre dispositivos basados en PUF en comunicación máquina a máquina**

(30) Prioridad:

16.08.2011 KR 20110081296

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.06.2017

(73) Titular/es:

ICTK CO., LTD. (100.0%)
2, 3rd Floor Jawon Building 912-31 Daechi-dong Gangnam-gu
Seoul 135-280, KR

(72) Inventor/es:

KIM, DONG KYUE;
CHOI, BYONG DEOK;
KIM, DONG HYUN;
PARK, SANG SEON;
JEE, KWANG HYUN y
JIN, BONG JAE

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Dispositivo y método para autenticación de seguridad entre dispositivos basados en PUF en comunicación máquina a máquina

Campo de la invención

La siguiente descripción de una o más realizaciones se relaciona con el campo de tecnología de comunicación máquina a máquina (M2M) y, más particularmente, con un método para realizar la autenticación segura entre dispositivos para la comunicación M2M.

Descripción de la técnica relacionada

La comunicación máquina a máquina (M2M) es una tecnología en la que un sistema u ordenador incorporado se equipa con un sensor capaz de recolectar información y un dispositivo capaz de transferir información y por lo tanto de forma autónoma puede recolectar y procesar información y tomar una decisión y tomar el control de sí mismo.

Dependiendo de la necesidad, la información procesada sólo necesita ser reportada a un administrador o a un usuario y, por lo tanto, se puede reducir la participación de los humanos. De acuerdo con lo anterior, la comunicación M2M puede ser útil para el trabajo ya que puede ser peligroso para un humano manejar, trabajar tomando una gran cantidad de tiempo, o campos en los que una máquina en lugar de un humano puede ser más adecuada, debido a problemas de seguridad.

Aunque se ha automatizado progresivamente el sistema de recolección de información con el desarrollo de un sensor, una función de procesar la información recolectada o tomar una decisión directa con base en la información recolectada ha dependido del hombre durante un largo período de tiempo.

Sin embargo, con el avance de un sistema social y de tecnología, ha sido necesaria la toma de decisiones sin tener en cuenta la hora o el lugar y se ha aumentado la cantidad de información que se va a procesar. Adicionalmente, la información se ha actualizado de forma continua y por lo tanto, se han aumentado las restricciones para que un humano procese la información y tome una decisión.

En esta situación, se ha concebido una idea de comunicación M2M para utilizar más útil y eficientemente datos de inundación. Las solicitudes iniciales de comunicación M2M en el año 1990 se han limitado a un simple control a distancia, un servicio de comunicación inalámbrica para vehículos, y similares. También se ha limitado al mercado o la industria.

Recientemente, se ha desarrollado rápidamente la tecnología de comunicación por cable e inalámbrica y se ha expandido significativamente un sistema de Internet. En particular, debido a la introducción de tecnología de comunicación nueva y económica, tales como identificación por radio frecuencia (RFID), comunicación de campo cercano (NFC), ZigBee, y Bluetooth, se ha reducido el costo de un sistema o aparato para comunicación M2M.

También, en una circunstancia en la que los servicios de telefonía móvil que han sido el centro del mercado de la comunicación, están alcanzando los límites en términos de crecimiento del mercado debido a la saturación de los abonados, se ha identificado la industria de la comunicación M2M como el nuevo mercado en el futuro.

Mientras tanto, un entorno de red seguro puede ser necesario para el crecimiento estable de la industria de la comunicación M2M. De acuerdo con lo anterior, se necesita un procedimiento de autenticación para verificar mutuamente la identidad entre los dispositivos antes de establecer una ruta de comunicación. Sin embargo, puede ser difícil aplicar un método de autenticación de seguridad convencional para la comunicación M2M como está. De acuerdo con lo anterior, subsiste la necesidad de un dispositivo de autenticación de seguridad y el método adecuado para la comunicación M2M.

Cuando el procesamiento de información o la toma de decisiones se realizan entre dispositivos en un entorno en el que está ausente la participación humana, una amenaza de seguridad con malas intenciones se puede convertir en un obstáculo en la tecnología de las comunicaciones M2M.

Se puede utilizar una autenticación de dos factores para autenticación de seguridad general. La autenticación de dos factores puede realizar tanto la autenticación con base en el conocimiento como la autenticación con base en la posesión. Es decir, la autenticación de dos factores puede mejorar la seguridad al realizar autenticación utilizando dos esquemas diferentes.

La autenticación con base en el conocimiento puede incluir un sistema de autenticación basado en una contraseña o un número de identificación personal (PIN), y la autenticación con base en posesión puede incluir una autenticación con base en posesión de un objeto tangible o intangible capaz de identificar un usuario, tal como una tarjeta de identificación.

Por ejemplo, en el caso del registro en un sitio web, la autenticación con base en conocimiento puede realizar sólo la autenticación de la contraseña. Sin embargo, en el caso de realizar transacciones financieras, puede ser necesario realizar la autenticación con base en conocimiento utilizando una contraseña, así como la autenticación con base en posesión utilizando un certificado oficial, una tarjeta de seguridad o una contraseña de un único uso (OTP).

Como se describió anteriormente, dependiendo de las circunstancias, se puede omitir la autenticación con base en posesión. Con este fin, en muchos casos, se puede realizar necesariamente la autenticación con base en conocimiento.

Para lograr una alta seguridad, una comunicación M2M puede requerir la autenticación de dos factores. En dicha comunicación, un dispositivo, no un humano, puede necesitar realizar de forma autónoma la autenticación con base en conocimiento.

Para llevar a cabo de forma autónoma la autenticación con base en conocimiento, el dispositivo puede necesitar ser capaz de generar una contraseña. En la técnica relacionada, fue difícil para el dispositivo generar una contraseña de forma autónoma.

Adicionalmente, muchos dispositivos de comunicación M2M pueden ser pequeños y portátiles, y pueden estar expuestos a un entorno externo. Por lo tanto, un dispositivo puede ser exigido físicamente.

De acuerdo con lo anterior, subsiste la necesidad de un método de autenticación de seguridad que permita que un dispositivo de comunicación M2M realice de forma autónoma la autenticación con base en conocimiento y también puede ser seguro contra un ataque a la seguridad externa, tal como un ataque de prueba de bus, y un ataque de exploración de memoria y un ataque al análisis de diseño.

Guajardo J. et al., “Key Distribution for Wireless Sensor Networks and Physical Unclonable Functions" se relaciona con el despliegue de claves seguras utilizando un tercero de confianza. El tercero de confianza realiza un procedimiento de inscripción, que tiene una respuesta de función física no clonable como entrada y produce datos clave y auxiliares como salida. Los datos clave y auxiliares para un nodo luego se envían a un usuario a través de un canal seguro y autenticado.

Guajardo, J. et al., "Physical Unclonable Functions and Public-Key Crypto for FPGA IP Protection" (International Conference on Field Programmable Logia and Applications, August 2007, pp. 189-195) se relaciona con el uso de la funciones físicas no clonables para proteger la propiedad intelectual en FPGAs.

Resumen

De acuerdo con la invención, se proporciona: un dispositivo terminal de acuerdo con la reivindicación 1; un dispositivo de autoridad de certificación de acuerdo con la reivindicación 9; y métodos de acuerdo con reivindicaciones 10 y 13.

Un aspecto de una o más realizaciones proporciona un aparato y método que permite que un dispositivo genere de forma autónoma una contraseña y utilice la contraseña generada para autenticación a través de nueva tecnología denominada una función no clonable física (PUF) en un campo de comunicación máquina a máquina (M2M), por lo cual se realiza autenticación de seguridad confiable para identificar dispositivos mutualmente y verificar si los dispositivos son entidades válidas.

Otro aspecto de una o más realizaciones también proporciona un dispositivo de autenticación de seguridad y método que es robusto contra un ataque físico o un acceso no autorizado a un sistema de autenticación de seguridad de un dispositivo cuando se aplica comunicación segura utilizando cifrado y descifrado a los sistemas o al dispositivo que realiza comunicación M2M.

De acuerdo con un aspecto de una o más realizaciones, se proporciona un dispositivo terminal que realiza comunicación máquina a máquina (M2M), el dispositivo terminal incluye: una función no clonable física (PUF) incorporada en el dispositivo terminal para generar una clave de autenticación para autenticación de contraseña asociada con el dispositivo terminal; y una unidad de autenticación para realizar la autenticación de contraseña asociada con el dispositivo terminal utilizando la clave de autenticación generada por la PUF.

La PUF se puede aislar físicamente desde un entorno externo para prevenir que la clave de autenticación se exponga al exterior.

De acuerdo con otro aspecto de una o más realizaciones, se proporciona un dispositivo terminal que realiza comunicación M2M, el dispositivo terminal incluye: un módulo de clave secreta para proporcionar una clave secreta para transferir, utilizando un esquema de cifrado de clave secreta, una clave pública utilizada para comunicación del dispositivo terminal utilizando un esquema de cifrado de clave pública; y un módulo de clave privada para proporcionar una clave privada para generar la clave pública. Por lo menos uno del módulo de clave secreta y el módulo de clave privada puede incluir un PUF.

El dispositivo terminal adicionalmente puede incluir una unidad de fusible bloqueada en respuesta a la aplicación de sobrecorriente para bloquear una ruta a través de la cual se extrae la clave secreta.

La unidad de fusible puede bloquear la ruta después de que se extrae inicialmente la clave secreta desde el dispositivo terminal.

El dispositivo terminal adicionalmente puede incluir: un almacenamiento de números de serie para almacenar un número de serie del dispositivo terminal; y una unidad de fusible para bloquear una ruta a través de la cual se extrae la clave secreta, después de que se almacena el número de serie en el almacenamiento de número de serie y se extrae la clave secreta.

El dispositivo terminal adicionalmente puede incluir un generador de clave pública para generar la clave pública utilizando la clave privada.

El dispositivo terminal puede almacenar una clave pública de un dispositivo externo utilizado para comunicación del dispositivo externo utilizando el esquema de cifrado de clave pública. Cuando un mensaje desde el dispositivo externo, el se recibe dispositivo terminal puede descifrar el mensaje utilizando la clave pública del dispositivo externo.

Cuando se descifra el mensaje, el dispositivo terminal puede verificar la validez del dispositivo externo dependiendo de si se conoce la identidad de un número de serie del dispositivo terminal.

