(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 950 336**

(51) Int. CI.:

H04L 9/06 (2006.01)
H04L 9/32 (2006.01)
H04L 9/40 (2012.01)
H04W 4/029 (2008.01)
G06Q 30/00 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **20.12.2018 E 21175935 (2)**

(97) Fecha y número de publicación de la concesión europea: **19.04.2023 EP 3890367**

(54) Título: **Métodos y sistemas para preparar y realizar una autenticación de objeto**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.10.2023

(73) Titular/es:

MERCK PATENT GMBH (100.0%)
Frankfurter Strasse 250
64293 Darmstadt, DE

(72) Inventor/es:

ENDRESS, THOMAS;
SZABO, DANIEL y
BERKERMANN, FREDERIC

(74) Agente/Representante:

ARIAS SANZ, Juan

DESCRIPCIÓN

Métodos y sistemas para preparar y realizar una autenticación de objeto

Campo de la invención

La presente invención se relaciona con el campo del seguimiento y la protección contra la falsificación de objetos físicos, tales como productos como por ejemplo productos farmacéuticos u otros productos relacionados con la salud, y en particular con preparar y realizar una autenticación segura de tales objetos. Específicamente, una solución de autenticación global proporcionada en la presente memoria comprende un método y un sistema para preparar una autenticación asegurada posterior de un objeto físico o grupo de objetos físicos por un destinatario del mismo, un método y sistema para autenticar un objeto físico o grupo de objetos físicos, un método y sistema para proporcionar de manera segura un esquema de combinación variable en el tiempo para autenticar un objeto físico o un grupo de objetos físicos según los métodos anteriores, y con programas informáticos relacionados correspondientes a dichos métodos.

Antecedentes

En muchas industrias, la falsificación de productos es un problema sustancial que impacta significativamente no solamente en los ingresos de los fabricantes de productos originales, sino que incluso puede representar una amenaza grave para la salud e incluso la vida de los consumidores u operadores de productos falsificados, es decir, falsos. Tales categorías de productos relevantes para la seguridad incluyen, en particular, piezas para automóviles y aeronaves, componentes para la construcción de edificios u otras infraestructuras, alimentos e incluso dispositivos médicos y productos farmacéuticos.

Además, en una amplia gama de industrias diferentes, la trazabilidad de bienes y objetos físicos es un requisito clave. Esto se aplica en particular a las infraestructuras de logística y cadena de suministro y a entornos de flujo de trabajo altamente regulados/estructurados. Ejemplos son lugares de trabajo industriales que están controlados por reguladores oficiales tales como la FDA (Administración de Alimentos y Medicamentos de EE. UU.) y/o que están certificados, por ejemplo, según GMP (Buenas prácticas de fabricación), GLP (Buenas prácticas de laboratorio), GCP (Buenas prácticas clínicas) o DIN ISO u otros estándares y reglas similares. Cada uno de estos entornos regulados requiere en particular un seguimiento de auditoría y tecnologías auditables. Un ejemplo adicional es la trazabilidad de productos de alto valor, tales como piezas de repuesto industriales, con el fin de probar la autenticidad y el uso previsto de estas piezas en mercados secundarios.

Con el fin de limitar la falsificación y proporcionar integridad en la cadena de suministro y el flujo de trabajo, incluyendo el reconocimiento y la autenticación de productos dentro de los flujos de trabajo y las cadenas de suministro, diversas industrias han desarrollado una serie de diferentes medidas de protección y soluciones de identificación. Medidas de protección ampliamente usadas comprenden añadir una denominada característica de seguridad a un producto, la característica que es bastante difícil de falsificar. Por ejemplo, los hologramas, las tintas ópticamente variables, los hilos de seguridad y las partículas magnéticas incrustadas son características de seguridad conocidas que son difíciles de reproducir por los falsificadores. Si bien algunas de estas características de seguridad son “abiertas”, es decir, se pueden ver fácilmente o reconocer de otro modo por un usuario del producto, otras características de seguridad están “encubiertas”, es decir, están ocultas y solamente se pueden detectar usando dispositivos específicos, tales como fuentes de luz ultravioleta, espectrómetros, microscopios o detectores de campo magnético, o incluso equipos forenses más sofisticados. Ejemplos de características de seguridad encubiertas son, en particular, impresiones con tinta luminiscente o tinta que solamente es visible en la parte infrarroja del espectro electromagnético pero no en su parte visible, composiciones de materiales específicos y pigmentos magnéticos.

Un grupo específico de características de seguridad, que se usan en particular en criptografía, se conoce como “Funciones Físicas no Clonables” (PUF). También se hace referencia algunas veces a las PUF como “Funciones Físicamente no Clonables” o “Funciones Físicas Aleatorias”. Una PUF es una entidad física que está incorporada en una estructura física y es fácil de evaluar pero difícil de predecir, incluso para un atacante con acceso físico a la PUF. Las PUF dependen de la singularidad de su microestructura física, que típicamente incluye un componente aleatorio que ya está intrínsecamente presente en la entidad física o se introduce o genera explícitamente en la entidad física durante su fabricación y que es sustancialmente incontrolable e impredecible. Por consiguiente, incluso las PUF que se producen exactamente mediante el mismo proceso de fabricación difieren al menos en su componente aleatorio y, de este modo, se pueden distinguir. Mientras que en la mayoría de los casos, las PUF son características encubiertas, esto no es una limitación y también son posibles las PUF abiertas. Además, las PUF son ideales para permitir la identificación pasiva (es decir, sin difusión activa) de objetos físicos.

Las PUF se conocen en particular en relación con su implementación en circuitos electrónicos integrados por medio de variaciones mínimas inevitables de las microestructuras producidas en un chip dentro de tolerancias relacionadas con el proceso dadas, y específicamente que se usan para derivar claves criptográficas a partir de las mismas, por ejemplo, en chips para tarjetas inteligentes u otros chips relacionados con la seguridad. Un ejemplo de una explicación y aplicación de tales PUF relacionadas con chips se describe en el artículo “Background on Physical

Unclonable Functions (PUFs)", Virginia Tech, Departamento de Ingeniería Eléctrica e Informática, 2011, que está disponible en Internet en el hipervínculo: http://rijndael.ece.vt.edu/puf/background.html.

No obstante, también se conocen otros tipos de PUF, tales como las distribuciones aleatorias de fibras en papel usadas como sustrato para fabricar billetes de banco, en donde la distribución y orientación de las fibras se pueden detectar mediante detectores específicos y usar como una característica de seguridad del billete de banco. También, los tintes de conversión ascendente (UCD), particularmente las mezclas secretas de los mismos, se pueden usar como PUF.

Con el fin de evaluar una PUF, se usa el llamado esquema de autenticación de desafío-respuesta. El "desafío" es un estímulo físico aplicado a la PUF y la "respuesta" es su reacción al estímulo. La respuesta es dependiente de la naturaleza incontrolable e impredecible de la microestructura física y, de este modo, se puede usar para autenticar la PUF y, de este modo, también un objeto físico del que la PUF forma parte. Un desafío específico y su correspondiente respuesta juntos forman la denominada "pareja desafío-respuesta" (CRP).

Los métodos y sistemas de protección contra la falsificación basados en el uso de PUF para autenticar productos se describen en cada una de las dos Solicitudes de Patente Europea publicadas como EP 3 340 212 A1 y EP 3 340 213 (A1) y en la Solicitud de Patente Europea EP 18 170 044.4 adicional.

En el documento WO 2014/095737 A1 se describen métodos y sistemas adicionales de protección contra la falsificación basados en el reconocimiento automático de objetos y la autenticación basada en tal reconocimiento.

La criptografía asimétrica, a la que también se hace referencia algunas veces como "criptografía de clave pública" o "criptografía de clave pública/privada", es una tecnología conocida basada en un sistema criptográfico que usa pares de claves, en donde cada par de claves comprende una clave pública y una clave privada. Las claves públicas se pueden diseminar ampliamente y, normalmente, están incluso disponibles públicamente, mientras que las claves privadas se mantienen secretas y, normalmente, solamente se conocen por su propietario o titular. La criptografía asimétrica permite tanto (i) autenticación, que es cuando la clave pública se usa para verificar que un titular de la clave privada emparejada originó una información particular, por ejemplo, un mensaje o datos almacenados que contienen la información, firmándola digitalmente con su clave privada, y (ii) protección de información, por ejemplo, un mensaje o datos almacenados, a modo de cifrado, por lo que solo el propietario/titular de la clave privada emparejada puede descifrar el mensaje cifrado con la clave pública por alguien más.

Recientemente, se ha desarrollado la tecnología de cadena de bloques, en donde una cadena de bloques es un libro mayor público en forma de una base de datos distribuida que contiene una pluralidad de bloques de datos y que mantiene una lista de registros de datos en constante crecimiento y está fortalecido contra la manipulación y la revisión por medios criptográficos. Una aplicación destacada de la tecnología de cadena de bloques es la moneda virtual Bitcoin usada para transacciones monetarias en Internet. Una plataforma de cadena de bloques adicional conocida se proporciona, por ejemplo, por el proyecto Ethereum. En esencia, una cadena de bloques se puede describir como un protocolo descentralizado para registrar transacciones entre partes, que captura y almacena de manera transparente cualquier modificación en su base de datos distribuida y las guarda "para siempre", es decir, siempre y cuando exista la cadena de bloques. El almacenamiento de información en una cadena de bloques implica firmar digitalmente la información a ser almacenada en un bloque de la cadena de bloques. Además, el mantenimiento de la cadena de bloques implica un proceso llamado "minería de cadena de bloques", en donde los llamados "mineros" que son parte de la infraestructura de la cadena de bloques, verifican y sellan cada bloque, de manera que la información contenida en el mismo se guarde "para siempre" y el bloque no pueda ser modificado.

Una nueva tecnología de libro mayor adicional se conoce con el nombre de "Tangle", que es una arquitectura de libro mayor distribuida sin bloques ni permisos, que es escalable, liviana y proporciona un consenso en un sistema descentralizado de igual a igual. Una tecnología relacionada destacada que usa Tangle como base técnica se conoce como "IOTA", que es una capa de integridad de datos y acuerdo transaccional para Internet de las Cosas. No obstante, el término "libro mayor distribuido sin bloques" no se pretende que se limite específicamente a la tecnología Tangle.

Compendio de la invención

Es un objeto de la presente invención proporcionar un método y un sistema para proporcionar de manera segura un esquema de combinación variable en el tiempo para autenticar un objeto físico o un grupo de objetos físicos, tal como un producto o un grupo de tales objetos, según un método de autenticación de un objeto físico o un grupo de objetos físicos cuyo método de autenticación se basa en el esquema de combinación.

Una solución a este problema se proporciona por la enseñanza de las reivindicaciones independientes adjuntas. Diversas reivindicaciones preferidas de la presente invención se proporcionan por las enseñanzas de las reivindicaciones dependientes. Con el fin de proporcionar una mejor orientación al lector, se han proporcionado varios encabezados (en cursiva) para estructurar la descripción general a continuación de los diversos aspectos de la solución de autenticación global proporcionada en la presente memoria. No obstante, estos encabezados no se pretende que limiten de ninguna forma la invención descrita en la presente memoria. En particular, cualquier

definición de términos proporcionados en la presente memoria es aplicable a lo largo de este documento y no se limita a una aplicación a una sección, aspecto o realización en particular contenido en la presente memoria.

1. Preparar una autenticación posterior

Un primer aspecto de la solución de autenticación global se dirige a un método de preparación de una autenticación asegurada posterior de un objeto físico o grupo de objetos físicos por un destinatario del mismo. En particular, el método se puede implementar como un método implementado por ordenador.

El método comprende: (i) recibir o generar datos de contexto predichos que representan una ubicación futura predicha en relación con un siguiente destinatario designado del objeto físico o grupo de objetos físicos y un tiempo futuro relacionado de presencia del objeto físico o grupo de objetos físicos en esa ubicación futura; (ii) recibir o generar datos de contexto aleatorios que indiquen una ubicación aleatoria y un tiempo aleatorio; (iii) combinar, según un primer esquema de combinación predeterminado, los datos de contexto predichos y los datos de contexto aleatorios para derivar por ello datos de contexto modificados que representan una ubicación aleatoria modificada y un tiempo aleatorio modificado, cada uno resultante de la combinación; (iv) cifrar los datos de contexto modificados para obtener un paquete de datos de inicio asegurado que represente los datos de contexto modificados; y (v) almacenar dicho paquete de datos de inicio asegurado (SSDP), o hacer que sea almacenado, en un primer almacenamiento de datos que sea accesible para proporcionar el paquete de datos asegurado para una autenticación asegurada posterior de un objeto físico o grupo de objetos físicos.

La ubicación se puede definir particularmente en términos de coordenadas geográficas, por ejemplo, en base a los datos de geolocalización respectivos generados por medio de un sistema de radionavegación por satélite, tal como los conocidos como GPS, GALILEO o GLONASS.

El término “objeto físico” o, para abreviar, “objeto”, como se usa en la presente memoria, se refiere a cualquier tipo de objeto físico, en particular a cualquier tipo de producto hecho por el hombre, tal como por ejemplo, y sin limitación, un producto farmacéutico u otro producto relacionado con la salud, o un objeto natural, tal como por ejemplo y sin limitación un vegetal o una pieza de una materia prima natural; o un embalaje de uno cualquiera o más de los anteriores. Un objeto físico puede comprender en sí mismo múltiples partes, por ejemplo, tanto un bien consumible como un embalaje del mismo. El término “grupo de objetos físicos”, como se usa en la presente memoria, se refiere a un grupo de objetos, que son por sí mismos separados o separables, pero que están destinados a ser distribuidos juntos, por ejemplo, en un mismo bulto o paquete ligado física y/o comercialmente, y que de este modo guardan cierta relación entre sí con respecto a su distribución a uno o más destinatarios.

El término “autenticación”, como se usa en la presente memoria, se refiere a confirmar la verdad de un atributo de un objeto físico, en particular su tipo y su originalidad, declarado verdadero por una entidad. El término “autenticación asegurada”, como se usa en la presente memoria, se refiere a una autenticación que está asegurada por una o más medidas de protección contra interferencias no autorizadas con el proceso de autenticación o los medios usados para él. A modo de ejemplo y sin limitación, tal seguridad puede implicar cifrado y/o información de firma digital en la que se basa tal autenticación como tales medidas de protección. Específicamente, dicho paquete de datos de inicio “asegurado” se puede considerar información que se asegura por una o más de tales medidas de protección con el fin de permitir una autenticación asegurada posterior de un objeto físico o grupo de objetos físicos en base a esta información asegurada.