De acuerdo con aún otro aspecto, se proporciona un dispositivo de CA para manejar un dispositivo terminal que realiza comunicación M2M, el dispositivo de CA incluye: una lista de números de identidad personal (PIN) para almacenar una clave secreta del dispositivo terminal y un número de serie del dispositivo terminal. Cuando un mensaje, en el que se cifran una clave pública utilizada para comunicación utilizando un esquema de cifrado de clave pública y el número de serie del dispositivo terminal utilizando la clave secreta, se transmite desde el dispositivo terminal, el dispositivo de CA descifra el mensaje utilizando la clave secreta. Cuando se descifra el mensaje, el dispositivo de CA puede verificar la validez del dispositivo externo dependiendo de si se conoce la identidad de un número de serie del dispositivo terminal.

De acuerdo con todavía otro aspecto de una o más realizaciones, se proporciona un método para realizar, mediante un dispositivo terminal, autenticación de seguridad con el fin de realizar comunicación M2M, el método incluye: generar, por el dispositivo terminal, una clave privada del dispositivo terminal utilizando una primera PUF incorporada en el dispositivo terminal; generar, por el dispositivo terminal, una clave pública para realizar autenticación de contraseña asociada con el dispositivo terminal utilizando la clave privada; y realizar la autenticación de contraseña con un terminal externo diferente del dispositivo terminal o una CA externa utilizando la clave pública.

El método de autenticación de seguridad adicionalmente puede incluir: generar una clave secreta para transferir la clave pública externamente utilizando un esquema de cifrado de clave secreta, utilizando una segunda PUF diferente de la primera PUF; e intercambiar la clave pública con la CA externa con base en un esquema de cifrado de clave secreta utilizando la clave secreta.

El método de autenticación de seguridad adicionalmente puede incluir: recibir, desde la CA externa, un mensaje cifrado utilizando un esquema de cifrado de clave pública; descifrar el mensaje cifrado utilizando una clave pública prealmacenada de la CA externa; y completar la autenticación de seguridad con la CA externa cuando un número de serie del dispositivo terminal se verifica desde el mensaje descifrado.

El método de autenticación de seguridad adicionalmente puede incluir bloquear un fusible presente en una ruta a través de la cual se extrae la clave secreta, después de que almacena un número de serie del dispositivo terminal en un almacenamiento de número de serie y se extrae inicialmente la clave secreta.

De acuerdo con un aspecto adicional de una o más realizaciones, se proporciona un método para retransmitir, mediante un dispositivo de CA, intercambio de clave pública para comunicación M2M entre un primer dispositivo terminal y un segundo dispositivo terminal, el método incluye: recibir, desde el segundo dispositivo terminal, una solicitud para una clave pública del primer dispositivo terminal; generar un primer mensaje cifrado al cifrar la clave pública del primer dispositivo terminal y un número de serie del segundo dispositivo terminal utilizando una clave privada del dispositivo de CA; y transmitir el primer mensaje cifrado al segundo dispositivo terminal.

El método de autenticación de seguridad adicionalmente puede incluir generar un segundo mensaje cifrado al cifrar una clave pública del segundo dispositivo terminal y un número de serie del primer dispositivo terminal utilizando la clave privada del dispositivo de CA; y transmitir el segundo mensaje cifrado al primer dispositivo terminal.

El segundo dispositivo terminal puede descifrar el primer mensaje cifrado utilizando una clave pública del dispositivo de CA que corresponde a la clave privada del dispositivo de CA, y puede confiar la clave pública transmitida del primer dispositivo terminal cuando el número de serie del segundo dispositivo terminal se verifica desde el primer mensaje descifrado cifrado.

El primer dispositivo terminal puede descifrar el segundo mensaje cifrado utilizando una clave pública del dispositivo de CA que corresponde a la clave privada del dispositivo de CA, y puede confiar la clave pública transmitida del segundo dispositivo terminal cuando el número de serie del primer dispositivo terminal se verifica desde el segundo mensaje descifrado cifrado.

Efecto de la invención

De acuerdo con las realizaciones, se puede realizar autenticación de seguridad segura entre dispositivos o entre un dispositivo y un sistema.

De acuerdo con lo anterior, se puede garantizar la fiabilidad de un proceso para identificar mutuamente entre los dispositivos que realizan la comunicación máquina a máquina (M2M) y verificar si los dispositivos son entidades válidas

También, se puede aplicar tecnologías convencionales utilizando cifrado y descifrado a sistemas o un dispositivo que realizan comunicación M2M.

Breve descripción de los dibujos

La figura 1 es un diagrama de bloques que ilustra un dispositivo de autenticación de seguridad de acuerdo con una realización;

La figura 2 es un diagrama de bloques que ilustra un dispositivo de autenticación de seguridad de acuerdo con otra realización;

La figura 3 es un diagrama para describir una estructura de ejemplo de una función no clonable física (PUF) utilizada para configurar un módulo de clave secreta o un módulo de clave privada de la figura 2 de acuerdo con una realización;

La figura 4 es un diagrama para describir un proceso para registrar un número de serie a un dispositivo de autenticación de seguridad, extraer un número de identidad personal (PIN), y registrar el PIN extraído en una lista de PIN de acuerdo con una realización;

La figura 5 es un diagrama para describir un proceso para distribuir dispositivos de autenticación de seguridad desde una fábrica y transferir y por lo tanto registrar una lista de PIN en una autoridad de certificación (CA) de acuerdo con una realización;

La figura 6 es un diagrama de flujo que ilustra un proceso para registrar claves públicas entre un dispositivo y una CA de acuerdo con una realización;

La figura 7 es un diagrama de flujo que ilustra un proceso para verificar la validez de un dispositivo de acuerdo con una realización; y

La figura 8 es un diagrama de flujo que ilustra un proceso para intercambiar claves públicas entre dispositivos a través de una CA con el fin de realizar autenticación de seguridad entre dispositivos que excluyen la CA, de acuerdo con una realización.

Descripción detallada

Ahora se hará referencia en detalle a realizaciones, cuyos ejemplos se ilustran en los dibujos acompañantes, en los que los números de referencia similares se refieren a elementos similares, como en todas partes. Las realizaciones de ejemplo descritas a continuación ilustran uno o más aspectos de la presente invención haciendo referencia a las figuras.

La figura 1 es un diagrama de bloques que ilustra un dispositivo 100 de autenticación de seguridad (en adelante también mencionado como un dispositivo 100) de acuerdo con una realización.

De acuerdo con una realización, al realizar comunicación máquina a máquina (M2M) entre dispositivos, el dispositivo 100 que realiza comunicación M2M puede generar de forma autónoma y mantener un número de identidad personal seguro (PIN) o una contraseña y de esta manera realizar autenticación con base en conocimiento .

Para la anterior autenticación con base en conocimiento, se puede incluir una función 110 no clonable física (PUF) que es robusta contra un ataque de seguridad externo y genera un PIN aleatorio y único en el dispositivo 100.

De acuerdo con una realización, la PUF 110 puede generar un PIN que se puede utilizar como una clave de autenticación para la autenticación con base en conocimiento. El PIN puede ser un valor digital aleatorio que se genera por la PUF 110 debido a la variación de proceso que ocurre durante un proceso de fabricación.

También, el PIN puede ser un valor digital que no varía en el tiempo que no varía en función del entorno que lo rodea, una vez se genera el valor. Cuando no se expone dicho PIN a un entorno externo, se puede utilizar para prevenir una amenaza a la seguridad con respecto a un sistema de autenticación del dispositivo 100.

Cuando el dispositivo 100 realiza comunicación M2M con otro dispositivo (no mostrado) a través de una interfaz 130 de comunicación, una unidad 120 de autenticación puede recibir el PIN que se genera de forma autónoma por la PUF 110, y puede realizar autenticación con base en conocimiento.

Una configuración de ejemplo del dispositivo 100 se describirá adicionalmente con referencia a la figura 2.

La figura 2 es un diagrama de bloques que ilustra un dispositivo de autenticación de seguridad 200 (en adelante también mencionado como dispositivo 200) de acuerdo con otra realización.

En la autenticación de seguridad de acuerdo con una realización, el dispositivo 200 puede incluir un módulo 220 de clave secreta y un módulo 250 de clave privada. Aquí, por lo menos uno del módulo 220 de clave secreta y el módulo 250 de clave privada puede incluir una PUF.

De acuerdo con una realización, cada uno del módulo 220 de clave secreta y el módulo 250 de clave privada puede incluir una única PUF. Cada PUF puede tener una clave secreta y una clave privada debido a sus propiedades físicas. En adelante, una clave secreta y/o una clave privada también se puede expresar como un PIN y, de esta manera, se puede entender que el PIN incluye la clave secreta, la clave privada, y similares, utilizada para autenticación de seguridad del dispositivo 200.

Una PUF puede ser un circuito que genera diferentes valores de la función utilizando variación de proceso, incluso si se fabrica con base en un diseño idéntico o equivalente. De acuerdo con algunas realizaciones, la PUF puede generar y proporcionar un PIN de un dispositivo de comunicación M2M. Específicamente, en lugar de ser un valor digital que se genera utilizando una propiedad física de la PUF, el PIN se puede generar utilizando el valor digital.

Por ejemplo, el PIN puede ser un valor obtenido como resultado de cifrar un valor digital original generado por la PUF con un valor germinal proporcionado desde una fuente externa confiable.

Durante el proceso anterior, de acuerdo con una realización, se puede emplear un método de entrada del valor germinal y un valor digital V_{PUF} proporcionado por la PUF en una función de información inservible. De acuerdo con lo anterior, el valor del PIN final puede ser Información inservible (Valor germinal de V_{PUF}||).

De acuerdo con una realización, cuando se expone o filtra una clave privada, un PIN se puede cambiar al simplemente cambiar un valor germinal, que mejora la seguridad y conveniencia.

Aquí, la generación de valor de PIN anterior es solo un ejemplo y de esta manera, las realizaciones pueden incluir cualquier caso en el que el valor digital generado por la PUF se utiliza como el PIN y cualquier caso en el que otro valor obtenido al procesar el valor digital se utiliza como el PIN. En adelante, incluso aunque no se puede describir en detalle un proceso para generar un nuevo PIN utilizando el valor digital generado por la PUF, se debe entender que una descripción relacionada con una generación del valor del PIN incluye dichas realizaciones.

Mientras tanto, la PUF puede tener un valor aleatorio impredecible que se puede utilizar para determinar un PIN del dispositivo 200. De acuerdo con lo anterior, se puede utilizar la PUF para evitar que el PIN se exponga al generar externamente, insertar, y almacenar el PIN en una memoria.

También, debido a que la PUF es físicamente imposible de duplicar, también puede ser posible reducir o eliminar la posibilidad de exposición o duplicación de un PIN del dispositivo 200.

También, un valor de PIN generado por la PUF puede tener aleatoriedad, y de acuerdo con las realizaciones, una vez se genera el valor de PIN, el valor de PIN puede ser invariante en tiempo y confiable. Una configuración de ejemplo de la PUF se describirá adicionalmente con referencia a la figura 3.

De acuerdo con una realización, se puede almacenar un único valor, por ejemplo, un número de serie del dispositivo 200 que se asigna desde una fábrica durante un proceso de fabricación del dispositivo 200 en un almacenamiento de número de serie 210. El único número de serie del dispositivo 200 se puede ingresar desde la fábrica hasta el dispositivo 200 a través de una interfaz 231 de entrada/salida (I/O). En este caso, se puede extraer una clave secreta una vez desde el módulo 220 de clave secreta a la fábrica o una fuente externa que tiene un derecho de manejo. La anterior extracción se puede designar para que se realice una vez por razones de seguridad, incluso si no se especifica en una política.

De acuerdo con una realización, el dispositivo 200 puede incluir una unidad 230 de fusible. Después de que inicialmente se extrae la clave secreta una vez, la unidad 230 de fusible puede bloquear físicamente una conexión entre el módulo 220 de clave secreta y la interfaz 231 I/O. el procedimiento de bloqueo puede ser irreversible.

De acuerdo con lo anterior, una entidad que tiene el derecho de manejo puede mantener de forma segura la clave secreta que inicialmente se extrae una vez, y la clave secreta del dispositivo 200 no se puede extraer después de bloqueo de la unidad 230 de fusible. El módulo 220 de clave secreta se configura por la PUF y de esta manera, puede ser imposible físicamente duplicarla. Puede ser difícil o incluso imposible extraer la clave secreta a través de un ataque de análisis de poder, una variedad de ingeniería inversa, y similares.

De acuerdo con una realización, el dispositivo 200 puede incluir el módulo 250 de clave privada para generar una clave privada utilizada para un esquema de comunicación de cifrado/descifrado de clave pública. El módulo 250 de clave privada puede proporcionar una clave privada utilizando una PUF diferente utilizada en el módulo 220 de clave secreta.

La clave privada que se genera y proporciona por el módulo 250 de clave privada se puede aislar físicamente desde un entorno externo, y no se puede extraer al exterior mientras que se fabrica, distribuye, o utiliza el dispositivo 200. Por la misma razón como se describió anteriormente con referencia al módulo 220 de clave secreta, puede ser imposible exponer la clave privada a través de un ataque físico.

Debido a que puede no ocurrir exposición de la clave privada proporcionada por el módulo 250 de clave privada, se puede realizar la autenticación del dispositivo a través de un PIN que se genera de forma autónoma por el dispositivo 200 en comunicación M2M.

De acuerdo con una realización, utilizando una clave privada generada por el módulo 250 de clave privada, un generador 240 de clave pública puede generar una clave pública que va a ser utilizada por el dispositivo 200 para el esquema de comunicación de cifrado/descifrado de la clave pública. La clave pública generada se puede almacenar en un almacenamiento 260 de clave pública. El almacenamiento 260 de clave pública, como un medio para almacenar la clave pública generada, puede ser una memoria volátil.

Opcionalmente se emplear el almacenamiento 260 de clave pública. De acuerdo con otra realización, en lugar de utilizar el almacenamiento 260 de clave pública, puede posible leer clave pública generada por el generador 240 de clave pública cada vez que se requiera autentificación.

Un procesador 270 de cifrado/descifrado se puede entender como un criptocoprocesador y similares que realiza cifrado y descifrado de datos generales. Una interfaz 280 de comunicación puede ser una configuración para transmitir y recibir sustancialmente datos hacia y desde el exterior en una red.

De acuerdo con una realización, se puede utilizar la clave secreta extraída una vez como un medio para verificar que el dispositivo 200 y una autoridad de certificación (CA) que es la entidad de manejo que tiene el derecho a realizar comunicación segura con el dispositivo 200, son entidades válidas, con el fin de intercambiar claves públicas entre el dispositivo 200 y la CA.

Es decir, se puede utilizar una clave secreta que se extrae una vez durante un proceso para transmitir la clave pública externamente utilizando un esquema de cifrado de clave secreta, en lugar de que se utilice directamente para cifrado y descripción de mensajes generales. Esto puede resultar en el aumento de la seguridad y, de acuerdo con lo anterior, una clave privada utilizada para la autenticación actual del dispositivo no se puede exponer al exterior.

En adelante, un proceso para fabricar el dispositivo 200 en la fábrica, un proceso para hacer circular y distribuir el dispositivo 200, un proceso para intercambiar claves públicas utilizando un esquema de comunicación de clave secreta en un uso actual del dispositivo 200, y un proceso en el que el dispositivo 200 verifica sustancialmente la validez con la CA u otros dispositivos y de esta manera realiza comunicación se describirá adicionalmente con referencia a la figura 3 en la figura 8.

La figura 3 es un diagrama que describe una estructura de ejemplo de una función no clonable física (PUF) que se puede utilizar para configurar un módulo de clave secreta o un módulo de clave privada de la figura 2 de acuerdo con una realización.

Para este fin, se describirá una diferencia entre la configuración de PUF de acuerdo con las realizaciones y configuración de PUF acuerdo con la técnica convencional y un ejemplo de la misma se describirá con referencia a la figura 3.

Una PUF puede proporcionar un valor digital aleatorio. A pesar de que se dé un proceso de fabricación exacto y se pueda fabricar una pluralidad de PUF a través del mismo proceso de fabricación, cada una de las PUF puede proporcionar un valor digital diferente.

De acuerdo con lo anterior, una PUF se puede denominar como una función de una sola vía física (POWF) que es imposible de duplicar, y también se puede mencionar como una función aleatoria física (PRF).

Se puede utilizar dicha PUF para generar una clave de cifrado para seguridad y/o autenticación. Por ejemplo, se puede utilizar la PUF para proporcionar una clave única para distinguir los dispositivos entre sí.

Para configurar dicha PUF de forma convencional, se puede configurar un recubrimiento de PUF utilizando partículas dopadas de forma aleatoria en una capa superior de un chip integrado (IC). Se puede configurar una PUF mariposa reciente configurable incluso en una matriz de puertas programables en campo (FPGA) utilizando la variación del proceso dentro de un dispositivo semiconductor de óxido metálico complementario (CMOS) utilizado en general para un chip de hardware, como un cerrojo.

Para aumentar la confiabilidad de una PUF de tal manera que se puede comercializar una aplicación que utiliza la PUF para la generación de PIN, puede ser necesario garantizar una característica de que un circuito PUF sea físicamente imposible de duplicar, la aleatoriedad de un valor PIN generado, y una característica de que el valor del PIN es invariante en el tiempo una vez que se genera el valor del PIN.

Sin embargo, muchos circuitos PUF convencionales no pueden, a un nivel alto, garantizar por lo menos una de las características de aleatoriedad y tiempo invariante que pueden ser necesarias para satisfacer una PUF o PRF, y de esta manera, puede tener dificultades en ser comercializado.

Una PUF como se describe en las realizaciones puede superar los problemas convencionales y puede garantizar el tiempo invariante y la aleatoriedad a un nivel confiable, y también se puede producir a bajo costes durante un proceso de fabricación de semiconductores.

De acuerdo con una realización, para satisfacer la aleatoriedad y tiempo invariante de un PIN generado por una PUF, se puede generar un valor aleatorio utilizando la aleatoriedad que se puede producir con base en los cortocircuitos entre los nodos presentes en un proceso de semiconductores.

De acuerdo con una realización de la figura 3, una PUF puede permitir que un cortocircuito sea determinado de forma aleatoria al configurar un tamaño de un contacto o una vía, que se puede utilizar para conectar eléctricamente las capas conductoras (de metal) dentro de un chip semiconductor, para que tenga un tamaño más pequeño que el tamaño proporcionado en una regla de diseño, es decir, lo suficientemente seguro para ser conectado durante el proceso. Es decir, se puede generar un valor del PIN aleatorio al violar la regla de diseño.

Debido a que se configura dicho nuevo circuito PUF como un simple corto circuito, no se requieren un circuito o proceso adicional ni un dispositivo de medición particular. De acuerdo con lo anterior, se puede configurar fácilmente el nuevo circuito PUF. Puesto que se utiliza un proceso característico, se puede satisfacer la estabilidad mientras se mantiene la aleatoriedad de un valor.

En lo sucesivo, la generación de PUF de acuerdo con una realización se describirá con referencia a la figura 3.

Con referencia a la figura 3, en un proceso de fabricación de semiconductores, las vías se pueden formar entre una capa 302 de metal 1 y una capa 301 de metal 2.

En un grupo de 310 en el que un tamaño de vía puede ser grande con base en una regla de diseño, todas las vías se pueden poner en cortocircuito con la capa 302 de metal 1 y la capa 301 de metal 2. Si las vías se ponen en cortocircuito la capa 302 de metal 1 y la capa 301 de metal 2 se pueden expresar como un valor digital "0".

Mientras tanto, en un grupo 330 en el que un tamaño de vía puede ser pequeño, no todas las vías se pueden poner en cortocircuito con la capa 302 de metal 1 y la capa 301 de metal 2. Si las vías se ponen en cortocircuito la capa 302 de metal 1 y la capa 301 de metal 2 se puede expresar como un valor digital "1".

En un grupo 320 en el que un tamaño de vía se puede establecer entre el tamaño de vía del grupo 310 y el tamaño de vía del grupo 330, una porción de vías puede poner en cortocircuito la capa 302 de metal 1 y la capa 301 de metal 2 y la otra parte de las vías puede no poner en cortocircuito la capa 302 del metal 1 y la capa 301 del metal 2.