El término “datos de contexto”, como se usa en la presente memoria, se refiere a datos que representan al menos una ubicación y tiempo específicos, que, de este modo, juntos definen un contexto específico, por ejemplo, de un evento. En particular, los datos de contexto se pueden relacionar con un evento que define o definido por la presencia de un objeto físico o un grupo de objetos físicos en particular en la ubicación y el tiempo representados por los datos de contexto relacionados. La ubicación definida en los datos de contexto se puede relacionar particularmente con una posición física real, por ejemplo, expresada en coordenadas geográficas, o con una posición virtual, tal como un paso o hito en particular dentro de un flujo de trabajo o flujo de proceso definido, o ambos.

El término “esquema de combinación”, como se usa en la presente memoria, se refiere a un esquema, tal como, pero no limitado a, una operación matemática, según la cual se pueden combinar dos o más elementos de datos o conjuntos de datos. El esquema necesita ser invertible y puede ser particularmente una función matemática invertible. Por ejemplo y sin limitación, tal función matemática se puede definir en términos de una multiplicación de matriz invertible. Específicamente, la combinación puede comprender, sin limitación, una mera agregación, tal como yuxtaponer los bits de dos o más conjuntos de datos binarios.

Los términos “almacenar” datos o “hacer que sean almacenados”, como se usan en la presente memoria, pueden incluir en particular almacenar los datos en una cadena de bloques o en un libro mayor distribuido de manera indirecta, es decir, solicitando el rendimiento real de tal almacenamiento a uno o más intermediarios, tales como un minero de una pluralidad de mineros en el caso de una cadena de bloques, que luego realiza o realizan realmente el almacenamiento.

Cuando el término “que comprende” o “comprende” se usa en la presente descripción y reivindicaciones, no excluye otros elementos o pasos. Cuando se usa un artículo indefinido o definido cuando se hace referencia a un sustantivo singular, por ejemplo, “un” o “una”, “el” o “la”, este incluye un plural de ese sustantivo a menos que se indique específicamente algo más.

Los términos “primero”, “segundo”, “tercero” y similares en la descripción y en las reivindicaciones se usan para distinguir entre elementos similares y no necesariamente para describir un orden secuencial o cronológico. Se ha de entender que los términos así usados son intercambiables en las circunstancias apropiadas y que las realizaciones de la invención descritas en la presente memoria son, a menos que esto se excluya explícitamente o sea técnicamente imposible, capaces de operación en secuencias distintas a las descritas o ilustradas en la presente memoria.

El método del primer aspecto define uno de varios aspectos de una solución global de autenticación de objeto presentada en la presente memoria. Dentro de la solución global, sirve para preparar una autenticación asegurada posterior de un objeto físico o grupo de objetos físicos por un destinatario del mismo, por ejemplo por un destinatario que representa un nodo en una cadena de suministro para dicho objeto u objetos físicos. Es un propósito de este método proporcionar un paquete de datos que se asegura por medio del cifrado y que pone a disposición de los destinatarios autorizados que están habilitados para descifrar el paquete de datos, un conjunto inicial de información que se necesita para dicho proceso de autenticación posterior. Se observa que este método de preparación de una autenticación asegurada posterior puede ser y en muchos casos se realizará por una entidad diferente a la autenticación posterior real en sí misma. En particular, el paquete de datos cifrados comprende información que se basa, en parte, en datos aleatorios, lo que añade un nivel adicional de seguridad al proceso de autenticación en su conjunto, porque a diferencia de los datos de contexto reales relacionados con la cadena de suministro, tales como ubicación y tiempo en el que un objeto físico en particular está presente en esa ubicación, los datos aleatorios típicamente no pueden ser predichos por un tercero no autorizado.

A continuación, se describen realizaciones preferidas de este método, que se pueden combinar arbitrariamente unas con otras o con otros aspectos de la presente solución global, a menos que tal combinación esté explícitamente excluida o sea técnicamente imposible.

(a) Realizaciones seleccionadas con relación en particular a la creación del paquete de datos de inicio seguro

En algunas realizaciones, cifrar los datos de contexto modificados comprende cifrar los datos de contexto modificados por medio de un esquema de cifrado asimétrico y una clave pública relacionada perteneciente a dicho siguiente destinatario designado. A diferencia del cifrado simétrico, donde la clave de cifrado tiene que ser mantenida en secreto y, de este modo, ha de ser intercambiada de una manera segura, usar cifrado asimétrico permite usar claves públicas para el cifrado. A diferencia de las claves para el cifrado simétrico, tales claves públicas se pueden intercambiar abiertamente sin crear problemas de seguridad.

En algunas realizaciones, cifrar los datos de contexto modificados comprende además firmar digitalmente los datos de contexto modificados o el paquete de datos de inicio asegurado resultante del cifrado. En particular, la firma digital se puede realizar por medio de un esquema de cifrado asimétrico y una clave privada relacionada perteneciente a un proveedor de dicho objeto físico o grupo de objetos físicos o a la entidad firmante. La firma digital se puede usar para aumentar aún más la seguridad de la autenticación posterior que se basa en los datos de contexto modificados, en la medida que añade un nivel de seguridad adicional que permite una verificación de la originalidad de los datos de contexto modificados cifrados por un destinatario.

El término “firma digital” o “firmar digitalmente”, etc., como se usa en la presente memoria, se refiere a (usar) un conjunto de uno o más valores digitales que confirman la identidad de un remitente u autor de datos digitales y la integridad de este último. Una forma usada frecuentemente de crear una firma digital comprende generar un valor de comprobación aleatoria a partir de los datos a ser protegidos por medio de la aplicación de una función de comprobación aleatoria criptográfica adecuada. Este valor de comprobación aleatoria luego se cifra con una clave privada (algunas veces también llamada “clave segura”) de un sistema criptográfico asimétrico, por ejemplo, basado en el sistema criptográfico RSA, en donde la clave privada típicamente se conoce solamente por el remitente/autor. Normalmente, la firma digital comprende los datos digitales en sí mismos, así como el valor de comprobación aleatoria derivado de ellos por el remitente/autor. Luego, un destinatario puede aplicar la misma función de comprobación aleatoria criptográfica a los datos digitales recibidos, usar la clave pública correspondiente a dicha clave privada para descifrar el valor de comprobación aleatoria comprendido en la firma digital y comparar el valor de comprobación aleatoria descifrado de la firma digital con el valor de comprobación aleatoria generado aplicando la función de comprobación aleatoria criptográfica a los datos digitales recibidos. Si ambos valores de comprobación aleatoria coinciden, esto indica que la información digital no se ha modificado y, de este modo, su integridad no se ha visto comprometida. Además, la autenticidad del remitente/autor de los datos digitales se confirma por medio del sistema criptográfico asimétrico, que asegura que el cifrado usando la clave pública solamente funciona si la información cifrada se cifró con la clave privada que está emparejada matemáticamente con esa clave pública. La representación de la firma digital se puede implementar particularmente usando un transmisor de RFID o un código de barras unidimensional o multidimensional, tal como un código QR o un código DATAMATRIX o simplemente como un número de múltiples dígitos.

El término “función de comprobación aleatoria criptográfica”, como se usa en la presente memoria, se refiere a un tipo especial de función de comprobación aleatoria, es decir, de una función o algoritmo matemático que mapea datos de tamaño arbitrario a una cadena de bits de un tamaño fijo (un valor de comprobación aleatoria), que está diseñado para ser también una función unidireccional, es decir, una función que es fácil de calcular en cada entrada, pero difícil de invertir dada la imagen de una entrada aleatoria. Preferiblemente, la función de comprobación aleatoria criptográfica es una función de comprobación aleatoria denominada “resistente a colisiones”, es decir, una función de comprobación aleatoria que está diseñada de manera que sea difícil, particularmente casi imposible en la práctica, encontrar dos conjuntos de datos diferentes d1 y d2 de manera que comprobación aleatoria(d1) = comprobación aleatoria (d2). Ejemplos destacados de tales funciones de comprobación aleatoria son las funciones de comprobación aleatoria de la familia SHA, por ejemplo, la función SHA-3 o las funciones de comprobación aleatoria de la familia BLAKE, por ejemplo, la función BLAKE2. En particular, se pueden usar las denominadas “funciones de comprobación aleatoria criptográficas probablemente seguras”. Estas son funciones de comprobación aleatoria para las cuales se puede demostrar matemáticamente un cierto nivel de seguridad suficiente.

En algunas realizaciones, almacenar dicho paquete de datos de inicio asegurado en dicho primer almacenamiento de datos implica almacenar el paquete de datos de inicio asegurado en una cadena de bloques o en un libro mayor distribuido sin bloques. De esta forma, el paquete de datos de inicio se puede guardar y almacenar de tal forma que sea sustancialmente imposible sabotearlo, por ejemplo, destruirlo o manipularlo, de una forma no autorizada y, en particular, sin que llegue a ser evidente tal intento de sabotaje. Además, almacenar el paquete de datos de inicio en una cadena de bloques o en un libro mayor distribuido sin bloques permite un fácil acceso al paquete de datos de inicio desde la distancia, por ejemplo, por un destinatario autorizado a lo largo de una cadena de suministro del objeto físico o grupo de objetos relacionados.

(b) Realizaciones seleccionadas con relación en particular a la creación de datos de inicialización

En algunas realizaciones, en una primera variante, el método comprende además: (i) detectar por medio de uno o más sensores al menos una característica discriminatoria de dicho objeto físico o grupo de objetos físicos, para obtener para cada característica discriminatoria datos de identificación respectivos que representen una identidad de dicho objeto físico o grupo de objetos físicos relacionados; y (ii) aplicar una segunda función de comprobación aleatoria criptográfica predeterminada a un conjunto de datos resultante de combinar, según un segundo esquema de combinación predeterminado, el uno o más datos de identificación respectivos obtenidos del conjunto de dicha al menos una característica discriminatoria y los datos de contexto aleatorios para obtener un valor de comprobación aleatoria original.

En una segunda variante, el método comprende además: (i) detectar por medio de uno o más sensores al menos una característica discriminatoria de dicho objeto físico o grupo de objetos físicos para obtener para cada característica discriminatoria datos de identificación respectivos que representan una identidad de dicho objeto físico o grupo de objetos físicos relacionados; (ii) aplicar, a cada uno de dichos datos de identificación, una primera función de comprobación aleatoria criptográfica predeterminada respectiva para obtener un valor de comprobación aleatoria inicial respectivo relacionado con la característica discriminatoria respectiva; (iii) aplicar una segunda función de comprobación aleatoria criptográfica predeterminada a un conjunto de datos resultante de combinar, según un segundo esquema de combinación predeterminado, el uno o más valores de comprobación aleatoria iniciales respectivos obtenidos del conjunto de dicha al menos una característica discriminatoria y los datos de contexto aleatorios para obtener un valor de comprobación aleatoria original (Ho). Por consiguiente, la segunda variante difiere de la primera variante en que se añade el paso (ii) de aplicar la primera función de comprobación aleatoria predeterminada.

En una tercera variante, el método comprende además aplicar una segunda función de comprobación aleatoria criptográfica predeterminada a los datos de contexto aleatorios para obtener un valor de comprobación aleatoria original. Por consiguiente, la tercera variante difiere de la primera y segunda variantes en que no se basa en detectar ninguna característica discriminatoria de dicho objeto físico o grupo de objetos físicos y derivar el valor de comprobación aleatoria original Ho basado en ello. En su lugar, se basa meramente en los datos de contexto aleatorios como entrada esencial.

Para todas de las variantes anteriores, el método comprende además emitir datos de inicialización que representan dicho valor de comprobación aleatoria original respectivo.

Específicamente, el planteamiento según la segunda variante se basa, de este modo, en una pila de comprobación aleatoria que comprende dos niveles de operación de comprobación aleatoria posteriores. El primer nivel se refiere a aplicar una primera función de comprobación aleatoria criptográfica respectiva a los datos de identificación respectivos y el segundo nivel se refiere a aplicar una segunda función de comprobación aleatoria criptográfica respectiva a dicha combinación de dichos valores de comprobación aleatoria iniciales resultantes del primer nivel y dichos datos de contexto aleatorios. El uso tanto de los valores de comprobación aleatoria iniciales derivados de dicha característica discriminatoria como de la información de contexto aumenta la entropía (en el sentido de la teoría de la información y las matemáticas) de los datos de inicialización resultantes. Esto permite un nivel muy alto de seguridad de todo el proceso de autenticación, incluso en los casos donde la entropía individual respectiva de dichos valores de comprobación aleatoria iniciales y/o de la información de contexto esté bastante limitada y no

permitiría en sí misma un nivel de seguridad suficiente. Además, también permite limitar la cantidad de datos involucrados, en particular de los datos que se han de intercambiar, directa o indirectamente, con un destinatario y, de este modo, optimizar la eficiencia o el proceso de autenticación. Con respecto al término “esquema de combinación”, se hace referencia a la definición del mismo proporcionada anteriormente.

La primera y tercera variantes, por otra parte, tienen la ventaja de una menor complejidad en comparación con la primera ventaja y pueden ser especialmente adecuadas para aplicaciones donde es suficiente un grado de seguridad menor que el que se puede lograr con la primera variante.

En algunas realizaciones relacionadas, la característica discriminatoria se proporciona como un conjunto particular de una o más propiedades discriminatorias individuales de dicho objeto físico o grupo de objetos físicos, por medio del cual se puede identificar con seguridad. Tales propiedades pueden comprender particularmente propiedades que son bastante difíciles de sabotear, por ejemplo porque están específicamente aseguradas contra el sabotaje y/o porque son muy difíciles de sabotear, ya en base a su naturaleza. La Solicitud de Patente Europea EP 18 170 047.7 describe en detalle tales características discriminatorias y su uso con el propósito de autenticar objetos.

En realizaciones relacionadas adicionales, la característica de discriminación se proporciona por una característica de seguridad específica añadida o creada específicamente en o sobre dicho objeto físico o grupo de objetos físicos. Esto permite en particular habilitar la autenticación de tales objetos físicos o grupos de objetos físicos que en sí mismos no proporcionan características discriminatorias fiables propias, en las que se podría basar una autenticación segura.

En realizaciones relacionadas adicionales, al menos una de dichas características discriminatorias comprende una función física no clonable, PUF. Además, (i) detectar dicha al menos una característica discriminatoria para obtener los datos de identificación respectivos relacionados con la misma comprende: (i-1) aplicar un desafío respectivo de un esquema de autenticación de desafío-respuesta predeterminado respectivo a la PUF para desencadenar una respuesta por la PUF según dicho esquema de autenticación en reacción a dicho desafío, y (i-2) detectar dicha respuesta respectiva y generar datos de identificación respectivos que representan dicha respuesta; (ii) aplicar una primera función de comprobación aleatoria criptográfica predeterminada respectiva comprende aplicar la primera función de comprobación aleatoria criptográfica predeterminada respectiva a dichos datos que representan dicha respuesta para obtener un valor de comprobación aleatoria inicial relacionado con la PUF respectivo; y (iii) emitir datos de inicialización comprende emitir datos de identificación respectivos relacionados con dicha característica discriminatoria, los datos de identificación que comprenden una representación de dicho valor de comprobación aleatoria inicial relacionado con la PUF respectivo. De esta forma, la característica discriminatoria particular de las funciones físicas no clonables se puede usar como base para habilitar la autenticación de dichos objetos físicos o grupos de objetos físicos, lo que permite un nivel de seguridad incluso mayor debido a la virtualmente imposible clonación de las PUF.