De acuerdo con una realización, se puede configurar un generador 210 de clave de identidad al establecer que una porción de las vías ponen en cortocircuito la capa 302 de metal 1 y la capa 301 de metal 2 y al establecer la otra porción de las vías que no ponen en cortocircuito la capa 302 del metal 1 y la capa 301 de metal 2, como se muestra en el grupo 320.

Una regla de diseño sobre un tamaño de vía puede ser diferente dependiendo del proceso de fabricación de semiconductores. Por ejemplo, cuando se `puede establecer que una regla de diseño sea de 0.25 micras en un proceso CMOS de 0.18 micras (um), el generador 210 de clave de identidad puede permitir que se pongan en cortocircuito entre las capas de metal que se van a distribuir probabilísticamente al establecer que el tamaño de vía es 0.19 micras.

Idealmente, la distribución de probabilidad con respecto a si la vía pone en cortocircuitos las capas de metal se puede establecer a una probabilidad del 50%. El módulo 220 de clave secreta y el módulo 250 de clave privada de acuerdo con una realización se pueden configurar al establecer el tamaño de vía para tener la distribución de probabilidad tan cerca del 50%. El ajuste por encima del tamaño de vía se puede realizar a través de una prueba de acuerdo con un proceso de semiconductores específico.

A través de la realización anteriormente mencionada, la PUF puede proporcionar una clave secreta o una clave privada de tal manera que se puede garantizar la aleatoriedad y el tiempo invariante. De acuerdo con lo anterior, puede ser innecesaria la resistencia a la manipulación para hacer frente a un ataque físico.

La resistencia a la manipulación utilizada generalmente para un módulo de cifrado con el fin de hacer frente a un ataque físico, tal como un ataque de desempaque, un ataque al análisis de diseño, y un ataque de memoria, puede proteger el contenido interno al provocar que el dispositivo funcione de forma incorrecta a través de borrar el contenido de una memoria y similares, cuando se hace un intento de desmontar el dispositivo. Sin embargo, se puede necesitar un dispositivo de protección adicional o puede ser complejo un medio de configuración, que puede resultar en un aumento de los costes y daño del equipo debido a errores de usuario o un mal funcionamiento del dispositivo. Sin embargo, al configurar una PUF con base en el principio descrito anteriormente con referencia a la figura 3, no pueden ocurrir los problemas anteriores.

También, puede ser difícil de acuerdo con una realización separar y de este modo observar cada celda de PUF dentro de un chip. Por lo tanto, puede ser difícil seleccionar sólo las celdas de PUF dentro del chip, que puede incluir diez a cientos de miles de puertas, y observar sólo los valores de las celdas seleccionadas.

También, una porción de las PUF puede tener un valor válido solo al operar en un estado de encendido. Por lo tanto, cuando un chip se daña parcialmente durante un proceso de desempaque por un ataque físico y similar, las PUF pueden tener un valor diferente de un valor original y, de esta manera, puede ser difícil estimar un valor original.

De acuerdo con lo anterior, cuando se utiliza una PUF de acuerdo con una realización de la presente invención, es posible proporcionar una clave secreta y una clave privada que tiene una configuración robusta contra un ataque físico y mantener la aleatoriedad y tiempo invariante sin requerir coste adicional tal como resistencia a la manipulación.

La figura 4 es un diagrama que describe un proceso para registrar un número de serie de un dispositivo 401, extraer un PIN que puede ser una clave secreta, y registrar el PIN extraído en una lista 403 de PIN de acuerdo con una realización.

Durante un proceso para fabricar el dispositivo 401 en una fábrica 402, se puede realizar el registro del número de serie y extracción de un valor de PIN.

En operación 410, la fábrica 402 que puede producir el dispositivo 401 puede insertar, en el dispositivo 401, un número de serie (SN) que puede ser un ID único.

En operación 420, la fábrica 402 puede extraer un PIN que puede ser una clave secreta del dispositivo 401. En operación 430, la fábrica 402 puede emparejar el SN y el PIN, y puede almacenar el SN y PIN emparejado en la lista 403 de PIN. Como se describió anteriormente, el PIN que puede ser la clave secreta del dispositivo 401 puede ser un valor digital que se puede generar por una PUF que puede ser el módulo 220 de clave secreta de la figura 2. De acuerdo con otra realización, el PIN puede tener un valor que se puede generar al procesar el valor digital utilizando una función de información inservible y similares.

Cuando se almacena el contenido que corresponde al dispositivo 401 en la lista 403 de PIN, se puede bloquear una ruta a través de la cual el PIN se extrae de la clave secreta en operación 440. De acuerdo con una realización, durante dicho proceso, se puede desconectar un fusible al hacer fluir sobrecorriente en un circuito de extracción. De acuerdo con lo anterior, como se describió anteriormente, se puede extraer la clave secreta solo una vez una vez y se vuelve imposible acceder o exponer el PIN es decir la clave secreta.

En adelante, se describirán cada una los elementos utilizados para describir autenticación de seguridad en comunicación M2M.

Los dispositivos individuales, un servidor y una CA se pueden incluir en un modelo de red de la siguiente comunicación M2M.

Los dispositivos de comunicación M2M, tales como un terminal de una comunicación M2M, pueden recolectar información a través de un sensor, o pueden generar datos y transmitir los datos generados a un servidor. También, los dispositivos de comunicación M2M pueden transmitir y recibir datos hacia y desde un dispositivo vecino de la misma forma.

Un servidor de comunicaciones M2M puede recolectar y procesar los datos generados por los dispositivos en la red, y puede proporcionar los datos procesados a un usuario como la base de una plataforma de servicios de comunicaciones M2M. Se puede ejecutar una variedad de aplicaciones al emplear una interfaz de plataforma de aplicaciones abierta (API) desde una plataforma de servicios. Cada una de las aplicaciones, que puede funcionar para diferentes propósitos, puede transmitir y recibir datos hacia y desde un dispositivo, y puede procesar los datos como información útil, y proporcionar la información procesada a un usuario a través de un terminal tal como una PC y un teléfono inteligente.

Una CA puede realizar un proceso de autenticación para determinar si cada dispositivo puede ser una entidad válida. Cuando se va a realizar comunicación entre dispositivos, la CA puede cifrar las claves públicas de los dispositivos utilizando una clave privada del CA y transmitir las claves públicas cifradas de tal manera que los respectivos dispositivos puede confiar o basarse sobre la validez de una clave pública de un dispositivo de una contraparte y utilizar la clave pública.

Dependiendo de los casos, se puede integrar la CA y el servidor. Cuando el servidor se puede integrar en la CA, la CA integrada puede autenticar cada uno de los dispositivos. En lo sucesivo, para facilitar la descripción, el servidor no se ilustra particularmente y sólo se ilustra la CA y se describe asumiendo que el servidor se integra en la CA.

Al realizar un método de autenticación de seguridad de acuerdo con las realizaciones, un protocolo puede requerir que una operación de información recolectada, por ejemplo, un PIN y una clave pública de dispositivos de comunicación M2M, re realice inicialmente para autenticación. La información recolectada se puede utilizar como información de referencia para determinar la validez de cada dispositivo en una red de comunicación M2M.

El proceso para realizar el método de autenticación de seguridad de acuerdo con realizaciones puede incluir cuatro operaciones, 1) una operación de insertar un número de serie (SN) en cada uno de los dispositivos individuales, extraer un PIN, y generar una lista de PIN, 2) una operación para registrar la lista de PIN a una CA, 3) una operación para intercambiar y de esta manera registrar una clave pública entre un dispositivo y la CA, y 4) una operación para autenticar el PIN para autenticación mutua antes de iniciar comunicación.

El anterior “1" se describió anteriormente con referencia a la figura 4, el anterior “2" se describirá más adelante con referencia a la figura 5, el anterior “3" se describirá más adelante con referencia a la figura 6, y el anterior “4" se describirá con referencia a la figura 7.

La figura 5 es un diagrama que ilustra un proceso para distribuir dispositivos de autenticación de seguridad 500 desde una fábrica 501 y transferir y de esta manera registrar una lista 403 de PIN a una CA 502 de acuerdo con una realización.

En operación 510, cada uno de los dispositivos 500 se puede distribuir en una posición para ser utilizado. El proceso de distribución anterior puede indicar un proceso general sobre las ventas o la circulación después de la fabricación de los dispositivos 500.

En operación 520, se puede entregar la lista 403 de PIN a la CA 502 a través de una ruta fuera de línea.

En operación 530, se puede registrar la lista 403 de PIN suministrada.

La figura 6 es un diagrama de flujo que ilustra un proceso para registrar claves públicas entre un dispositivo 601 y una CA 602 de acuerdo con una realización.

En operación 610, la CA 602 puede transmitir, al dispositivo 601, un mensaje que puede hacer una solicitud para una clave pública.

En operación 620, el dispositivo 601 puede generar un mensaje P al cifrar un número de serie (SN) y una clave pública del dispositivo 601 utilizando un PIN que puede ser una clave secreta del dispositivo 601.

En operación 630, el dispositivo 601 puede transmitir el mensaje P a la CA 602. Es decir, el dispositivo 601 puede transmitir la clave pública del dispositivo 601 a la CA 602 utilizando un algoritmo cifrado de clave secreta.

Cuando la CA 602 recibe el mensaje P y descifra el mensaje P utilizando el PIN que puede ser la clave secreta del dispositivo 601 en operación 640, se puede obtener la PUB_KEY_D que puede ser la clave pública del dispositivo 601.

Aquí, en operación 650, la CA 602 puede comparar el SN descifrado con el SN del dispositivo 601 cuya autenticación puede estar en curso.

Cuando el SN descifrado se verifica para ser idéntico al SN del dispositivo 601, se puede verificar la validez del dispositivo 601. En operación 660, la CA 602 puede registrar la PUB_KEY_D que puede ser la clave pública del dispositivo 601 para una lista de PIN del CA 602.

En operación 670, la CA 602 puede generar un mensaje Q al cifrar el SN y la PUB_KEY_{CA} que puede ser una clave pública del CA 602 utilizando el PIN de clave secreta del dispositivo 601. En operación 680, la CA 602 puede transferir el mensaje Q generado al dispositivo 601.