En algunas realizaciones, aplicar dicha segunda función de comprobación aleatoria criptográfica predeterminada para obtener el valor de comprobación aleatoria original comprende además aplicarla igual además de una información de tiempo y ubicación invariables que identifica o que está específicamente relacionada de otro modo con el objeto físico o grupo de objetos físicos, respectivamente. Específicamente, el objeto físico o grupo de objetos físicos puede ser un producto o grupo de productos, respectivamente, y dicha información de tiempo invariable o ubicación invariable puede comprender un número de serie con relación a ese producto o grupo de productos. Aplicar dicha segunda función de comprobación aleatoria criptográfica predeterminada a dicha información de tiempo invariable o ubicación invariable se puede realizar en particular aplicando dicha función de comprobación aleatoria a un conjunto u otra combinación de datos, en donde tal conjunto u otra combinación de datos representa, entre otros, dicha información de tiempo invariable o ubicación invariable. Añadir dicha información de tiempo y ubicación invariables a los datos a los que se aplica la segunda función de comprobación aleatoria criptográfica predeterminada añade incluso más entropía y, de este modo, puede incluso aumentar la seguridad alcanzable del proceso de autenticación general. La información de tiempo y ubicación invariables, tal como por ejemplo uno o más números de serie, se puede representar particularmente mediante una marca en el objeto físico o grupo de objetos físicos y/o se puede implementar usando un transmisor de RFID o un código de barras unidimensional o multidimensional, tal como un código QR o un código DATAMATRIX o simplemente como un número de múltiples dígitos.

En algunas realizaciones, emitir dichos datos de inicialización comprende uno o más de los siguientes: (i) añadir una representación de dichos datos de inicialización a dicho objeto físico o grupo de objetos físicos; (ii) almacenar dicha representación de dichos datos de inicialización o hacerlos que se almacenen en un tercer almacenamiento de datos y añadir a dicho objeto físico o grupo de objetos físicos una representación de un puntero que indica dónde se puede acceder a dichos datos de inicialización en el tercer almacenamiento de datos. Este tercer almacenamiento de datos puede ser igual o diferente de dicho primer almacenamiento de datos mencionado anteriormente. Ambas de estas opciones (i) y (ii) permiten una forma particularmente sencilla de comunicar dichos datos de inicialización a destinatarios adicionales a lo largo de una cadena de suministro para el objeto físico o grupo de objetos físicos. Específicamente, no se ha de establecer ningún enlace de comunicación directa, tal como un intercambio electrónico de datos, entre un proveedor y el destinatario respectivo de dichos objetos o grupo de objetos.

(c) Realizaciones seleccionadas con relación en particular a preparar una autenticación posterior adicional por un destinatario adicional

En algunas realizaciones, el método comprende además: (i) recibir una solicitud de determinación de un paquete de datos de inicio asegurados adicional con relación a datos de contexto predichos adicionales que representan una ubicación futura predicha adicional con relación a un siguiente destinatario designado adicional diferente del objeto físico o grupo de objetos físicos y un tiempo futuro relacionado de presencia del objeto físico o grupo de objetos físicos en esa ubicación futura adicional; y (ii) realizar el presente método en base a esos datos de contexto predichos adicionales para determinar y almacenar, o hacerlos que sean almacenados, dicho paquete de datos de inicio asegurados adicional solicitado con relación a datos de contexto predichos adicionales. Este planteamiento habilita un reenvío de los objetos físicos o grupo de objetos físicos a lo largo de una cadena de suministro de tal forma que tal siguiente destinatario designado adicional pueda solicitar a un nodo anterior respectivo a lo largo de la cadena de suministro que está adaptado para realizar el método según estas realizaciones que genere un paquete de datos de inicio asegurados respectivo para un siguiente salto a lo largo de la cadena de suministro que comienza en ese siguiente destinatario designado adicional. Por consiguiente, no todos los nodos a lo largo de la cadena de suministro tienen que ser capaces de preparar la autenticación en un destinatario adicional más, sino que en su lugar a tal nodo anterior, que en particular puede jugar el papel de una autoridad central o general para gestionar la determinación y el almacenamiento de paquetes de datos de inicio asegurados adicionales, se le puede solicitar que realice esa preparación en su lugar y proporcionar un paquete de datos de inicio asegurados respectivo para dicho siguiente salto. Específicamente, el paquete de datos de inicio adicional solicitado se puede determinar en base, además de los datos de contexto predichos respectivos, a datos de contexto aleatorios recién generados o a datos de contexto aleatorios determinados anteriormente en el curso de la determinación de un paquete de datos de inicio respectivo para un destinatario anterior.

En algunas realizaciones relacionadas, el método comprende además almacenar el paquete de datos de inicio adicional resultante o hacer que sea almacenado en un almacenamiento de datos que es accesible por el siguiente destinatario designado adicional. Específicamente, sin limitación, dicho almacenamiento de datos puede ser dicho primer almacenamiento de datos mencionado anteriormente. Almacenar el paquete de datos de inicio adicional resultante en dicho almacenamiento de datos proporciona una forma eficiente de ponerlo a disposición de dicho siguiente destinatario solicitante de una forma donde no se necesita ningún enlace de comunicación directo entre el nodo que proporciona el paquete de datos de inicio y el siguiente destinatario solicitante. En particular, el almacenamiento de datos puede ser de nuevo una cadena de bloques o un libro mayor distribuido sin bloques, lo que proporciona un nivel de seguridad muy alto contra el sabotaje de ese paquete de datos de inicio adicional por terceros no autorizados.

(d) Realizaciones con relación en particular a la firma digital del valor de comprobación aleatoria original

En algunas realizaciones, el método comprende además: (i) firmar dicho valor de comprobación aleatoria original obtenido con una firma digital perteneciente a un proveedor de dicho objeto físico o grupo de objetos físicos al siguiente destinatario respectivo; y (ii) incluir dicha firma digital en los datos de inicialización respectivos de salida o datos de inicialización adicionales, respectivamente. En particular, el proveedor puede ser un proveedor original o un proveedor intermediario a lo largo de la cadena de suministro para dicho objeto físico o grupo de objetos físicos. Por consiguiente, los datos de inicialización respectivos se refieren a los datos de inicialización originales en el caso de un proveedor original y a los datos de inicialización adicionales respectivos en el caso de un proveedor intermediario. Añadir una firma digital aumenta aún más el nivel de seguridad, porque proporciona una posibilidad segura de verificar, por el destinatario respectivo, la autenticidad del valor de comprobación aleatoria original firmado en los datos de inicialización de salida.

(e) Sistema para preparar una autenticación asegurada posterior

Un segundo aspecto de la presente solución global se refiere a un sistema para preparar una autenticación asegurada posterior de un objeto físico o grupo de según el primer aspecto de la presente solución global. Específicamente, el sistema se puede adaptar para realizar este método según una cualquiera o más de sus realizaciones descritas en la presente memoria. Por consiguiente, la descripción de este método y sus realizaciones y sus ventajas se aplica cambiando lo que se deba de cambiar a este sistema.

2. Método de autenticación de un objeto físico o grupo de objetos físicos

Un tercer aspecto de la presente solución global se refiere a un método de autenticación de un objeto físico o un grupo de objetos físicos. En particular, el método comprende diferentes variantes alternativas y se puede implementar como un método implementado por ordenador.

El método comprende:

(i) recibir y descifrar un paquete de datos de inicio asegurados que representa datos de contexto cifrados que representan una ubicación y un tiempo relacionado para recuperar dichos datos de contexto;

(ii) recibir o determinar datos de contexto actuales que representan una ubicación actual del objeto físico o grupo de objetos físicos y un tiempo actual relacionado de presencia del objeto físico o grupo de objetos físicos en esa ubicación actual;

(iii) combinar, según un esquema de combinación predeterminado, los datos de contexto actuales con los datos de contexto descifrados para determinar por ello los datos de contexto de prueba, en donde el esquema de combinación define una operación inversa a una operación de combinación correspondiente usada previamente para generar los datos de contexto recibidos;

(iv) acceder a los datos de inicialización relacionados con dicho objeto físico o grupo de objetos físicos para recuperar de ellos un valor de comprobación aleatoria original que se representa por los datos de inicialización.

El método comprende además, según dichas diferentes variantes, (v) uno de los siguientes procesos a) a c):

a) Detectar, por medio de uno o más sensores, al menos una característica discriminatoria de dicho objeto físico o grupo de objetos físicos para obtener datos de identificación respectivos relacionados con dicha característica discriminatoria respectiva, estos datos de identificación que representan una identidad supuesta de dicho objeto físico o grupo de objetos físicos relacionados; y

generar un valor de comprobación aleatoria de prueba mediante la aplicación de una segunda función de comprobación aleatoria criptográfica predeterminada a una combinación, según un esquema de combinación predeterminado adicional, de los datos de contexto de prueba y cada uno de dichos datos de identificación y preferiblemente una información de tiempo invariable y ubicación invariable que identifica o que está de otro modo específicamente relacionada con dicho objeto físico o grupo de objetos físicos; o

b) Detectar, por medio de uno o más sensores, al menos una característica discriminatoria de dicho objeto físico o grupo de objetos físicos para obtener datos de identificación respectivos relacionados con dicha característica discriminatoria respectiva, estos datos de identificación que representan una identidad supuesta de dicho objeto físico o grupo de objetos físicos relacionados;

aplicar una primera función de comprobación aleatoria criptográfica predeterminada respectiva a los datos de identificación respectivos para obtener un valor de comprobación aleatoria inicial respectivo relacionado con dicha característica discriminatoria; y

generar un valor de comprobación aleatoria de prueba mediante la aplicación de una segunda función de comprobación aleatoria criptográfica predeterminada a una combinación, según un esquema de combinación predeterminado adicional, de los datos de contexto de prueba y cada uno de dichos valores de comprobación aleatoria iniciales, y preferiblemente una información de tiempo invariable y ubicación invariable que identifica o que está de otro modo específicamente relacionada con dicho objeto físico o grupo de objetos físicos;

c) generar un valor de comprobación aleatoria de prueba mediante la aplicación de una segunda función de comprobación aleatoria criptográfica predeterminada a los datos de contexto de prueba o a una combinación, según un esquema de combinación predeterminado adicional, de los datos de contexto de prueba y una información de tiempo invariable y ubicación invariable que identifica o que está de otro modo específicamente relacionada con dicho objeto físico o grupo de objetos físicos.

Para cada uno de los procesos anteriores a) a c), la segunda función de comprobación aleatoria criptográfica predeterminada es igual a una función de comprobación aleatoria criptográfica correspondiente usada anteriormente para determinar el valor de comprobación aleatoria original representado por los datos de inicialización, y en donde dicho esquema de combinación adicional es igual a un esquema de combinación correspondiente usado anteriormente para determinar el valor de comprobación aleatoria original representado por los datos de inicialización.

El método comprende además: (vi) generar un primer resultado de lectura que comprende (vi-1) una representación del valor de comprobación aleatoria de prueba y una representación del valor de comprobación aleatoria original, o (vi-2) una salida de coincidencia que indica si, según al menos un criterio de coincidencia predeterminado, el valor de comprobación aleatoria de prueba coincide o no con dicho valor de comprobación aleatoria original y, de este modo, indica la autenticidad del objeto físico o grupo de objetos físicos.

En caso de que uno cualquiera o más de los pasos anteriores del método falle por cualquier razón, por ejemplo, si no se puede acceder con éxito a los datos de inicialización o no se puede leer el paquete de datos de inicio asegurados, el primer resultado de lectura puede comprender o consistir particularmente en una salida que indica un fallo de autenticación.

Este método de autenticación (método de autenticación) se relaciona con el método del primer aspecto de la presente solución global (método de preparación) en que este último sirve para preparar una autenticación posterior de un objeto físico o grupo de objetos físicos según este método de autenticación según el tercer aspecto de la presente solución global. Además, este método de autenticación se basa en el concepto de que la autenticación se

puede realizar comparando dos valores de comprobación aleatoria, uno de los cuales fue generado previamente por otra entidad por medio de dicho método de preparación de una autenticación posterior según el primer aspecto, y el otro de los cuales se produce por el destinatario de autenticación respectivo en sí mismo en base tanto al paquete de datos de inicio seguros relacionado proporcionado como resultado de dicho método de preparación como a los datos de identificación que se derivan del objeto físico o grupo de objetos a ser autenticados.

Por consiguiente, el paquete de datos de inicio proporciona información con relación a los datos de contexto predichos del destinatario, es decir, en particular, la ubicación y el tiempo, dónde y cuándo el destinatario se supone que recibe dicho objeto físico o grupo de objetos físicos, y el método de autenticación usa entonces este paquete de datos de inicio, el valor de comprobación aleatoria original recibido generado por el método de preparación, sus datos de contexto actuales y para las variantes de proceso a) y b), además de los datos de identificación (o valores de comprobación aleatoria iniciales correspondientes) derivados de una detección de la una o más características discriminatorias del objeto físico o grupo de objetos físicos para generar un valor de comprobación aleatoria de prueba. Si el objeto físico o grupo de objetos físicos es original y se recibe en el destinatario en la ubicación y tiempo predichos (al menos dentro de algún margen de tolerancia definido que puede corresponder particularmente a la precisión de la determinación de los datos de contexto predichos y los datos de contexto actuales) el valor de comprobación aleatoria de prueba será una reconstrucción exitosa del valor de comprobación aleatoria original generado por el método de preparación y, por consiguiente, el segundo y los valores de comprobación aleatoria de prueba derivados por el método de autenticación coincidirán, indicando de este modo una autenticación exitosa. De otro modo, la autenticación falla. El proceso de comparar los valores de comprobación aleatoria originales y de prueba se puede realizar automática o manualmente en base a los valores de salida de estos dos valores de comprobación aleatoria.

(a) Realizaciones seleccionadas con relación en particular a la obtención de los datos de identificación

En algunas realizaciones, al menos una de dichas características discriminatorias comprende una función física no clonable, PUF, y detectar dicha característica discriminatoria para obtener los datos de identificación respectivos relacionados con la misma comprende: (i) aplicar un desafío respectivo de un esquema de autenticación de desafío-respuesta predeterminado respectivo a la PUF para desencadenar una respuesta según dicho esquema de autenticación en reacción a dicho desafío; y (ii) detectar una respuesta respectiva por la PUF de acuerdo con el esquema de autenticación de desafío-respuesta respectivo en reacción al desafío y derivar a partir de la misma dichos datos de identificación respectivos. Dado que las PUF son por sí mismas virtualmente imposibles de clonar o reconstruir de otro modo, su uso aumenta aún más el nivel de seguridad alcanzable de la solución de autenticación global.

En algunas realizaciones, obtener los datos de identificación comprende: (i) detección basada en sensores de una o más características discriminatorias de dicho objeto físico o grupo de objetos físicos; (ii) generar datos de objeto que representen dicha una o más características discriminatorias de dicho objeto físico o grupo de objetos físicos; (iii) comunicar dichos datos de objeto a un sistema para el reconocimiento automático de objetos; y (iv) recibir los datos de identificación firmados digitalmente de dicho sistema en respuesta a dicha comunicación de dichos datos de objeto. Estas realizaciones se relacionan particularmente con un método de autenticación, tal como los descritos en el documento EP 18 170 047.7, donde particularmente una o más características de un objeto físico o grupo de objetos físicos a ser autenticados, cuyas características forman parte de los objetos o grupo de objetos por sí mismos y no necesitan ser añadidos como una característica de seguridad separada, forman la base de identificación y, de este modo, autenticar el objeto o grupo de objetos. En este caso, dicho sistema para el reconocimiento automático de objetos típicamente es diferente del destinatario en sí mismo y está adaptado para recibir los datos de objeto y a cambio proporcionar un resultado de reconocimiento de objeto en forma de datos de identificación firmados digitalmente.

En algunas realizaciones, dicho objeto físico o grupo de objetos físicos comprende una marca. La marca comprende una representación de dichos datos de inicialización y/o una representación de un puntero que indica una ubicación donde se puede acceder a dichos datos de inicialización; y acceder a dichos datos de inicialización comprende, según sea aplicable: (i) leer la representación de dichos datos de inicialización en la marca, o (ii) leer la representación del puntero en la marca y adquirir los datos de inicialización de una ubicación de almacenamiento de datos indicada por el puntero; y si los datos de inicialización comprenden una firma digital, verificar el proveedor respectivo de dicho objeto físico o grupo de objetos físicos en base a una verificación de dicha firma digital. Por consiguiente, estas realizaciones son particularmente útiles cuando la marca sirve para comunicar los datos de inicialización, directa o indirectamente a través del puntero, a un destinatario como entrada al método de autenticación. De esta forma, los datos de inicialización se transportan por el objeto o grupo de objetos en sí mismo, de modo que no necesita ser establecido ningún canal de comunicación adicional desde el proveedor respectivo hasta el siguiente destinatario respectivo.

(b) Realizaciones seleccionadas con relación en particular a la salida y el almacenamiento de datos con relación a la autenticación

En algunas realizaciones, el método comprende además emitir una representación de dichos datos de contexto actuales o un subconjunto de los mismos o información derivada de los mismos, como un segundo resultado de

lectura. Por consiguiente, el segundo resultado de lectura puede representar en particular datos con relación a la gestión de la cadena de suministro, en la medida que indica datos de contexto que describen una ubicación y un tiempo en los que el objeto o grupo de objetos está o estuvo presente en el destinatario actual que define un nodo a lo largo de la cadena de suministro. De este modo, el método de autenticación sirve al mismo tiempo como fuente de datos de gestión de la cadena de suministro.

En algunas realizaciones, el método comprende además un proceso de almacenamiento que comprende almacenar el primer resultado de lectura, o hacerlo que sea almacenado, en un bloque de una cadena de bloques de un primer conjunto de una o más cadenas de bloques o en uno o más nodos de un libro mayor distribuido sin bloques de un primer conjunto de uno o más libros mayores distribuidos sin bloques. En particular, hacer que el primer resultado de lectura sea almacenado puede comprender hacer que otro dispositivo, tal como un ordenador separado y, opcionalmente, incluso ubicado de manera remota, esté configurado para realizar (i) minería de cadenas de bloques o (ii) escribir en un nodo de un libro mayor distribuido sin bloques, respectivamente, para almacenar el primer resultado de lectura en consecuencia. Estas realizaciones permiten un almacenamiento seguro y fiable con una integridad de datos muy alta, de manera que sea esencialmente imposible manipular o borrar o sabotear de otro modo o perder tales datos, por ejemplo, debido a la eliminación involuntaria o deliberada o debido a la corrupción de datos. De este modo, el historial de autenticación completo permanece disponible. Además, se puede acceder a la información almacenada dondequiera que esté disponible el acceso al libro mayor distribuido de cadena de bloques respectivamente. Esto permite un almacenamiento y acceso seguro y distribuido a los datos almacenados, por ejemplo, con propósitos de verificación de integridad, tales como verificar si un proveedor de un producto (objeto) fue de hecho el autor del producto o no. En base a esta realización, el mundo físico, al que pertenecen los objetos, se puede conectar al poder de la tecnología de cadena de bloques o de libro mayor distribuido sin bloques. De este modo, se puede lograr un alto grado de trazabilidad del origen y la cadena de suministro de objetos físicos, tales como productos.

En algunas realizaciones relacionadas, (i) la detección de características discriminatorias del objeto físico o grupo de objetos físicos comprende detectar una pluralidad de diferentes de tales características discriminatorias para obtener en base a ello para cada una de las características discriminatorias el conjunto individual respectivo de datos de identificación que representan el objeto físico o grupo de objetos físicos; (ii) generar el valor de comprobación aleatoria de prueba se realiza para cada uno de los conjuntos individuales de datos de identificación por separado tal como para obtener para cada uno de los conjuntos individuales de datos de identificación un valor de comprobación aleatoria de prueba individual respectivo; (iii) generar el primer resultado de lectura se realiza para cada uno de los valores de comprobación aleatoria de prueba individuales por separado tal como para obtener para cada una de las características discriminatorias un primer resultado de lectura individual respectivo; y (iv) el proceso de almacenamiento comprende almacenar cada uno de dichos primeros resultados de lectura individuales respectivamente haciendo que se almacene en un bloque de una cadena de bloques dedicada individual respectiva en dicho primer conjunto de cadenas de bloques o en uno o más nodos de un libro mayor distribuido sin bloques dedicado individual respectivo en dicho primer conjunto de libros mayores distribuidos sin bloques. De esta forma, se puede aumentar aún más la seguridad alcanzable, porque por una parte están involucradas características discriminatorias adicionales del objeto físico o grupo de objetos físicos, lo que aumenta la dificultad de falsificación del mismo y, por otra parte, los primeros resultados de lectura individuales se almacenan en diferentes cadenas de bloques dedicadas individuales, lo que aumenta la dificultad de manipular o, de otro modo, comprometer de una forma no autorizada el seguimiento de datos relacionados almacenado en el entorno de la cadena de bloques o el entorno del libro mayor distribuido sin bloques respectivo. En algunas variantes, estas realizaciones se pueden implementar además en cualquiera de los procesos a) y b) descritos anteriormente.

En algunas realizaciones relacionadas adicionales, el proceso de almacenamiento comprende además almacenar dicho segundo resultado de lectura o hacerlo que sea almacenado, respectivamente, en un bloque de una cadena de bloques de un segundo conjunto de una o más cadenas de bloques, la cadena de bloques que está separada de las cadenas de bloques en el primer conjunto de cadenas de bloques, o en uno o más nodos de un libro mayor distribuido sin bloques de un segundo conjunto de uno o más libros mayores distribuidos sin bloques, el libro mayor distribuido sin bloques que está separado de los libros mayores distribuidos sin bloques en el primer conjunto de libros mayores distribuidos sin bloques, respectivamente. Estas realizaciones permiten almacenar adicionalmente y, de este modo, guardar el segundo resultado de lectura independientemente del primer resultado de lectura, en otra cadena de bloques respectiva, proporcionando de este modo las ventajas tratadas en conexión con la realización inmediatamente anterior también en relación con el segundo resultado de lectura. Usar diferentes cadenas de bloques o libros mayores distribuidos sin bloques para el primer y segundo resultados de lectura proporciona además la ventaja de soportar fácilmente una combinación de una (segunda) cadena de bloques existente o un libro mayor distribuido sin bloques, respectivamente, para el segundo resultado de lectura con una primera cadena de bloques o libro mayor distribuido sin bloques adicional, respectivamente, para el primer resultado de lectura. Por consiguiente, se pueden habilitar fácilmente diferentes derechos de acceso y la gestión de las cadenas de bloques puede estar en manos de diferentes autoridades. En particular, estas realizaciones se pueden usar para verificar tanto si un proveedor de un producto fue de hecho su autor como si la cadena de suministro fue como se esperaba o no. Además, esto se puede utilizar para aumentar aún más la seguridad alcanzable, porque la información de contexto se puede usar para identificar retroactivamente las ubicaciones o las personas que están involucradas en la

cadena de suministro, donde podría haber ocurrido un fraude potencial, así como las fechas o intervalos de tiempo potenciales relacionados.

En algunas realizaciones relacionadas adicionales, donde el proceso de almacenamiento se relaciona con cadenas de bloques:

(i) almacenar un primer resultado de lectura individual respectivo en un bloque de una cadena de bloques respectiva en el primer conjunto de cadenas de bloques comprende además almacenar un puntero de cadena de bloques cruzadas que mapea lógicamente dicho bloque de dicha cadena de bloques en el primer conjunto de cadenas de bloques a un bloque correspondiente de una cadena de bloques respectiva en el segundo conjunto de cadenas de bloques, en dicho bloque de dicha cadena de bloques en el primer conjunto de cadenas de bloques; y

(ii) almacenar dicho segundo resultado de lectura en un bloque de la cadena de bloques en el segundo conjunto de cadenas de bloques comprende además almacenar un puntero de cadenas de bloques cruzadas, que mapea lógicamente dicho bloque de dicha cadena de bloques en el segundo conjunto de cadenas de bloques a un bloque correspondiente de una cadena de bloques respectiva en el primer conjunto de cadenas de bloques, en dicho bloque de dicha cadena de bloques en el segundo conjunto de cadenas de bloques.

De manera similar, en algunas realizaciones relacionadas adicionales, donde el proceso de almacenamiento se relaciona con libros mayores distribuidos sin bloques:

(i) almacenar un primer resultado de lectura individual respectivo en un nodo de un libro mayor distribuido sin bloques respectivo en el primer conjunto de libros mayores distribuidos sin bloques comprende almacenar un puntero de libro mayor cruzado que mapea lógicamente el nodo de dicho libro mayor distribuido sin bloques en el primer conjunto de libros mayores distribuidos sin bloques a un nodo correspondiente del libro mayor distribuido sin bloques respectivo en el segundo conjunto de libros mayores distribuidos sin bloques, al nodo de dicho libro mayor distribuido sin bloques en el primer conjunto de libros mayores distribuidos sin bloques; y

(ii) almacenar dicho segundo resultado de lectura en un nodo del libro mayor distribuido sin bloques respectivo en el segundo conjunto de libros mayores distribuidos sin bloques comprende además almacenar un puntero de cadena de bloques cruzada, que mapea lógicamente dicho nodo del libro mayor distribuido sin bloques respectivo en el segundo conjunto de libros mayores distribuidos sin bloques a un nodo correspondiente del libro mayor distribuido sin bloques respectivo en el primer conjunto de libros mayores distribuidos sin bloques, en dicho bloque de dicho libro mayor distribuido sin bloques en el segundo conjunto de libros mayores distribuidos sin bloques.

De esta forma, las cadenas de bloques o los libros mayores distribuidos sin bloques del primer conjunto de cadenas de bloques o libros mayores distribuidos sin bloques, respectivamente, se pueden interconectar mediante los punteros de cadenas de bloques cruzadas o los punteros de libros mayores cruzados, respectivamente, al segundo conjunto de cadenas de bloques o libros mayores distribuidos sin bloques, respectivamente, y viceversa. Esto se puede usar para aumentar aún más el nivel de seguridad alcanzable de la presente solución de autenticación de objetos. En particular, esto se puede usar para rastrear intentos de sabotaje o falsificación de objetos en diferentes puntos a lo largo de una cadena de suministro. Por ejemplo, esta realización permite rastrear una ubicación y/o un punto en el tiempo de tal intento.

(c) Realizaciones seleccionadas con relación en particular a la determinación de datos de inicialización adicionales para una autenticación asegurada posterior más

En algunas realizaciones relacionadas adicionales, el método comprende además determinar un paquete de datos de inicio asegurados adicional y, opcionalmente, datos de inicialización relacionados adicionales para una autenticación asegurada posterior más de dicho objeto físico o grupo de objetos físicos en un destinatario adicional más del mismo. Estas realizaciones se refieren a una posible variante de habilitar una o más autenticaciones aseguradas posteriores adicionales más de dicho objeto físico o grupo de objetos físicos por destinatarios adicionales a lo largo de una cadena de suministro. De hecho, según esta variante, el proceso descrito aquí se repite esencialmente para cada siguiente paso de distribución, es decir, salto, a lo largo de la cadena de suministro, de manera que para cada tal salto se generen nuevos datos de inicialización dedicados y se usen para la siguiente autenticación posterior en el siguiente destinatario. Esto tiene la ventaja de que se pueden reutilizar los mismos procesos para múltiples saltos a lo largo de la cadena de suministro.

En algunas realizaciones relacionadas, determinar dicho paquete de datos de inicio asegurados adicional (y opcionalmente dichos datos de inicialización adicionales) comprende emitir una solicitud para determinar tal paquete de datos de inicio asegurados adicional (y opcionalmente dichos datos de inicialización adicionales) para una autenticación asegurada posterior más de dicho objeto físico o grupo de objetos físicos en un destinatario adicional más del mismo a un proveedor autorizado de dicho paquete de datos de inicio asegurados adicional (y opcionalmente dichos datos de inicialización adicionales) y recibir, por ejemplo, a través de una cadena de bloques o libro mayor distribuido u otro almacenamiento, dicho paquete de datos de inicio asegurados adicional solicitado (y opcionalmente dichos datos de inicialización adicionales) en respuesta a la solicitud. Esto permite, en particular, centralizar la determinación del paquete de datos de inicio asegurados adicional (y opcionalmente dichos datos de inicialización adicionales) para múltiples saltos a lo largo de una cadena de suministro en una única entidad,

proporcionando de este modo una eficiencia particularmente alta. El proveedor central autorizado puede coincidir particularmente con la entidad que realiza la determinación inicial, es decir, la primera, del primer paquete de datos de inicio asegurados adicional respectivo (y opcionalmente dichos datos de inicialización adicionales) al comienzo de una cadena de suministro, por ejemplo, el fabricante original o distribuidor del objeto u objetos físicos suministrados y autenticados a lo largo de la cadena de suministro.

En algunas realizaciones alternativas, determinar dicho paquete de datos de inicio asegurados adicional comprende realizar el método del primer aspecto, de manera que los datos de contexto predichos representen una ubicación futura predicha de un siguiente destinatario designado adicional del objeto físico o grupo de objetos físicos y un tiempo de presencia futuro relacionado del objeto físico o grupo de objetos físicos en esa ubicación futura. Según estas realizaciones, cada destinatario actual respectivo del objeto físico o grupo de objetos determina por sí mismo el paquete de datos de inicio asegurados para el siguiente destinatario respectivo, es decir, para el siguiente salto respectivo, a lo largo de la cadena de suministro. Esto tiene la ventaja de que ninguna entidad central autorizada necesita hacerse cargo de determinar todo el paquete de datos de inicio asegurados para los múltiples saltos respectivos a lo largo de la cadena de suministro y, por consiguiente, no necesitan estar presentes enlaces de comunicación respectivos entre los destinatarios y tal autoridad central.