En operación 690, el dispositivo 601 puede obtener el SN y la PUB_KEY_{CA} al descifrar el mensaje Q utilizando un algoritmo de clave secreta.

En operación 691, el dispositivo 601 puede verificar la validez al verificar la identidad del SN. Cuando se verifica la identidad del SN, el dispositivo 601 puede almacenar la clave pública PUB_KEY_{CA} del CA 602 en una memoria no volátil del dispositivo 601 en operación 692.

Cuando las claves públicas se intercambian mutualmente entre el dispositivo 601 y la CA 602 a través del proceso anterior, se puede realizar la comunicación de datos utilizando cada clave pública de las contrapartes.

Con referencia a la figura 7, la validez entre un dispositivo 701 y una CA 702 se puede verificar antes de hincar la comunicación mutual

Se pueden presentar dos casos pueden para realizar un proceso de autenticación para verificar la validez. Uno puede ser un caso en el que un servidor puede ser idéntico a una CA y la CA se comunica directamente con un dispositivo. El otro puede ser un caso en el que un servidor puede ser diferente de una CA, o un dispositivo individual y otro dispositivo individual se comunican entre sí. El primer caso se describirá con referencia a la figura 7 y el segundo caso se describirá con referencia a la figura 8.

La figura 7 es un diagrama de flujo que ilustra un proceso para verificar la validez del dispositivo 701 de acuerdo con una realización.

En operación 710, la CA 702 puede generar un mensaje P al cifrar un número de serie (SN) del dispositivo 701 y un presente R que puede ser un número aleatorio para autenticación, utilizando $PRIV\_KEY_{CA}$ que puede ser una clave privada del CA 702.

Cuando el mensaje P se transmite al dispositivo 701 en operación 720, el dispositivo 701 puede descifrar el mensaje P utilizando la PUB_KEY_{CA} que puede ser una clave pública del CA 702 en operación 730.

De acuerdo con lo anterior, se puede obtener el SN y el presente R. Cuando la validez se verifica al comparar la identidad del SN en operación 740, el dispositivo 701 puede cifrar el presente R de nuevo utilizando $PRIV\_KEY_D$ que puede ser una clave privada del dispositivo 701 en operación 750.

El mensaje cifrado Q se puede transmitir a la CA 702 en operación 760, y la CA 702 puede descifrar el presente R utilizando la clave pública PUB_KEY_D del dispositivo 701 en operación 770. Cuando el presente R se verifica en operación 780, se puede verificar la validez que permite la comunicación entre el dispositivo 701 y la CA 702. De acuerdo con lo anterior, el dispositivo 701 y la CA 702 se pueden comunicar entre sí al transmitir y recibir datos utilizando el esquema de clave pública cifrado/descifrado.

El primer caso en el que un servidor puede ser idéntico a una CA y la CA se comunica con un dispositivo se describió anteriormente. En adelante, el segundo caso en el que un servidor puede ser diferente de una CA, o un dispositivo individual y otro dispositivo individual se comunican entre sí, se describirá con referencia a la figura 8.

Aquí, el dispositivo que desee comunicarse con el servidor u otro dispositivo necesita recibir una clave pública del dispositivo. Excluyendo una configuración en la que la CA puede actuar como un mediador durante un proceso de intercambio de clave pública, el segundo caso puede ser similar al primer caso.

Es decir, sólo la CA puede mantener cada PIN que puede ser una clave secreta de los dispositivos individuales y puede verificar la validez con respecto a cada uno de los dispositivos individuales al intercambiar claves públicas. Debido a que no se puede mantener una clave secreta entre los dispositivos o entre un dispositivo y el servidor, la CA puede servir como un mediador durante un proceso para verificar si un dispositivo correspondiente puede ser un objetivo para intercambiar una clave pública o un proceso para intercambiar claves públicas. El proceso anterior se describirá con referencia a la figura 8.

La figura 8 es un diagrama de flujo que ilustra un proceso para intercambiar una clave pública entre dispositivos, por ejemplo, un primer dispositivo 801 y un segundo dispositivo 803 a través de una CA 802 con el fin de realizar autenticación de seguridad entre los dispositivos (que excluyen la CA 802), de acuerdo con una realización.

Aquí, se puede asumir que el segundo dispositivo 803 puede desear intercambiar las claves públicas con el primer dispositivo 801 para realizar comunicación con el primer dispositivo 801.

En operación 810, el segundo dispositivo 803 puede solicitar la CA 802 para la PUB_KEY_{D1} que puede ser una clave pública del primer dispositivo 801.

En operación 820, la CA 802 puede generar un mensaje P al cifrar la PUB_KEY_{D2} que puede ser una clave pública del segundo dispositivo 803 y el SN_{D1} que puede ser un número de serie (SN) del primer dispositivo 801 utilizando $PRIV\_KEY_{CA}$ que puede ser una clave privada del CA 802.

En operación 830, la CA 802 puede generar un mensaje Q al cifrar clave pública PUB_KEY_{D1} del primer dispositivo 801 y el SN_{D2} que puede ser un SN del segundo dispositivo 803 utilizando la clave privada $PRIV\_KEY_{CA}$ del CA 802.

Cuando la CA 802 transfiere el mensaje P al primer dispositivo 801 en operación 840, el primer dispositivo 801 puede obtener SN_{D1} y la clave pública PUB_KEY_{D2} del segundo dispositivo 803 al descifrar el mensaje P utilizando la clave pública PUB_KEY_{CA} del CA 802 en operación 850.

Cuando la validez se verifica a través de comparar la identidad de SN_{D1} en operación 860, el primer dispositivo 801 puede almacenar la clave pública PUB_KEY_{D2} del segundo dispositivo 803 y utilizar la misma para cifrar un mensaje que se va a transmitir al segundo dispositivo 803.

Cuando la CA 802 transfiere el mensaje Q el segundo dispositivo 803 en operación 870, el segundo dispositivo 803 puede obtener el SN_{D2} y la clave pública PUB_KEY_{D1} del primer dispositivo 801 al descifrar el mensaje Q utilizando la clave pública PUB_KEY_{CA} del CA 802 en operación 880.

Cuando la validez se verifica a través de comparar la identidad de SN_{D2} en operación 890, el segundo dispositivo 803 puede almacenar la clave pública PUB_KEY_{D1} del primer dispositivo 801 y utilizar la misma para cifrar un mensaje que se va a transmitir al primer dispositivo 801.

Cuando se intercambian mutualmente claves públicas entre el primer dispositivo 801 y el segundo dispositivo 803, el primer dispositivo 801 y el segundo dispositivo 803 se pueden comunicar directamente entre sí al cifrar un mensaje que se va a transmitir a las contrapartes utilizando claves públicas de las contrapartes, que pueden ser las mismas que la comunicación mencionada anteriormente entre la CA y el dispositivo.

Incluso en un caso en el que una CA y un servidor pueden ser diferentes y un dispositivo se puede comunicar con el servidor, el proceso puede ser el mismo a excepción de una configuración en la que el segundo dispositivo 803 puede ser el servidor.

De acuerdo con las realizaciones, requisitos, tales como imposibilidad de la exposición, imposibilidad de duplicación, y singularidad, se podrán satisfacerse al aplicar un PIN de clave secreta con base en PUF a un esquema de autenticación con base en conocimiento.

De acuerdo con las realizaciones, la confiabilidad de la autenticación de seguridad se puede garantizar en comunicación M2M, por ejemplo, una variedad de aplicaciones tales como una aplicación que utiliza un RFID, una aplicación de red

inteligente, una aplicación de computación en la nube, y similares. No obstante, los costes para garantizar la fiabilidad pueden ser económicos.

Las realizaciones descritas anteriormente se pueden grabar en medios legibles por ordenador como una forma de instrucciones de programa operados por varios tipos de ordenadores. Los medios también pueden incluir, solo o en combinación con las instrucciones del programa, archivos de datos, estructuras de datos, y similares. Ejemplos de medios legibles por ordenador incluyen medios magnéticos tales como discos duros, disquetes y cintas magnéticas; medios ópticos tales como discos CD ROM y DVD; medios magneto-ópticos tales como disquetes; y dispositivos de hardware que se configuran especialmente para almacenar y realizar instrucciones de programa, tales como memoria de sólo lectura (ROM), memoria de acceso aleatorio (RAM), memoria flash, y similares. Ejemplos de instrucciones de programa pueden incluir código máquina, tal como es el producido por un compilador y archivos que contienen código de nivel superior que pueden ser ejecutados por el ordenador utilizando un intérprete. Los dispositivos de hardware descritos se pueden configurar para actuar como uno o más módulos de software con el fin de realizar las operaciones de las realizaciones de ejemplo descritas anteriormente, o viceversa.

Aunque se han mostrado y descrito unas pocas realizaciones de la presente invención, la presente invención no se limita a las realizaciones descritas. En su lugar, se apreciará por los expertos en la técnica que se pueden hacer cambios a estas realizaciones sin apartarse de la invención, cuyo alcance se define por las reivindicaciones y sus equivalentes.

REIVINDICACIONES

1. Un dispositivo (200) terminal para realizar comunicación máquina a máquina, el dispositivo terminal comprende:

un módulo (220) de clave secreta que incluye una función no clonable física,

caracterizado porque se configura el módulo (220) de clave secreta para proporcionar una clave secreta utilizando la función no clonable física para transferir, utilizando un esquema de cifrado de clave secreta, una clave pública utilizada para comunicación del dispositivo terminal utilizando un esquema de cifrado de clave pública; y en el que el dispositivo terminal comprende adicionalmente un módulo (250) de clave privada para proporcionar una clave privada para generar la clave pública.

2. El dispositivo terminal de la reivindicación 1, en el que el módulo (250) de clave privada incluye una función no clonable física.

3. El dispositivo terminal de la reivindicación 1 o reivindicación 2, comprende adicionalmente:

una unidad (230) de fusible para bloquear una ruta a través de la cual se extrae la clave secreta en respuesta a la aplicación de sobrecorriente.

4. El dispositivo terminal de la reivindicación 3, en el que se configura la unidad (230) de fusible para bloquear la ruta después de que se extrae inicialmente la clave secreta desde el dispositivo (200) terminal.