En algunas realizaciones relacionadas, el método comprende además, realizando el método del primer aspecto según las realizaciones relacionadas con relación a la determinación de los datos de inicialización, determinar datos de inicialización adicionales en base a los mismos datos de contexto aleatorios que dicho paquete de datos de inicio asegurados adicional y almacenar o hacer que se almacenen dichos datos de inicialización adicionales. A este respecto, los datos de contexto predichos representan una ubicación futura predicha de un siguiente destinatario designado adicional del objeto físico o grupo de objetos físicos y un tiempo de presencia futuro relacionado del objeto físico o grupo de objetos físicos en esa ubicación futura. Por consiguiente, según estas realizaciones, en lugar de reutilizar el paquete de datos de inicio seguros existente anteriormente, se usa un nuevo paquete de datos de inicio seguros generado para al menos la siguiente autenticación posterior. Opcionalmente, se determinan incluso unos nuevos (es decir, adicionales) datos de inicialización, por ejemplo, en base a nuevos datos de contexto aleatorios. Estas diversas medidas pueden aumentar aún más, solas o en combinación, el nivel de seguridad alcanzable, porque la entropía del proceso de autenticación global aumenta aún más.

(d) Sistema de autenticación de objeto

Un cuarto aspecto de la presente solución global se refiere a un sistema de autenticación de objetos que se adapta para realizar el método del tercer aspecto, preferiblemente según una cualquiera o más de sus realizaciones descritas en la presente memoria.

En algunas realizaciones, el sistema de autenticación de objetos se adapta además para realizar el método del primer aspecto.

(e) Programa informático

Un quinto aspecto de la presente solución global se refiere a un programa informático que comprende instrucciones que, cuando se ejecutan en uno o más procesadores de un sistema de autenticación de objetos, tal como el que es según el cuarto aspecto, hace que se realice el método de autenticación según el tercer aspecto de la presente solución global.

3. Método y sistema para proporcionar de manera segura un esquema de combinación variable en el tiempo

Un sexto aspecto de la presente solución global se refiere a un método para proporcionar de manera segura un esquema de combinación variable en el tiempo para autenticar un objeto físico o un grupo de objetos físicos según el método de autenticación del tercer aspecto, que comprende: (i) Recibir y almacenar datos que representan el esquema de combinación predeterminado, una información de tiempo y ubicación invariables que identifica o que está específicamente relacionada de otro modo con dicho objeto físico o grupo de objetos físicos, y metadatos que definen un período de validez limitado del esquema de combinación CS; (ii) Recibir una solicitud del esquema de combinación y la información de identidad que identifique o esté específicamente relacionada de otro modo con un objeto físico o grupo de objetos físicos de un sistema solicitante; (iii) Autenticar el sistema solicitante, por ejemplo, por medio de un esquema de autenticación de dos factores; y (iv-1). Si el sistema solicitante se autentica con éxito como que está autorizado y según los metadatos almacenados anteriormente correspondientes a la información de identidad recibida, el esquema de combinación relacionado al que pertenecen los metadatos todavía es válido, emitir datos que representan ese esquema de combinación relacionado a través de un canal de datos que está asegurado contra interceptación al sistema solicitante; y (iv-1) de otro modo, denegar la solicitud.

De esta forma, uno o más de los esquemas de combinación que se usan en los métodos y sistemas de los otros aspectos de la presente solución global se pueden proporcionar de manera segura a los nodos relevantes (sistemas solicitantes) a lo largo de la cadena de suministro, que tienen la necesidad de autenticar los objetos físicos o grupos de objetos físicos. En particular, esto permite usar uno o más esquemas de combinación variables en el tiempo con períodos de validez limitados para tales autenticaciones, que se pueden usar para aumentar aún más el nivel de seguridad alcanzable de la solución de autenticación global.

Aspectos adicionales se refieren a un sistema y un programa informático, respectivamente, para realizar el método del sexto aspecto.

Cada uno de los programas informáticos descritos en la presente memoria se puede implementar en particular en forma de un soporte de datos en el que se almacenan uno o más programas para realizar el método. Preferiblemente, este es un soporte de datos, tal como un CD, un DVD o un módulo de memoria rápida. Esto puede ser ventajoso, si el producto de programa informático está destinado a ser distribuido como un producto individual independiente de la plataforma de procesador en la que se han de ejecutar el uno o más programas. En otra implementación, el producto de programa informático se proporciona como un archivo en una unidad de procesamiento de datos, en particular en un servidor, y se puede descargar a través de una conexión de datos, por ejemplo, Internet o una conexión de datos dedicada, tal como una red de área local o propietaria.

Breve descripción de los dibujos

Ventajas, características y aplicaciones adicionales de la presente solución global se proporcionan en la siguiente descripción detallada y las figuras adjuntas, en donde:

La Fig. 1 ilustra esquemáticamente una descripción general del sistema ejemplar de una solución de seguridad global que comprende las realizaciones preferidas respectivas de diversos aspectos de la presente solución global;

Las Figs. 2A y 2B muestran un diagrama de flujo que ilustra una realización preferida de una primera fase de un método de preparación de una autenticación asegurada posterior de un objeto físico o grupo de objetos físicos por un destinatario del mismo según la presente solución global;

Las Figs. 3A y 3B muestran un diagrama de flujo que ilustra una primera realización preferida de la segunda fase del método de preparación de una autenticación asegurada posterior según la presente solución global;

Las Figs. 4A y 4B muestran un diagrama de flujo que ilustra una segunda realización preferida de la segunda fase del método de preparación de una autenticación asegurada posterior según la presente solución global;

Las Figs. 5A y 5B muestran un diagrama de flujo que ilustra una primera realización preferida de un método de autenticación de un objeto físico o un grupo de objetos físicos según la presente solución global, que está configurado para ser usado en conexión con el método de las Figs. 2 y 3;

Las Figs. 6A y 6B muestran un diagrama de flujo que ilustra una segunda realización preferida de un método de autenticación de un objeto físico o un grupo de objetos físicos según la presente solución global, que está configurado para ser usado en conexión con el método de las Figs. 2 y 4;

La Fig. 7 muestra un diagrama de flujo que ilustra una realización preferida de un método de uso de uno o más esquemas de combinación variables en el tiempo en conexión con los métodos de las Figs. 3A/3B a 6A/6B; y

Las Figs. 8A y 8B ilustran diversas opciones diferentes de habilitación de pasos de suministro (saltos) adicionales a lo largo de una cadena de suministro usando cadenas de bloques como almacenamientos de datos en conexión con uno o más de los métodos descritos anteriormente con respecto a las Figs. 2 a 7.

En las figuras, se usan líneas y contornos discontinuos para ilustrar variantes adicionales, opcionales, de los sistemas y métodos respectivos. Además, los mismos signos de referencia en diferentes figuras se refieren a las mismas o correspondientes características. Se ha de entender que las figuras meramente describen realizaciones específicas y que una o más características o pasos descritos en las mismas pueden ser de hecho opcionales, incluso si no están marcados con líneas discontinuas o que se describen explícitamente como “opcionales”.

Descripción detallada de realizaciones preferidas

La Fig. 1 ilustra esquemáticamente una descripción general del sistema ejemplar de una solución de seguridad global 10 con relación a una cadena de suministro que tiene los nodos A, B y C y, opcionalmente un nodo B' adicional. Por ejemplo, A puede relacionarse con un fabricante de productos originales que suministra un objeto físico PO o un grupo de objetos físicos PO, en lo sucesivo denominados colectivamente PO(s), es un producto o grupo de productos, respectivamente. En principio, este puede ser cualquier tipo de producto o productos y, en particular, estos productos pueden ser productos farmacéuticos o dispositivos médicos. Por consiguiente, la presente solución global es sustancialmente independiente del tipo de objetos físicos a los que se aplica. El nodo B puede ser un sitio de logística, tal como un almacén, de un mayorista intermedio, y C puede ser un punto de venta, por ejemplo, una tienda, donde los PO(s) distribuidos a lo largo de la cadena de suministro se venden finalmente a los clientes finales. El nodo adicional B’ puede pertenecer comercialmente a B y puede ser, por ejemplo, un almacén alternativo que se sitúa remoto a B, de manera que B pueda elegir tener los PO(s) entregados por A o bien al almacén B o bien al almacén B’.

Al principio del proceso de suministro, el proveedor A usa un sistema de preparación 20, que puede comprender particularmente un ordenador y medios para emitir un desafío a una PUF perteneciente los PO(s) y uno o más sensores para detectar una respuesta generada por la PUF en reacción al desafío. Alternativamente o además, el

sistema de preparación 20 puede comprender un sistema de cámara configurado para crear una o más imágenes de los PO(s) y enviarlas a un sistema de reconocimiento de objetos que está configurado para reconocer los PO(s) en base a dicha una o más imágenes y devolver un resultado de reconocimiento respectivo que comprende al menos una característica discriminatoria de dichos PO(s) al sistema de preparación 20, por ejemplo como se describe en detalle en la Solicitud de Patente Europea EP 18 170 044.4.

El sistema de preparación 20 está configurado para realizar el método ilustrado en la Fig. 2 en combinación con la Fig. 3 o la Fig. 4. Como se describirá en detalle a continuación con referencia a estas figuras, el sistema de preparación 20 genera, mientras que se realizan estos métodos, un paquete de datos de inicio asegurado SSDP y lo almacena o hace que sea almacenado en un primer almacenamiento de datos DS1. Opcionalmente, el sistema de preparación 20 también genera y cifra y preferiblemente también firma digitalmente datos de contexto aleatorios RCD y los almacena o hace que sean almacenados en un segundo almacenamiento de datos DS2. Además, el sistema de preparación 20 genera datos de inicialización IND y los almacena en un tercer almacenamiento de datos DS3. Los tres almacenamientos de datos DS1, DS2 y DS3 pueden ser almacenamientos de datos separados o dos de ellos o incluso los tres pueden ser los mismos. Específicamente, cada uno de los almacenamientos de datos se puede implementar, por ejemplo y sin limitación, como una cadena de bloques o un libro mayor distribuido sin bloques o como un almacenamiento en una infraestructura de clave pública PKI. Específicamente, las diversas entradas de datos almacenadas en los almacenamientos de datos pueden estar entrecruzadas por uno o más punteros cruzados CP, por ejemplo, en el caso de las cadenas de bloques, por punteros de cadenas de bloques cruzadas, cada uno de los cuales que conecta dos bloques correspondientes de un par específico de cadenas de bloques.

Cada uno de los nodos B, B' y C adicionales comprende un respectivo sistema de autenticación 30a, 30b y 30c, respectivamente. Cada uno de estos sistemas de autenticación 30a, 30b y 30c está configurado para realizar el método de autenticación de la Fig. 5 y/o la Fig. 6. Como se describirá en detalle a continuación con referencia a estas figuras, un sistema 30a, 30b o 30c respectivo que realiza la autenticación de los PO(s) recibidos lee el paquete de datos de inicio seguros del primer almacenamiento de datos DS1 y los datos de inicialización IND del tercer almacenamiento de datos DS3. Luego, se realiza la autenticación en base a estos resultados de lectura.

La Fig. 2A muestra un diagrama de flujo que ilustra una realización preferida de una primera fase 100 de un método de preparación de una autenticación asegurada posterior de un objeto físico o grupo de objetos físicos por un destinatario del mismo según la presente solución global. En particular, para el caso de la cadena de suministro, este método se realiza preferentemente al principio de la cadena de suministro por el primer nodo de la misma. En el presente ejemplo de la Fig. 1, este es el nodo A, respectivamente su sistema de preparación 20 y, por consiguiente, la siguiente descripción se basa en este ejemplo no limitativo. La Fig. 2B muestra una forma compacta del mismo método de la Fig. 2A, pero en la forma más compacta de un diagrama de flujo de datos.

En un paso 110, el sistema de preparación 20 recibe de otra entidad, tal como un centro logístico central, o genera él mismo datos de contexto predichos PCD con relación al siguiente nodo a lo largo de la cadena de suministro, es decir, en el presente ejemplo, el nodo B. Los datos complejos predichos PCD representan la ubicación x_B del nodo B, o más específicamente de su sistema 30a, y un tiempo predicho t_B, en el que se espera que lleguen los PO(s) a B. Los datos de contexto predichos PCD se pueden derivar particularmente de los datos de planificación logística, tales como un programa de entrega, para la cadena de suministro. La precisión de los datos de contexto predichos (por ejemplo, en términos de rango de coordenadas geográficas y unidades de tiempo, por ejemplo, horas, días o semanas) se adaptan preferiblemente para coincidir con la precisión con la que una ubicación futura y el punto en el tiempo correspondiente en el que ha de ocurrir la autenticación de los PO(s) en el siguiente nodo de la cadena de suministro, es decir, en el presente ejemplo, el nodo B, se puede predecir de manera fiable. Por ejemplo, si según los datos de planificación logística actuales, los PO(s) están programados para llegar al nodo B en una fecha particular, y el nodo B se relaciona con instalaciones industriales que tienen una extensión espacial de aproximadamente 500m x 500m, los PCD se pueden definir con una precisión en el tiempo de un día (24h) y una precisión en la ubicación de ±500m.

En un paso 120 adicional, el sistema de preparación 20 recibe de otra entidad, tal como dicho centro logístico central o un ordenador externo, o genera él mismo datos de contexto aleatorios RCD que representan una ubicación aleatoria x_r y un tiempo aleatorio t_r.

Luego, en un paso 130, los PCD y los RCD se combinan según un primer esquema de combinación CS1 predeterminado para derivar por ello datos de contexto modificados MCD que representan una ubicación aleatoria modificada x_m y un tiempo aleatorio modificado t_m. El primer esquema de combinación CS1 predeterminado puede ser un esquema de tiempo invariable que necesita ser establecido y poner a disposición de cada uno de los nodos de la cadena de suministro, donde los PO(s) se han de autenticar, solamente una vez. Alternativamente, el CS1 puede ser variable en el tiempo, lo que aumenta aún más la entropía de la solución de seguridad y, de este modo, el nivel de seguridad alcanzable. A continuación se proporcionará un ejemplo del uso de un esquema de combinación CS1 variable en el tiempo según las realizaciones de la presente solución global en conexión con la discusión de la Fig. 7.

Cada uno de los RCD y PCD puede representar además opcionalmente información adicional, aunque esto no se requiere por el presente método. En un paso adicional 150, los datos de contexto modificados MCD se cifran, por ejemplo, mediante una clave pública PubB del siguiente destinatario B, para obtener un paquete de datos de inicio asegurado SSDP que representa los MCD.