5. El dispositivo terminal de la reivindicación 1 o reivindicación 2, adicionalmente comprende:

un almacenamiento (210) de número de serie para almacenar un número de serie del dispositivo (200) terminal; y

una unidad (230) de fusible para bloquear una ruta a través de la cual se extrae la clave secreta, después de que se almacena el número de serie en el almacenamiento (210) de número de serie y se extrae la clave secreta.

6. El dispositivo terminal de la reivindicación 1 o reivindicación 2, adicionalmente comprende:

un generador (240) de clave pública para generar la clave pública utilizando la clave privada.

7. El dispositivo terminal de la reivindicación 1 o reivindicación 2, en el que:

se configura el dispositivo (200) terminal para almacenar una clave pública de un dispositivo (702) externo utilizado para comunicación del dispositivo externo utilizando el esquema de cifrado de clave pública, y

se configura el dispositivo (200) terminal para descifrar un mensaje recibido desde el dispositivo externo utilizando la clave pública del dispositivo externo.

8. El dispositivo terminal de la reivindicación 7, en el que cuando se descifra el mensaje, se configura el dispositivo (200) terminal para verificar la validez del dispositivo (702) externo dependiendo de si se verifica la identidad de un número de serie del dispositivo (200) terminal.

9. Un dispositivo (602) de autoridad de certificación para manejar un dispositivo terminal que realiza comunicación máquina a máquina, el dispositivo de autoridad de certificación caracterizado por:

una lista de números de identidad personal para almacenar una clave secreta del dispositivo (601) terminal y un número de serie del dispositivo terminal,

en el que cuando se recibe un mensaje en el que se cifran una clave pública utilizada para comunicación utilizando un esquema de cifrado de clave pública y el número de serie del dispositivo (601) terminal utilizando la clave secreta, por el dispositivo (602) de autoridad de certificación desde el dispositivo terminal, el dispositivo de autoridad de certificación se configura para descifrar el mensaje utilizando la clave secreta, y

cuando se descifra el mensaje, se configura el dispositivo (602) de autoridad de certificación para verificar la validez del dispositivo (601) terminal dependiendo de si se verifica la identidad de un número de serie del dispositivo terminal, y

cuando se verifica la validez del dispositivo (601) terminal, se configura el dispositivo (602) de autoridad de certificación para almacenar la clave pública del dispositivo terminal.

10. Un método para realizar, mediante un dispositivo (601) terminal, autenticación de seguridad con el fin de realizar comunicación máquina a máquina, el método comprende:

generar una clave privada del dispositivo (601) terminal utilizando una primera función no clonable física incorporada en el dispositivo terminal; y

generar una clave pública para realizar autenticación de seguridad utilizando la clave privada;

caracterizado porque el método comprende adicionalmente:

generar una clave secreta para transferir la clave pública externamente utilizando un esquema de cifrado de clave secreta, que utiliza una segunda función no clonable física diferente de la primera función no clonable física;

transmitir (630) la clave pública a una autoridad (602) de certificación externa con base en un esquema de cifrado de clave secreta utilizando la clave secreta; y

realizar la autenticación de seguridad con un terminal (803) externo diferente del dispositivo (601) terminal o la autoridad (602) de certificación externa utilizando la clave pública.

11. El método de la reivindicación 10, adicionalmente comprende:

recibir, desde la autoridad (702) de certificación externa, un mensaje cifrado utilizando un esquema de cifrado de clave pública;

descifrar (730) el mensaje cifrado utilizando una clave pública prealmacenada de la autoridad (702) de certificación externa; y

completar la autenticación de seguridad con la autoridad de certificación externa cuando se verifica (740) un número de serie del dispositivo (701) terminal desde el mensaje descifrado.

12. El método de la reivindicación 10, adicionalmente comprende:

bloquear un fusible presente en una ruta a través de la cual se extrae la clave secreta, después de que almacena un número de serie del dispositivo terminal en un almacenamiento de número de serie y se extrae inicialmente la clave secreta.

13. Un método para retransmitir, mediante un dispositivo (802) de autoridad de certificación, claves públicas para comunicación máquina a máquina entre un primer dispositivo (801) terminal y un segundo dispositivo terminal de acuerdo con la reivindicación 1 (803), el método comprende:

recibir, desde el segundo dispositivo (803) terminal, una solicitud para una clave pública del primer dispositivo (801) terminal;

caracterizado porque el método comprende adicionalmente:

generar (830) un primer mensaje cifrado al cifrar la clave pública del primer dispositivo (801) terminal y un número de serie del segundo dispositivo (803) terminal utilizando una clave privada del dispositivo (802) de autoridad de certificación;

generar (820) un segundo mensaje cifrado al cifrar una clave pública del segundo dispositivo (803) terminal y un número de serie del primer dispositivo (801) terminal utilizando la clave privada del dispositivo (802) de autoridad de certificación;

transmitir (870) el primer mensaje cifrado al segundo dispositivo (803) terminal; y

transmitir (840) el segundo mensaje cifrado al primer dispositivo (801) terminal.

14. El método de la reivindicación 13, en el que el segundo dispositivo (803) terminal descifra (880) el primer mensaje utilizando una clave pública del dispositivo (802) de autoridad de certificación que corresponde a la clave privada del dispositivo de autoridad de certificación, y confía la clave pública transmitida del primer dispositivo (801) terminal cuando se verifica el número de serie del segundo dispositivo (803) terminal desde el primer mensaje descifrado.

15. El método de la reivindicación 13 o reivindicación 14, en el que el primer dispositivo (801) terminal descifra (850) el segundo mensaje utilizando una clave pública del dispositivo (802) de autoridad de certificación que corresponde a la clave privada del dispositivo de autoridad de certificación, y confía la clave pública transmitida del segundo dispositivo (803) terminal cuando se verifica el número de serie del primer dispositivo (801) terminal desde el segundo mensaje descifrado.

16. Un medio de grabación legible por ordenador no transitorio que almacena un programa para implementar el método de acuerdo con cualquiera de las reivindicaciones 10 a 15.

FIG. 1

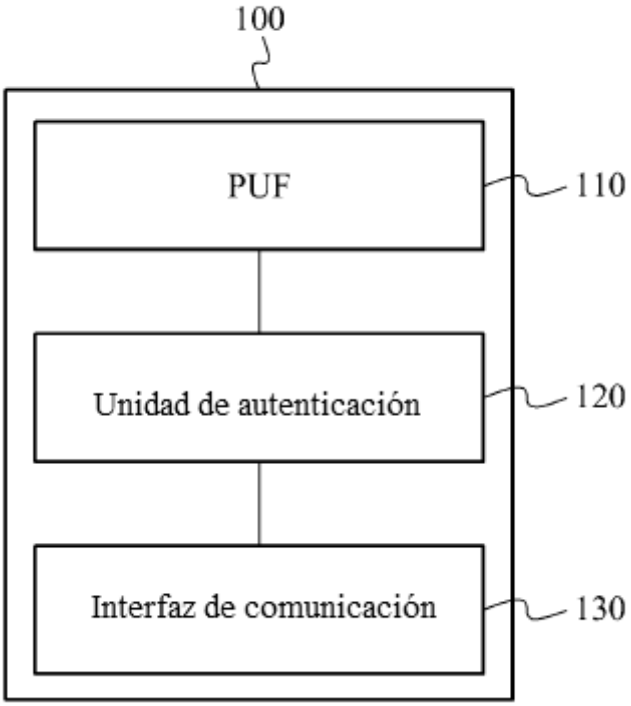

100
PUF
110
Unidad de autenticación
120
Interfaz de comunicación
130

FIG. 2

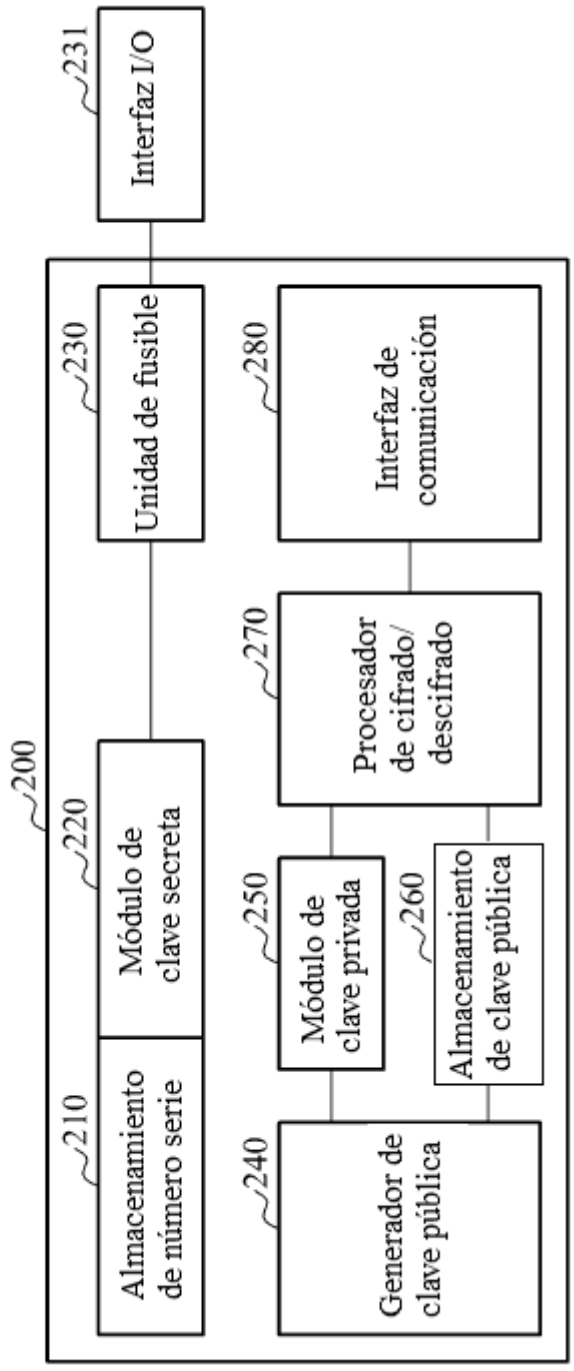

231
Interfaz I/O
200
230
Unidad de fusible
280
Interfaz de comunicación
220
Módulo de clave secreta
270
Procesador de cifrado/ descifrado
210
Almacenamiento de número serie
250
Módulo de clave privada
260
Almacenamiento de clave pública
240
Generador de clave pública