Además, los MCD se pueden firmar digitalmente por el nodo de envío, es decir, en el presente ejemplo, el nodo A, con una firma digital perteneciente a A. El paso de firma se puede realizar o bien (i) antes del cifrado según el paso 140 (opción 1), o bien (ii) después del cifrado en un paso 160 (opción 2), en donde en lugar de los MCD originales, el SSDP resultante del cifrado de los MCD está firmado digitalmente por A con su clave privada PrivA. Luego, en un paso 170 que completa la primera fase 100, a menos que se aplique un paso 180 adicional opcional, el SSDP se almacena o se hace que sea almacenado por otra entidad, tal como un ordenador externo, en el primer almacenamiento de datos DS1, como se describió anteriormente con referencia a la Fig. 1.

El paso 180 opcional se relaciona con una realización específica que se trata a continuación en detalle con referencia a la Fig. 8. En esta realización, los datos de contexto aleatorios se almacenan en un tercer almacenamiento de datos DS3 para permitir que otro nodo en la cadena de suministro asuma el papel de nodo A en un tiempo posterior, por ejemplo, en un tiempo cuando A ya no está disponible para la cadena de suministro, incluso si ese otro nodo no ha almacenado por sí mismo los datos de contexto aleatorios RCD recuperados durante un proceso de autenticación anterior, por ejemplo, según la Fig. 5A/5B o la Fig. 6A/6B.

La Fig. 3A muestra un diagrama de flujo que ilustra una primera realización 200 preferida de la segunda fase del método de preparación de una autenticación asegurada posterior según la presente solución global. La Fig. 3B muestra un diagrama de flujo de datos correspondiente. Específicamente, esta primera realización se refiere al caso donde los PO(s) a ser autenticados a lo largo de la cadena de suministro tienen o portan ellos mismos un número n = 1, 2, 3, ... de características discriminatorias específicas, cada una de las cuales puede ser particularmente una Función Física no Clonable PUF, por ejemplo según uno o más de los tipos de PUF descritos anteriormente.

En un paso 210 de la segunda fase 200 del método, el sistema de preparación 20 detecta las n características discriminatorias, en el presente ejemplo PUF, de los PO(s) a ser autenticados a lo largo de la cadena de suministro para obtener para cada característica discriminatoria datos de identificación IDD respectivos que representan una identidad de dichos PO(s) relacionados.

Luego, en un paso opcional 220, para cada una de las características discriminatorias $k \in \{1,..., n\}$, se aplica una primera función de comprobación aleatoria criptográfica $HF_{1,k}$ respectiva a los IDD_k obtenidos de la característica discriminatoria k respectiva para obtener una valor de comprobación aleatoria inicial Hi_k respectivo relacionado con esta característica discriminatoria k particular. Las primeras funciones de comprobación aleatoria criptográficas $HF_{1,k}$ respectivas relacionadas con diferentes características discriminatorias o IDD, respectivamente, pueden ser o bien iguales o bien diferentes. También es posible que algunas de ellas sean iguales mientras que otras sean diferentes, siempre y cuando la relación entre una característica discriminatoria/IDD particular y una primera función de comprobación aleatoria $HF_{1,k}$ respectiva permanezca conocida y sin cambios. En caso de que se omita el paso 220 opcional, los IDD_k obtenidos asumen el papel del valor de comprobación aleatoria inicial Hi_k correspondiente y, de este modo, forman ellos mismos entradas para el paso de combinación posterior 240, descrito a continuación.

En un paso 230 adicional, el sistema de preparación 20 lee de los PO(s), por ejemplo de una marca respectiva en los mismos, información de ubicación invariable y de tiempo invariable con relación específicamente a los PO(s). Por ejemplo, la información puede comprender uno o más números de serie que se asignan a los PO(s). Alternativamente, particularmente si tal información no existe todavía, el sistema de preparación 20 puede generar por sí mismo tal información de ubicación invariable y de tiempo invariable y asignarla a los PO(s) en cuestión. En el presente ejemplo no limitativo, la información de ubicación invariable y de tiempo invariable será uno o más números de serie asignados a los PO(s) respectivos. En la presente memoria, se hace referencia colectivamente a los números de serie como SN.

En un paso 240 adicional más, si $n > 1$, los n valores de comprobación aleatoria iniciales H_1, ... , H_n (si se implementa el paso 220) o los valores IDD_1, ... , IDD_n (si no se implementa el paso 220) se combinan con los datos de contexto aleatorios RCD y el número o números de serie SN según un segundo esquema de combinación CS2 que da como resultado un conjunto de datos H (que puede ser, por ejemplo, solamente un único valor H) que representa el resultado de esta operación de combinación. Preferiblemente, el esquema de combinación CS2 es conservador de información y/o idealmente conservador de entropía. Por ejemplo, el conjunto de datos resultante de la combinación según el esquema de combinación CS2 puede adoptar la forma de una mera agregación de datos de los datos de entrada respectivos, es decir, los valores a ser combinados. La agregación se puede representar particularmente por una matriz unidimensional o multidimensional u otro tipo de matriz. Como con el primer esquema de combinación CS1, también el segundo esquema de combinación CS2 puede ser un esquema de tiempo invariable que necesita ser establecido y puesto a disposición de cada uno de los nodos de la cadena de suministro, donde se han de autenticar los PO(s), solamente una vez. Alternativamente, de nuevo como CS1, también puede ser variable en el tiempo, en donde cada uno de los nodos de la cadena de suministro entonces necesita ser informado acerca del segundo esquema de combinación CS2 aplicable respectivo, con el fin de habilitar la autenticación respectiva de los PO(s) en ese nodo. A continuación se proporcionará un ejemplo del uso de

esquemas de combinación CS1 y/o CS2 variables en el tiempo según las realizaciones de la presente solución global en conexión con la discusión de la Fig. 7.

Luego, en un paso 250, se genera un valor de comprobación aleatoria adicional Ho, al que se hará referencia en la presente memoria como “valor de comprobación aleatoria original”, aplicando una segunda función de comprobación aleatoria criptográfica al conjunto de datos H.

En un paso 260 adicional, el sistema de preparación 20 firma digitalmente el valor de comprobación aleatoria original Ho con la clave privada PrivA de A con el fin de permitir una verificación posterior del origen de Ho en una autenticación posterior en un nodo de la cadena de suministro, es decir, en el presente ejemplo en los nodos B, B’ y C.

En un paso 270 adicional más, que se puede implementar particularmente junto con el paso 260 como un único paso combinado, el sistema de preparación 20 genera datos de inicialización IND que representan el valor de comprobación aleatoria original Ho obtenido en el paso 250 junto con la firma digital del mismo obtenida en el paso 260.

La fase 200 del método se concluye mediante un paso 280 adicional, en donde se añade una representación de los datos de inicialización IND, por ejemplo, una marca respectiva, a dichos PO(s) y/o dicha representación de IND se almacena o hace que se almacene en un tercer almacenamiento de datos DS3 junto con añadir a dichos PO(s) una representación de un puntero que indica dónde se puede acceder a los IND en DS3. La ubicación de almacenamiento para los IND dentro del DS3 y, por lo tanto, también el puntero, se puede determinar, por ejemplo, en base a uno o más números de serie SN de los PO(s).

La Fig. 4A muestra un diagrama de flujo que ilustra una segunda realización preferida 300 de la segunda fase del método de preparación de una autenticación asegurada posterior según la presente solución global. La Fig. 4B muestra un diagrama de flujo de datos correspondiente. Específicamente, esta segunda realización se refiere al caso donde los PO(s) a ser autenticados a lo largo de la cadena de suministro pueden no tener o portar ellos mismos una característica discriminatoria específica, tal como por ejemplo una Función Física no Clonable PUF.

En un paso 310, que es igual al paso 230 en la Fig. 2A/2B, el sistema de preparación 20 lee de los PO(s) o genera él mismo información de ubicación invariable y de tiempo invariable específicamente con relación a los PO(s), por ejemplo uno o más números de serie SN que se asignan a los PO(s).

En un paso 320 adicional más, el sistema de preparación 20 determina un conjunto de datos H de una combinación, según un esquema de combinación predeterminado CS3, de los datos de contexto aleatorios RCD y una información de tiempo y ubicación invariables que identifica o que está relacionada específicamente de otro modo con los PO(s). Por ejemplo, esta información puede ser uno o más números de serie SN de los PO(s). Como con el CS2, el esquema de combinación CS3 puede ser un esquema de tiempo invariable o un esquema de tiempo variable (véase la Fig. 7).

En un paso 330 adicional más, el sistema de preparación 20 genera un valor de comprobación aleatoria original Ho aplicando una función de comprobación aleatoria criptográfica al conjunto de datos obtenido H.

En un paso 340 adicional (opcional) más, el sistema de preparación 20 firma digitalmente el valor de comprobación aleatoria original Ho con la clave privada de A con el fin de permitir una verificación posterior del origen de Ho en una autenticación posterior en un nodo en la cadena de suministro, es decir, en el presente ejemplo en los nodos B, B’ y C.

En un paso 350 adicional más, que se puede implementar particularmente junto con el paso 340 como un único paso combinado, el sistema de preparación 20 genera datos de inicialización IND que representan el valor de comprobación aleatoria original Ho obtenido en el paso 320, junto con la firma digital del mismo obtenida en el paso 330, si se implementa.

La fase 300 del método se concluye mediante un paso 360 adicional, en donde una representación de los datos de inicialización IND, por ejemplo, una marca respectiva, se añade a dichos PO(s) y/o dicha representación de IND se almacena o hace que se almacene en un tercer almacenamiento de datos DS3 junto con añadir a dichos PO(s) una representación de un puntero que indica dónde se puede acceder a los IND en el DS3. La ubicación de almacenamiento para los IND dentro de DS3 y, por lo tanto, también el puntero, se puede determinar, por ejemplo, en base al uno o más números de serie SN de los PO(s).

La Fig. 5A muestra un diagrama de flujo que ilustra una primera realización preferida 400 de un método de autenticación de un objeto físico o un grupo de objetos físicos según la presente solución global, que está configurado para ser usado en conexión con el método de las Figuras 2 y 3. La Fig. 5B muestra un diagrama de flujo de datos correspondiente.

El método 400 está diseñado para ser usado en particular por aquellos nodos B, B’, C a lo largo de la cadena de suministro que no son el punto de inicio A de la distribución de los PO(s) y que de este modo tienen el deseo de

autenticar correctamente los PO(s) recibidos del nodo inmediatamente anterior respectivo en la cadena de suministro. El método se explicará ahora de manera ejemplar en relación con los PO(s) que portan dos o más PUF diferentes como características discriminatorias. Por supuesto, se pueden usar en su lugar métodos similares basados en otras características discriminatorias no de PUF o una mezcla de características discriminatorias de PUF y no de PUF, según realizaciones adicionales no ilustradas en la presente memoria.

El método 400 comprende un paso 410, en donde el sistema de autenticación 30a, 30b o 30c respectivo, que realiza el método, se aplica a cada una de las PUF de los PO(s) a ser autenticados un desafío respectivo de un esquema de autenticación AS de desafío-respuesta predeterminado respectivo para desencadenar una respuesta según el AS en reacción al desafío. Por simplificación, la siguiente descripción en las Figs. 5A, B y 6A, B se centrará en el sistema de autenticación 30a en el nodo B, aunque necesita ser entendido que el mismo método 400 se puede usar también por todos los demás nodos a lo largo de la cadena de suministro.

En el paso 415, cada una de las respuestas de las diversas PUF se detecta de acuerdo con el esquema de autenticación de desafío-respuesta respectivo y los datos de identificación IDD respectivos, que representan la respuesta, que se derivan del mismo.

En un paso 420 adicional (opcional), para cada una de las PUF k, se aplica una respectiva primera función de comprobación aleatoria criptográfica predeterminada $HF_{1,k}$ que es igual a la primera función de comprobación aleatoria criptográfica correspondiente que se usó anteriormente en el método de la Fig. 3 durante la fase de preparación 200 para la misma PUF, a los IDD respectivos para obtener un valor de comprobación aleatoria inicial Hi_k respectivo relacionado con esos IDD_k de PUF k, respectivamente. Los pasos 410 a 420 sirven para proporcionar el conjunto de valores de comprobación aleatoria iniciales Hi_k como una primera entrada para un paso de combinación posterior 450 que se describirá a continuación en detalle. Si no se implementa el paso 420, la primera entrada con respecto al paso de combinación 450 será en su lugar los valores de IDD_k correspondientes derivados en el paso 415.

Los pasos 425 a 440 adicionales están diseñados para proporcionar una segunda entrada al paso de combinación 450. En el paso 425, el sistema considerado 30a, por ejemplo, lee, del primer almacenamiento de datos DS1, un paquete de datos de inicio asegurado SSDP que representa datos de contexto CD cifrados que a su vez representan una ubicación x_0 y un tiempo t_0 relacionado. El SSDP se descifra para recuperar dichos datos de contexto CD.

Además, en un paso 430, datos de contexto actuales CCD que representan la ubicación actual x y el tiempo actual t relacionado de presencia de los PO(s) en su ubicación actual x se generan por el sistema 30a o se reciben de otra entidad, tal como un base de datos de logística. Preferiblemente, los datos de contexto actuales CCD tienen una precisión similar a la de los datos de contexto predichos.

En un paso 435 adicional, el sistema 30a determina un esquema de combinación CS3 aplicable, que define una operación inversa con la operación correspondiente según el esquema de combinación CS1 correspondiente usado anteriormente para generar los datos de contexto CD recibidos. Esta determinación se puede realizar, por ejemplo, como se describe a continuación con referencia a la Fig. 7.

Luego, en un paso 440, los datos de contexto actuales CCD se combinan, según el esquema de combinación CS3 determinado, con los datos de contexto CD descifrados para determinar por ello los datos de contexto de prueba TCD. Esta operación combinada del paso 440 es, en efecto, la operación inversa de la operación realizada por el paso 140 de la Fig. 2. Cuando los PCD y los CCD tienen una precisión similar, y esa precisión se hace coincidir con la fiabilidad en el contexto de la logística de la cadena de suministro, la autenticación llega a ser más robusta frente a diferencias aceptables entre las ubicaciones y/o particularmente los puntos en el tiempo indicados por los PCD y los CCD, respectivamente. Por consiguiente, si los datos de contexto actuales CCD coinciden con los PCD correspondientes, al menos dentro de dicha precisión, y el SSDP no se ha corrompido, se espera que los TCD resultantes coincidan con los datos de contexto aleatorios RCD originales.