FIG. 3

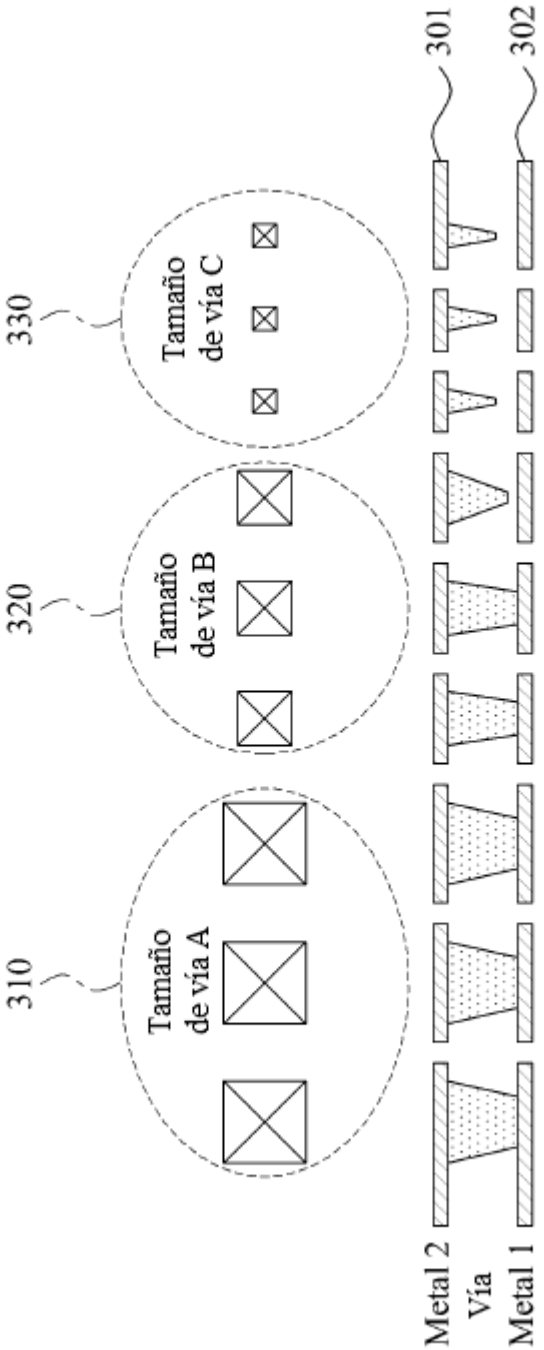

310
Tamaño de vía A
320
Tamaño de vía B
330
Tamaño de vía C
301
302
Metal 2
Vía
Metal 1
Valor
0 0 0 0 1 1 1 1

FIG. 4

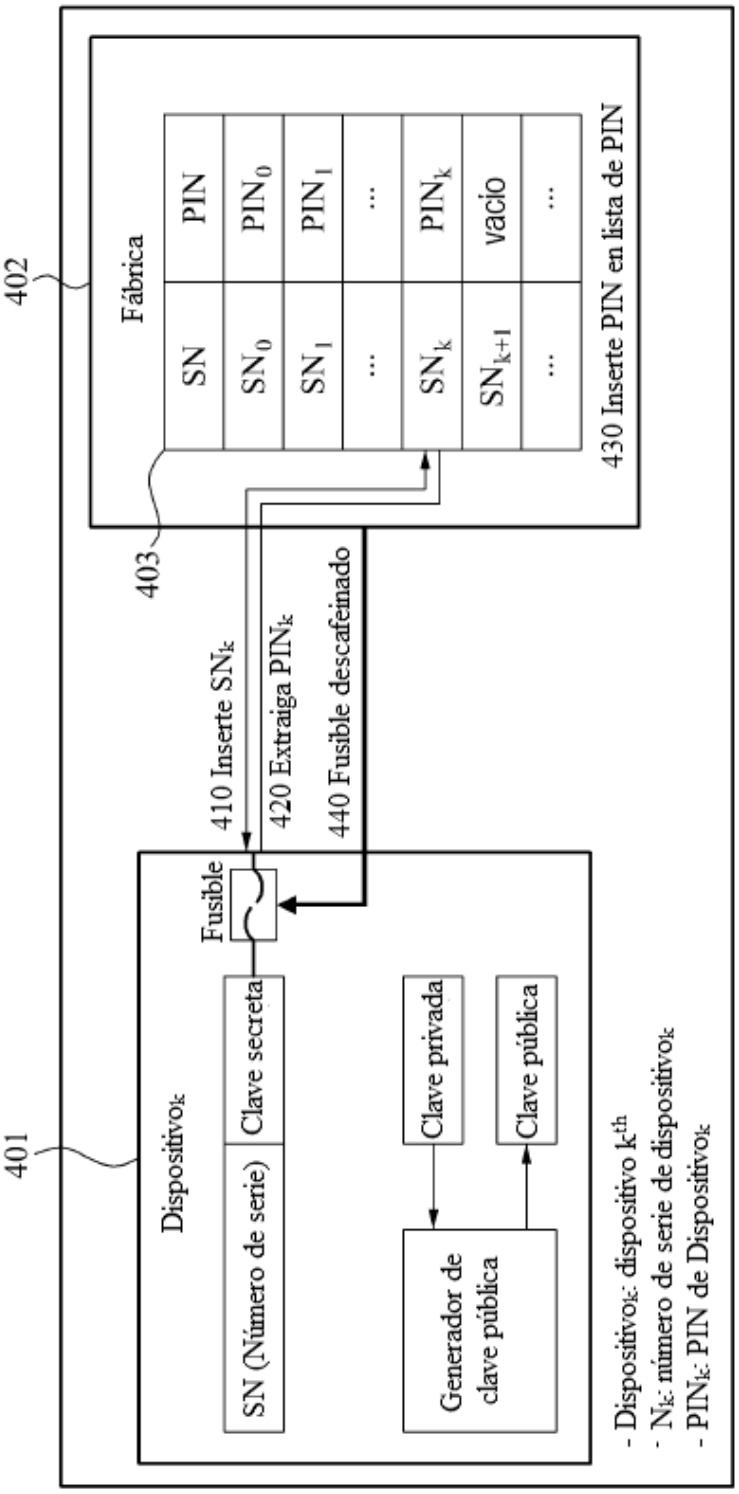

401
402
403
Dispositivo$_k$
SN (Número de serie)
Clave secreta
Fusible
Generador de clave pública
Clave privada
Clave pública
Fábrica
SN
PIN
SN$_0$
PIN$_0$
SN$_1$
PIN$_1$
...
...
SN$_k$
PIN$_k$
SN$_{k+1}$
vacío
...
...
410 Inserte SN$_k$
420 Extraiga PIN$_k$
430 Inserte PIN en lista de PIN
440 Fusible descafeinado
- Dispositivo$_k$: dispositivo kth
- N$_k$: número de serie de dispositivo$_k$
- PIN$_k$: PIN de Dispositivo$_k$

FIG. 5

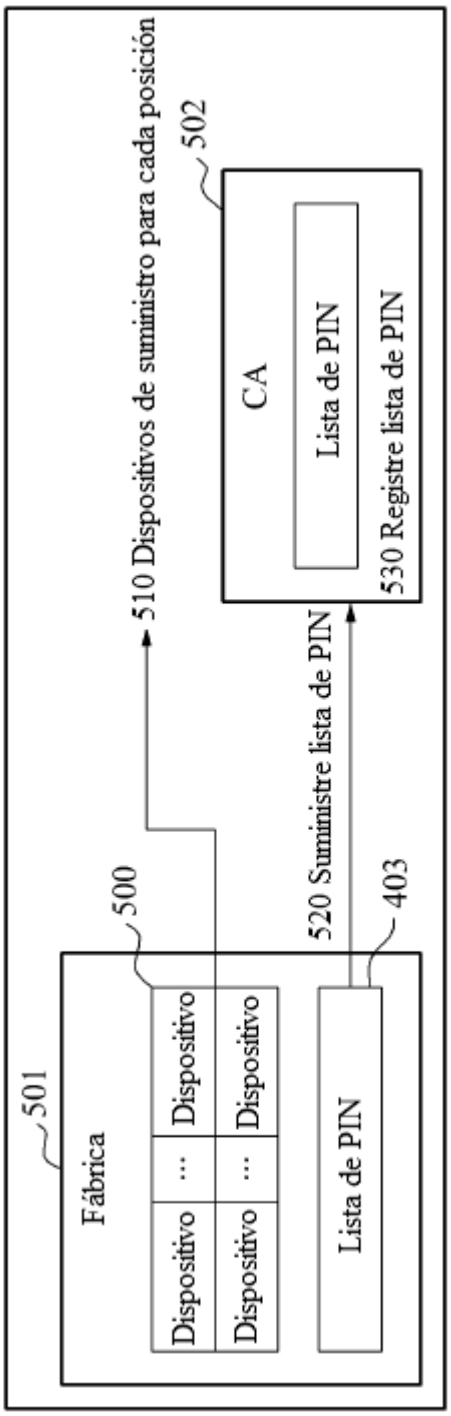

501
Fábrica
500
Dispositivo
...
Dispositivo
Dispositivo
...
Dispositivo
Lista de PIN
403
510 Dispositivos de suministro para cada posición
520 Suministre lista de PIN
502
CA
Lista de PIN
530 Registre lista de PIN

FIG. 6

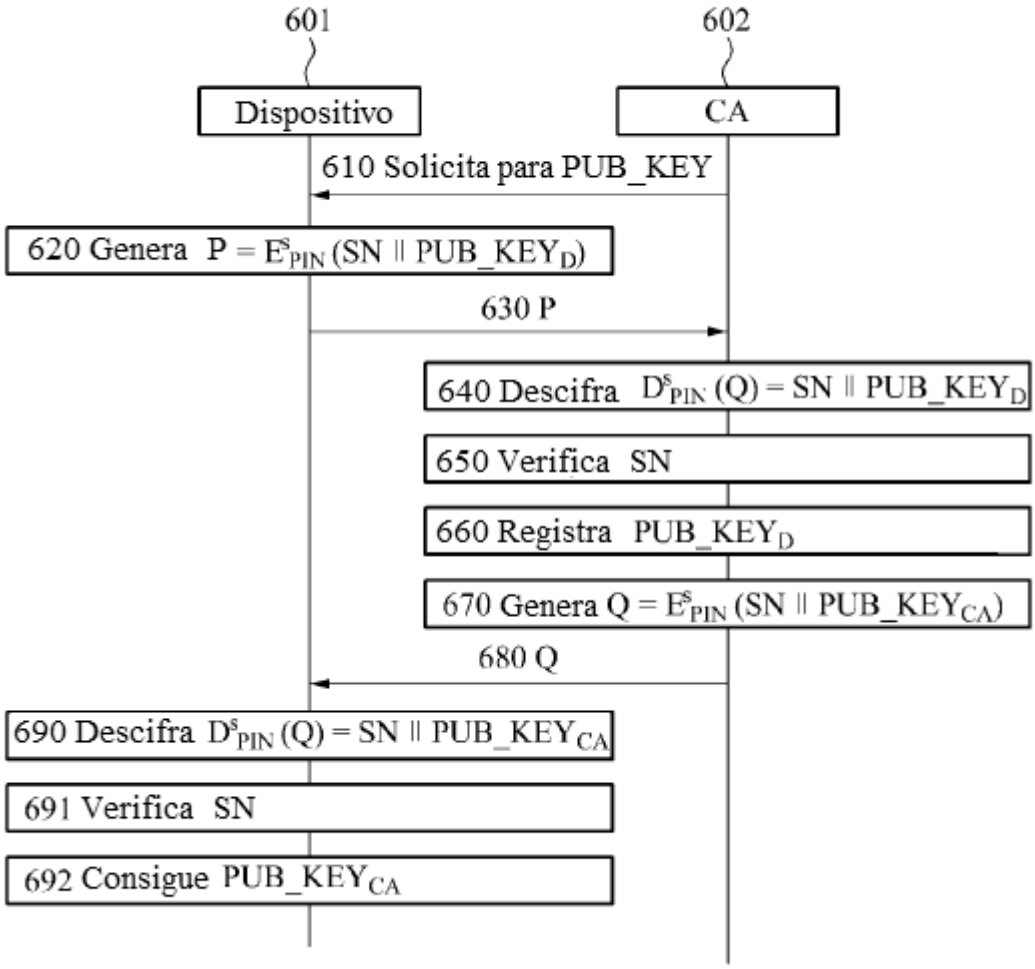

601
602
Dispositivo
CA
610 Solicita para PUB_KEY
620 Genera P = E^s_PIN (SN || PUB_KEY_D)
630 P
640 Descifra D^s_PIN (Q) = SN || PUB_KEY_D
650 Verifica SN
660 Registra PUB_KEY_D
670 Genera Q = E^s_PIN (SN || PUB_KEY_CA)
680 Q
690 Descifra D^s_PIN (Q) = SN || PUB_KEY_CA
691 Verifica SN
692 Consigue PUB_KEY_CA

FIG. 7

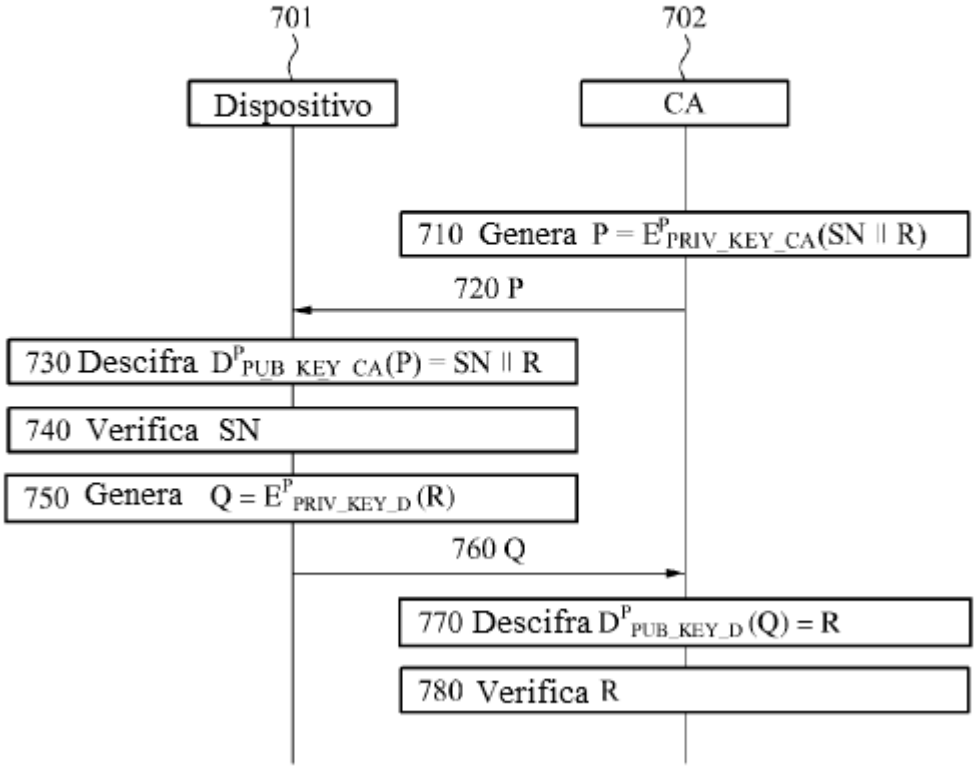
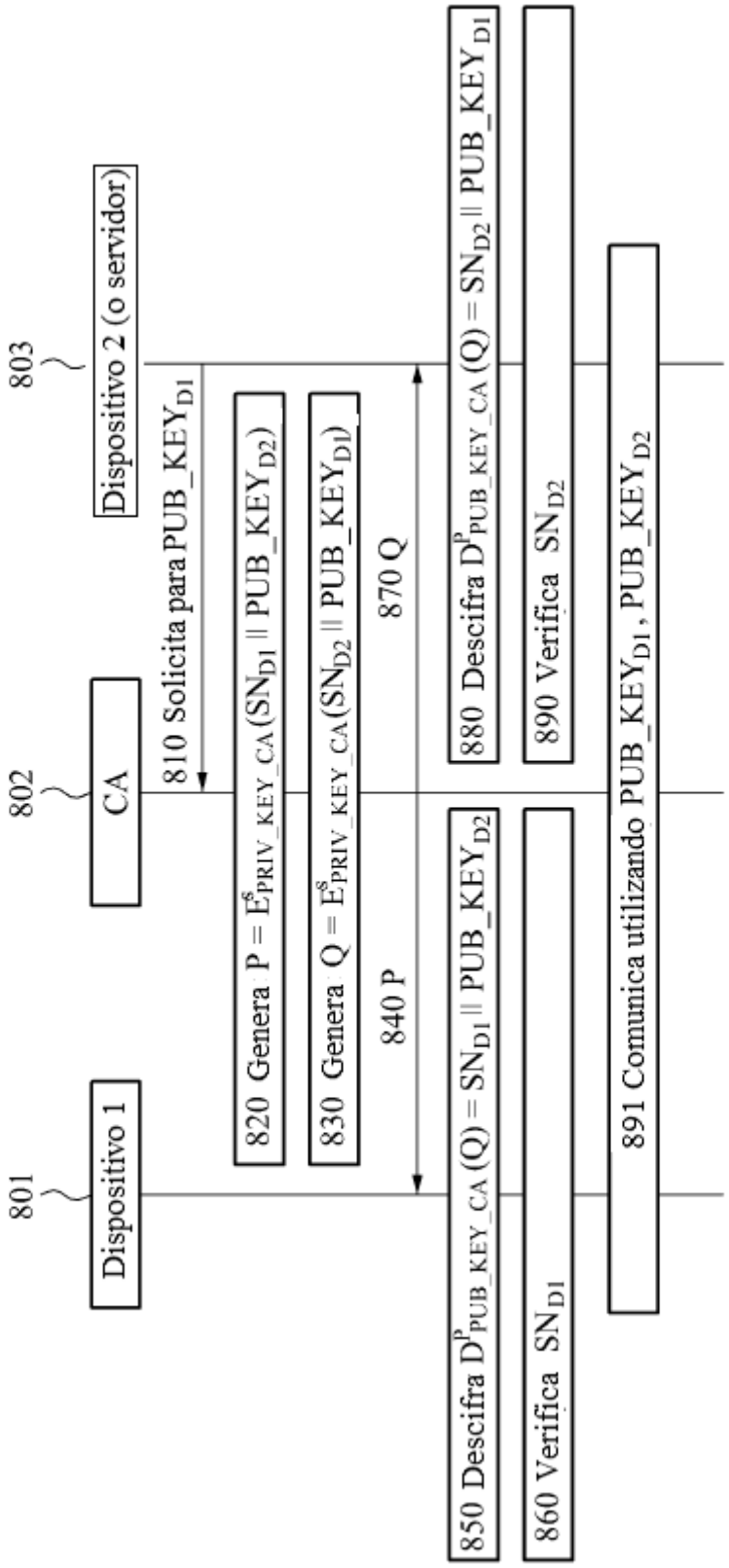

701
702
Dispositivo
CA
710 Genera $P = E^{P}_{PRIV\_KEY\_CA}(SN \| R)$
720 P
730 Descifra $D^{P}_{PUB\_KEY\_CA}(P) = SN \| R$
740 Verifica SN
750 Genera $Q = E^{P}_{PRIV\_KEY\_D}(R)$
760 Q
770 Descifra $D^{P}_{PUB\_KEY\_D}(Q) = R$
780 Verifica R

FIG. 8


801
Dispositivo 1
802
CA
803
Dispositivo 2 (o servidor)
810 Solicita para PUB_KEY_D1
820 Genera P = E^S_PRIV_KEY_CA(SN_D1 || PUB_KEY_D2)
830 Genera Q = E^S_PRIV_KEY_CA(SN_D2 || PUB_KEY_D1)
840 P
870 Q
850 Descifra D^P_PUB_KEY_CA(Q) = SN_D1 || PUB_KEY_D2
860 Verifica SN_D1
880 Descifra D^P_PUB_KEY_CA(Q) = SN_D2 || PUB_KEY_D1
890 Verifica SN_D2
891 Comunica utilizando PUB_KEY_D1, PUB_KEY_D2