El paso 445 adicional está diseñado para proporcionar una tercera entrada al paso de combinación 450 posterior. En el paso 445, el sistema 30a lee del almacenamiento de datos DS3 los datos de inicialización IND relacionados con dichos PO(s) que se almacenaron anteriormente en el DS3 según el paso 340 de la fase de método 300. Si los datos de inicialización IND almacenados se firmaron digitalmente antes de almacenarlos, leer los datos de inicialización IND comprende verificar la firma digital respectiva mediante la cual se firmaron digitalmente los IND y recuperar el valor de comprobación aleatoria original Ho representado por los datos de inicialización IND. Ho está entonces disponible como dicha tercera entrada al paso de combinación 450, que sigue.

En dicho paso de combinación 450, el sistema 30a genera un valor de comprobación aleatoria de prueba Ht mediante la aplicación de una segunda función de comprobación aleatoria criptográfica predeterminada a una combinación predeterminada Hc de los valores de comprobación aleatoria iniciales Hi_k, los TCD y el uno o más números de serie SN proporcionados en los PO(s). La segunda función de comprobación aleatoria criptográfica predeterminada es igual a la función de comprobación aleatoria criptográfica HF2 correspondiente usada para determinar Ho, como se representa por los IND, en el paso 230 de la fase del método 200.

Finalmente, el método 400 se concluye por el paso 455, en donde el sistema de autenticación 30a genera y emite un primer resultado de lectura RR1 que indica si, según al menos un criterio de coincidencia predeterminado, HT coincide o no con Ho y, de este modo, indica la autenticidad de los PO(s).

La Fig. 6A muestra un diagrama de flujo que ilustra una segunda realización preferida 500 de un método de autenticación de un objeto físico o un grupo de objetos físicos según la presente solución global, que está configurado para ser usado en conexión con el método de las Figuras 2 y 4.

La Fig. 6B muestra un diagrama de flujo de datos correspondiente.

La segunda realización 500 difiere de la primera realización 400 descrita anteriormente en conexión con la Fig. 5 en que no están disponibles ni se usan características discriminatorias de los PO(s).

Por consiguiente, en el método 500, por una parte, no hay pasos que correspondan a los pasos 410 a 420 del método 400, mientras que, por otra parte, hay pasos 510 a 530 que corresponden y pueden ser particularmente idénticos a los pasos 425 a 445. El paso adicional 535 del método 500 difiere del paso 450 correspondiente del método 400 en que ahora el valor de comprobación aleatoria de prueba Ht se genera mediante la aplicación de una función de comprobación aleatoria criptográfica HF2 respectiva a una combinación Hc predeterminada de los datos de contexto de prueba TCD y el uno o más números de serie SN proporcionados en los PO(s). El paso de salida final 540 del método 500 es de nuevo idéntico al paso 455 del método 400.

Si bien se puede usar la realización del método 400 (y el método 200) para lograr niveles de seguridad más altos que los que están disponibles cuando se usa el método 500 (y el método 300), este último tiene la ventaja de una menor complejidad y, de este modo, puede ser preferible, cuando, en vista de un nivel de seguridad deseado moderado, que mantiene la complejidad y de este modo los costes y esfuerzos para implementar el sistema bajos, tiene prioridad.

La Fig. 7 muestra un diagrama de flujo que ilustra una realización preferida de un método 600 de usar uno o más esquemas de combinación de tiempo variable en conexión con los métodos de las Figs. 3A/3B a 6A/6B. Cuando un destinatario, tal como el nodo B, necesita autenticar unos PO(s) recibidos, primero tendrá que recuperar los esquemas de combinación CS de tiempo variable aplicables, tales como por ejemplo el CS2 y/o CS3.

La solución a este problema según la realización de la Fig. 7 se basa en una autoridad de confianza TC, tal como por ejemplo un centro de confianza como se conoce a partir de las infraestructuras de clave pública (PKI). En otro ejemplo, el proveedor original A puede ser él mismo o proporcionar el centro de confianza TC.

Durante un proceso de preparación de una autenticación posterior, por ejemplo en el proceso según los métodos 100/200 o 100/300 descritos anteriormente con referencia a la Fig. 2 y las Figs. 3A/3B, o la Fig. 2 y las Figs. 4A/4B, en un paso 605, el nodo A almacena o hace que sean almacenados en un almacenamiento de datos DS, por ejemplo, el DS1, del centro de confianza TC uno o más números de serie SN y pertenecientes a unos PO(s) particulares a ser distribuidos y autenticados a lo largo de una cadena de suministro dada, el esquema de combinación CS relevante, tal como una fórmula matemática invertible u otro esquema de procesamiento de datos invertible adecuado, y metadatos MD(CS(SN)) relacionados con el esquema de combinación CS aplicable para los PO(s) con número o números de serie SN. Los metadatos MD(CS(SN)) pueden comprender en particular información que define un período de validez limitado del esquema de combinación CS, de manera que ya no sea aplicable una vez que haya expirado el período de validez.

Cuando B recibe los PO(s) y necesita autenticarlos, envía en un paso 610 una solicitud respectiva al centro de confianza TC junto con el número o números de serie SN de los PO(s) e información de identificación predefinida que permite una autenticación de dos factores 2FA, es decir, una autenticación adicional de B por el centro de confianza que es independiente de la clave privada PrivB de B (que se usa, por ejemplo, para descifrar el SSDP durante el proceso de autenticación de los PO(s)). La información de identificación puede comprender, por ejemplo, un PIN y un TAN, similar a los procedimientos conocidos para la banca en línea, una foto TAN, una contraseña o se puede basar en un par de claves públicas/privadas independientes adicionales.

El centro de confianza TC luego verifica en un paso de 2FA 615 la información de identificación recibida de B con el fin de autenticar a B y también recupera en un paso 620 los metadatos MD(CS (SN)) del almacenamiento de datos DS. En el paso 625, se comprueban los metadatos MD(CS (SN)) con el fin de determinar si el esquema de combinación CS solicitado todavía es válido y se evalúa el resultado del paso de autenticación 615. Si esta autenticación de B y/o la comprobación falla (625 - no), se devuelve un mensaje de error a B en el paso 630. De otro modo (625 - sí), el número o números de serie SN recibidos se usan en un paso 635 como un índice para consultar una base de datos en el almacenamiento de datos DS para recuperar en un paso 640 el esquema de combinación CS(SN) deseado y cifrado en un paso adicional 645, por ejemplo, con la clave pública de B. Cuando B recibe el esquema de combinación CS(SN) cifrado, se descifra en el paso 650, por ejemplo, con su clave privada, con el fin de obtener el esquema de combinación CS(SN) deseado. Mientras que usar el cifrado asimétrico es un planteamiento adecuado para implementar el cifrado/descifrado de los pasos 645 y 650, en su lugar se puede usar cualquier otro planteamiento para asegurar suficientemente la comunicación entre el TC y B contra la intercepción. En la Fig. 7, la comunicación asegurada entre B y el TC se indica como un “túnel” T asegurado respectivo que puede

estar separado para cada una de las comunicaciones o un túnel conjunto para dos o más de los enlaces de comunicación. Por ejemplo, se puede usar un cifrado simétrico. También, si se usa el cifrado asimétrico para ese propósito, se puede usar un par de claves diferente que en otros pasos de los métodos descritos anteriormente.

En resumen, con el fin de que B autentique con éxito los PO(s) recibidos, necesitan ser cumplidas tres condiciones (factores): (1) B necesita procesar su clave privada PrivB, (2) la autenticación necesita tener lugar en la ubicación correcta (nodo B) y período de tiempo definido por A en los datos de contexto predichos PCD durante la fase de preparación 200, y (3) B necesita tener la información de identificación válida necesaria para acceder a uno o más esquemas de combinación CS de tiempo variable relevantes, por ejemplo, el CS2 y/o CS3. Por consiguiente, la autenticación de los PO(s) fallaría, si los PO(s) estaban programados originalmente para llegar al nodo B en un tiempo dado, como se define en los datos de contexto predichos PCD relacionados, pero los PO(s) en realidad se proporcionaron en su lugar a otra ubicación de almacén de B (nodo B'), es decir, en un tiempo diferente y en una ubicación diferente (véase la Fig. 1). De este modo, cuando B quiere que A redirija la distribución de los PO(s) del modo A al nodo B' (en lugar del nodo B), B necesita informar a A de este deseo y luego A necesita preparar y almacenar un paquete de datos de inicio de actualización SSDP que refleja esta redirección al nodo B'.

Las Figuras 8A y 8B ilustran diversas opciones diferentes para habilitar pasos de suministro (saltos) adicionales a lo largo de una cadena de suministro usando cadenas de bloques como almacenamientos de datos en conexión con uno o más de los métodos descritos anteriormente con respecto a las Figs. 2 a 7. Específicamente, la Fig. 8A se refiere a realizaciones, donde el nodo A se define como la única autoridad a lo largo de la cadena de suministro para determinar el paquete de datos de inicio respectivo para cada salto. Además, A puede ser la única autoridad para definir también datos de inicialización IDD adicionales que sustituyan a los datos de inicialización originales con relación a los PO(s) particulares. Si bien para cada salto a lo largo de la cadena de suministro, se necesita un nuevo paquete de datos de inicio asegurado, que se basa en los datos de contexto predichos PCD respectivos para el destinatario del siguiente salto respectivo, los datos de inicialización se pueden o bien mantener sin cambios o bien también cambiar.

Por ejemplo, cuando en la realización de la Fig. 8A, los PO(s) suministrados a lo largo de la cadena de suministro de A a C han alcanzado el nodo B y se han autenticado con éxito allí, B emite una solicitud R a la única autoridad, que es el nodo A, para emitir el nuevo SSDP(C) necesario para el salto de B a C. Típicamente, B proporcionará datos de contexto predichos para C a A para permitir la determinación de un SSDP(C) correcto o bien a través de uno de los almacenamientos de datos DS1 a DS3 o bien a través de un canal de información separado preferiblemente asegurado. Opcionalmente, B también puede solicitar, por ejemplo, como parte de la solicitud R, nuevos datos de inicialización IND(C) basados en nuevos datos de contexto aleatorios RCD. En la medida que se necesitan los RCD para determinar tanto el SSDP(C) como los IND(C) solicitados, estos dos elementos de datos solicitados están relacionados, en la medida que se basan en los mismos RCD. Según la solicitud, A determina el SSDP(C) y opcionalmente también los IND(C) y almacena el resultado en el almacenamiento de datos DS1 y DS3 relacionado, respectivamente. Cuando los PO(s) enviados por B llegan al nodo C, el sistema 30c de C puede leer el SSDP(C) y, si es aplicable, los IND(C) y autenticar con éxito los PO(s) en base a ello, siempre que los datos de contexto actuales (CCD) de C coincidan con los PCD basados en que el SSDP(C) se determinó por A.

La Fig. 8B, por el contrario, se refiere a realizaciones donde un destinatario anterior de los PO(s) puede asumir él mismo el papel de determinar el SSDP necesario y, opcionalmente, también los IND adicionales relacionados para el siguiente salto que comienza en ese nodo. Por ejemplo, el nodo B puede asumir el papel anterior que tenía A en relación con el salto de A a B para el salto adicional de B a C. En cualquier caso, B necesita determinar el nuevo SSDP(C) para C basado en los datos de contexto predichos relacionados para C. Los datos de contexto aleatorios RCD usados para esta determinación pueden seguir siendo los mismos en cuanto al salto anterior. Por consiguiente, en la primera variante, B puede usar los RCS determinados como resultado de la autenticación anterior de los PO(s) en el nodo B tras la llegada desde el nodo A. En la segunda variante, no obstante, B necesita generar o recibir nuevos datos de contexto aleatorios y, de este modo, determinar también el SSDP(C) y los nuevos datos de inicialización IND(C) basados en los mismos y almacenarlos en el DS1 y DS3, respectivamente. El proceso de autenticación para los PO(s) en el nodo C es entonces similar al del caso de la Fig. 8A.

Otra variante relacionada de las realizaciones de la Fig. 8B es un caso donde el nuevo SSDP(C) y, opcionalmente, los nuevos datos de inicialización IND(C) necesitan ser determinados en base a los datos de contexto aleatorios RCD originales determinados originalmente por A, pero donde tales RCD ya no está disponibles en A y B o tal vez incluso A o sus datos ya no existen en absoluto. Esto puede ocurrir, por ejemplo, en casos donde el tiempo de recorrido bruto de los PO(s) a lo largo de la cadena de suministro es bastante largo (por ejemplo, años), como puede ser el caso de mercancías que típicamente tienen largos tiempos de almacenamiento entre saltos consecutivos, por ejemplo, en el caso de los diamantes (en bruto). Entonces, una solución puede ser que, como se ilustra en las Figs. 1 y 8B, A almacena sus RCD en un almacenamiento de datos, por ejemplo, el DS2, es una manera asegurada, por ejemplo, cifrados, de manera que B o cualquier nodo B adicional autorizado pueda acceder a ellos incluso cuando los RCD originales ya no estén disponibles para B de otro modo. B puede entonces acceder a los RCD en el DS2 y continuar en base a los mismos el flujo de datos correspondiente a la cadena de suministro en base al método de la Fig. 8B y los RCD originales.

Si bien anteriormente se ha descrito al menos una realización ejemplar de la presente invención, se tiene que señalar que existe un gran número de variaciones de la misma. Además, se aprecia que las realizaciones ejemplares descritas solamente ilustran ejemplos no limitativos de cómo se puede implementar la presente invención y que no se pretende que limiten el alcance, la aplicación o la configuración del aparato y los métodos descritos en la presente memoria. Más bien, la descripción anterior proporcionará a los expertos en la técnica instrucciones para implementar al menos una realización ejemplar de la invención, en donde se tiene que entender que se pueden hacer diversos cambios de funcionalidad y la disposición de los elementos de la realización ejemplar, sin desviarse del objeto definido por las reivindicaciones adjuntas y sus equivalentes legales.

Lista de signos de referencia

10	solución de seguridad global
20	sistema de preparación de nodo A
30 a, b, c	sistemas de autenticación de nodos B, B’ y C, respectivamente
2FA	autenticación de dos factores
A, B, C	nodos de cadena de suministro
CCD	datos de contexto actuales
CP	puntero cruzado, por ejemplo, puntero de cadena de bloques cruzada
CD	datos de contexto cifrados
CS	esquema de combinación, por ejemplo, uno de CS1, CS2 y CS3
CS1	primer esquema de combinación
CS2	segundo esquema de combinación
CS3	tercer esquema de combinación, inverso del CS1
Dec	descifrado
DS	almacenamiento de datos, en particular uno del DS1, DS2 y DS3
DS1,…, DS3	almacenamiento de datos, por ejemplo, cadenas de bloques
Enc	cifrado
H	conjunto de datos, por ejemplo, valor único
HF1, HF2	funciones de comprobación aleatoria
Hc	combinación predeterminada de los valores de comprobación aleatoria iniciales
Hi	valor de comprobación aleatoria inicial
Ho	valor de comprobación aleatoria original
Ht	valor de comprobación aleatoria de prueba
IDD	datos de identificación
IND	datos de inicialización
k	característica discriminatoria o índice correspondiente a la misma, respectivamente
MCD	datos de contexto modificados
PCD	datos de contexto predichos
PIN	número de identificación personal
PO(s)	objetos físicos o grupo de objetos físicos
PrivA	clave privada de A
PrivB	clave privada de B

PubA	clave pública de A
PubB	clave pública de B
PUF1-PUFn	funciones físicas no clonables (PUF)
R	solicitud
RCD	datos de contexto aleatorios
RR1	primer resultado de lectura
Sign	crear firma digital
SN	número o números de serie
SSDP	paquete de datos de inicio asegurado
T	canal asegurado, túnel
TAN	número de transacción
TC	sistema para proporcionar de manera segura un esquema de combinación de tiempo variable, centro de confianza
TCD	datos de contexto de prueba

REIVINDICACIONES

1. Un método (600) de provisión de manera segura de un esquema de combinación (CS) variable en el tiempo para autenticar un objeto físico o un grupo de objetos físicos (PO(s)) según un método (400; 500) de autenticación de un objeto físico o grupo de objetos físicos (PO(s)), el método (600) de provisión del esquema de combinación (CS) que comprende:

recibir y almacenar (605) datos que representan el esquema de combinación (CS) predeterminado, una información de tiempo y de ubicación invariables (SN) que identifica o que está relacionada de otro modo específicamente con dicho objeto físico o grupo de objetos físicos, y metadatos (MD(CS(SN))) que definen un período de validez limitado del esquema de combinación (CS);

recibir (610) una solicitud del esquema de combinación (CS) y la información de identidad (SN) que identifica o que está relacionada de otro modo específicamente con un objeto físico o un grupo de objetos físicos (PO(s)) de un sistema de autenticación solicitante (30a, 30b, 30c);

autenticar (615) el sistema de autenticación solicitante (30a, 30b, 30c); y

si el sistema solicitante (30a, 30b, 30c) se autentica con éxito (615) como que está autorizado y según los metadatos (MD(SN)) previamente almacenados correspondientes a la información de identidad recibida (SN), el esquema de combinación (CS(SN)) relacionado al que pertenecen los metadatos (MD(SN)) sigue siendo válido, emitir (640) datos que representan ese esquema de combinación (CS(SN)) relacionado a través de un canal de datos (T) que está asegurado (645) contra la intercepción al sistema solicitante (30a, 30b, 30c); o, de otro modo, denegar la solicitud.

2. El método (600) de provisión del esquema de combinación (CS) según la reivindicación 1, en donde el método (400; 500) de autenticación de un objeto físico o un grupo de objetos físicos (PO(s)), comprende:

recibir (425; 510) y descifrar un paquete de datos de inicio asegurado (SSDP) que representa datos de contexto (CD) cifrados que representan una ubicación y un tiempo relacionado para recuperar dichos datos de contexto (CD);

recibir o determinar (430; 515) datos de contexto actuales (CCD) que representan una ubicación actual del objeto físico o grupo de objetos físicos (PO(s)) y un tiempo actual relacionado de presencia del objeto físico o grupo de objetos físicos (PO(s)) en esa ubicación actual;

combinar (440; 525), según un esquema de combinación (CS3) predeterminado (435; 520), los datos de contexto actuales (CCD) con los datos de contexto (CD) descifrados para determinar por ello los datos de contexto de prueba (TCD), en donde el esquema de combinación (CS3) define una operación inversa a una operación de combinación (CS1) correspondiente usada anteriormente para generar los datos de contexto (CD) recibidos;

acceder (445; 530) a los datos de inicialización (IND) relacionados con dicho objeto físico o grupo de objetos físicos (PO(s)) para recuperar de ellos un valor de comprobación aleatoria original (Ha) que se representa por los datos de inicialización (IND);

el método que comprende además uno de los siguientes procesos a) a c):

a) detectar (410, 415) por medio de uno o más sensores al menos una característica discriminatoria (k) de dicho objeto físico o grupo de objetos físicos (PO(s)) para obtener los datos de identificación (IDD_k) respectivos relacionados con dicha característica discriminatoria (k) respectiva, estos datos de identificación (IDD_k) que representan una identidad supuesta de dicho objeto físico o grupo de objetos físicos (PO(s)) relacionado; y

generar (450) un valor de comprobación aleatoria de prueba (Ht) mediante la aplicación de una segunda función de comprobación aleatoria (HF2) criptográfica predeterminada a una combinación (Hc), según un esquema de combinación (CS2) predeterminado adicional, de los datos de contexto de prueba (TCD) y cada uno de dichos datos de identificación (IDD_k); o

b) detectar (410, 415) por medio de uno o más sensores al menos una característica discriminatoria (k) de dicho objeto físico o grupo de objetos físicos (PO(s)) para obtener los datos de identificación (IDD_k) respectivos relacionados con dicha característica discriminatoria (k) respectiva, estos datos de identificación (IDD_k) que representan una identidad supuesta de dicho objeto físico o grupo de objetos físicos (PO(s)) relacionado;

aplicar (420) una primera función de comprobación aleatoria ($HF_{1,k}$) criptográfica predeterminada respectiva a los datos de identificación (IDD_k) respectivos para obtener un valor de comprobación aleatoria inicial (Hi_k) respectivo relacionado con dicha característica discriminatoria (k); y

generar (450) un valor de comprobación aleatoria de prueba (Ht) mediante la aplicación de una segunda función de comprobación aleatoria (HF2) criptográfica predeterminada a una combinación (Hc), según el segundo esquema de combinación (CS2) predeterminado, de los datos de contexto de prueba (TCD) y cada uno de dichos valores de comprobación aleatoria iniciales (Hi_k);

c) generar (535) un valor de comprobación aleatoria de prueba (Ht) mediante la aplicación de una segunda función de comprobación aleatoria (HF2) criptográfica predeterminada a los datos de contexto de prueba (TCD) o a una combinación (Hc), según el segundo esquema de combinación (CS2) predeterminado, de los datos de contexto de prueba (TCD) y una información de tiempo invariable y de ubicación invariable que identifica o que está relacionada de otro modo específicamente con dicho objeto físico o grupo de objetos físicos;

en donde para el respectivo de los procesos a) a c), esta segunda función de comprobación aleatoria (HF2) criptográfica predeterminada es igual a una función de comprobación aleatoria criptográfica correspondiente usada anteriormente para determinar el valor de comprobación aleatoria original (Ho) representado por los datos de inicialización (IND), y en donde dicho segundo esquema de combinación (CS2) es igual a un esquema de combinación correspondiente usado anteriormente para determinar el valor de comprobación aleatoria original (Ho) representado por los datos de inicialización (IND); y

el método comprende además:

generar (455; 540) un primer resultado de lectura (RR1) que comprende:

- una representación del valor de comprobación aleatoria de prueba (Ht) y una representación del valor de comprobación aleatoria original (Ho), o

- una salida de coincidencia que indica si, según al menos un criterio de coincidencia predeterminado, el valor de comprobación aleatoria de prueba coincide o no con dicho valor de comprobación aleatoria original y, de este modo, indica la autenticidad del objeto físico o grupo de objetos físicos.

3. El método de la reivindicación 2, en donde en el proceso a), se genera el valor de comprobación aleatoria de prueba (Ht) (450) aplicando la segunda función de comprobación aleatoria (HF2) criptográfica predeterminada a una combinación (Hc), según un esquema de combinación (CS2) predeterminado adicional, de los datos de contexto de prueba (TCD) y cada uno de dichos datos de identificación (IDD_k) y una información de tiempo invariable y de ubicación invariable (SN) que identifica o que está relacionada de otro modo específicamente con dicho objeto físico o grupo de objetos físicos (PO(s)).

4. El método de la reivindicación 2 o 3, en donde en el proceso b), el valor de comprobación aleatoria de prueba (Ht) se genera (450) aplicando la segunda función de comprobación aleatoria (HF2) criptográfica predeterminada a una combinación (Hc), según el segundo esquema de combinación (CS2) predeterminado, de los datos de contexto de prueba (TCD) y cada uno de dichos valores de comprobación aleatoria iniciales (H_{ik}) y una información de tiempo invariable y de ubicación invariable (SN) que identifica o que está relacionada de otro modo específicamente con dicho objeto físico o grupo de objetos físicos (PO(s)).

5. El método (600) de cualquiera de las reivindicaciones 2 a 4,

en donde al menos una de dichas características discriminatorias (k) comprende una función física no clonable, PUF; y

en donde, en el método (400; 500) de autenticación de un objeto físico o grupo de objetos físicos (PO(s)), detectar dicha característica discriminatoria para obtener los datos de identificación respectivos relacionados con el mismo comprende:

aplicar (410) un desafío respectivo de un esquema de autenticación de desafío-respuesta predeterminado respectivo a la PUF para desencadenar una respuesta según dicho esquema de autenticación en reacción a dicho desafío; y

detectar (415) una respuesta respectiva por la PUF de acuerdo con el esquema de autenticación de desafío-respuesta respectivo en reacción al desafío y derivar de la misma dichos datos de identificación respectivos.

6. El método (600) de cualquiera de las reivindicaciones 2 a 5, en donde, en el método (400; 500) de autenticación de un objeto físico o grupo de objetos físicos (PO(s)), obtener los datos de identificación (IDD_k) comprende:

la detección en base a sensores de una o más características discriminatorias (k) de dicho objeto físico o grupo de objetos físicos (PO(s));

generar datos de objeto que representen dicha una o más características discriminatorias (k) de dicho objeto físico o grupo de objetos físicos (PO(s)); y

comunicar dichos datos de objeto a un sistema de reconocimiento automático de objetos; y

recibir los datos de identificación firmados digitalmente desde dicho sistema en respuesta a dicha comunicación de dichos datos de objeto.

7. El método (600) de cualquiera de las reivindicaciones 2 a 6, en donde el método (400; 500) de autenticación de un objeto físico o un grupo de objetos físicos (PO(s)) comprende además un proceso de almacenamiento que

comprende almacenar el primer resultado de lectura (RR1), o hacer que se almacene, en un bloque de una cadena de bloques de un primer conjunto de una o más cadenas de bloques o en uno o más nodos de un libro mayor distribuido sin bloques de un primer conjunto de uno o más libros distribuidos sin bloques.

8. El método (600) de la reivindicación 7, en donde, en el método (400; 500) de autenticación de un objeto físico o grupo de objetos físicos (PO(s)):

la detección (410, 415) de características discriminatorias del objeto físico o grupo de objetos físicos (PO(s)) comprende detectar una pluralidad de unas diferentes de tales características discriminatorias para obtener en base a las mismas para cada una de las características discriminatorias (k) el conjunto individual respectivo de datos de identificación (IDD_k) que representa el objeto físico o grupo de objetos físicos (PO(s));

generar el valor de comprobación aleatoria de prueba (Ht) se realiza para cada uno de los conjuntos individuales de datos de identificación (IDD_k) por separado tal como para obtener para cada uno de los conjuntos individuales de datos de identificación (IDD_k) un valor de comprobación aleatoria de prueba individual (Hi_k) respectivo;

generar el resultado de la primera lectura se realiza para cada uno de los valores de comprobación aleatoria de prueba individuales por separado para obtener para cada una de las características discriminatorias un resultado de la primera lectura individual respectivo; y

el proceso de almacenamiento comprende almacenar cada uno de dichos resultados de la primera lectura individuales respectivamente haciendo que se almacene en un bloque de una cadena de bloques dedicada individual respectiva en dicho primer conjunto de cadenas de bloques o en uno o más nodos de un libro mayor distribuido sin bloques dedicado individual respectivo en dicho primer conjunto de libros mayores distribuidos sin bloques.

9. El método (600) de cualquiera de las reivindicaciones 2 a 8, en donde el método (400; 500) de autenticación de un objeto físico o grupo de objetos físicos (PO(s)) comprende además determinar un paquete de datos de inicio asegurado (SSDP) adicional para una autenticación asegurada posterior más de dicho objeto físico o grupo de objetos físicos (PO(s)) en un destinatario (C) adicional más del mismo.

10. El método (600) de la reivindicación 9, en donde, en el método (400; 500) de autenticación de un objeto físico o un grupo de objetos físicos (PO(s)), determinar dicho paquete de datos de inicio asegurado (SSDP) adicional comprende:

emitir una solicitud (R) para determinar tal paquete de datos de inicio asegurado (SSDP) adicional para una autenticación asegurada posterior más de dicho objeto físico o grupo de objetos físicos (PO(s)) en un destinatario (C) adicional más del mismo a un proveedor autorizado (A) de dicho paquete de datos de inicio asegurado (SSDP) adicional y recibir dicho paquete de datos de inicio asegurado (SSDP) adicional solicitado en respuesta a la solicitud.

11. El método (600) de la reivindicación 9, en donde, en el método (400; 500) de autenticación de un objeto físico o un grupo de objetos físicos (PO(s)), determinar dicho paquete de datos de inicio asegurado (SSDP) adicional comprende preparar una autenticación asegurada posterior del objeto físico o grupo de objetos físicos (PO(s)) por el destinatario (C), la preparación que comprende:

recibir o generar (110) datos de contexto predichos (PCD) que representan una ubicación futura predicha en relación con el siguiente destinatario (C) designado del objeto físico o grupo de objetos físicos (PO(s)) y un tiempo futuro relacionado de presencia del objeto físico o grupo de objetos físicos (PO(s)) en esa ubicación futura;

recibir o generar (120) datos de contexto aleatorios (RCD) que indican una ubicación aleatoria y un tiempo aleatorio;

combinar (130), según un primer esquema de combinación predeterminado (CS1), los datos de contexto predichos (PCD) y los datos de contexto aleatorios (RCD) para derivar por ello datos de contexto modificados (MCD) que representan una ubicación aleatoria modificada y un tiempo aleatorio modificado, cada uno resultante de la combinación;

cifrar (150) los datos de contexto modificados (MCD) para obtener el paquete de datos de inicio asegurado (SSDP) adicional que representa los datos de contexto modificados (MCD); y

almacenar (170) dicho paquete de datos de inicio asegurado (SSDP) adicional, o hacer que se almacene, en un primer almacenamiento de datos (DS1) que sea accesible para proporcionar el paquete de datos asegurado (SSDP) adicional para una autenticación asegurada posterior de un objeto físico o grupo de objetos físicos (PO(s)).

12. El método (600) de la reivindicación 11, en donde el método (400; 500) de autenticación de un objeto físico o grupo de objetos físicos (PO(s)) comprende además:

- determinar datos de inicialización (IND) adicionales basados en los mismos datos de contexto aleatorios (RCD) que dicho paquete de datos de inicio asegurado (SSDP) adicional, la determinación de los datos de inicialización (IND) adicionales que comprende:

a) detectar (210) por medio de uno o más sensores al menos una característica discriminatoria (k) de dicho objeto físico o grupo de objetos físicos (PO(s)), para obtener para cada característica discriminatoria (k) datos de identificación (IDD_k) respectivos que representan una identidad de dicho objeto físico o grupo de objetos físicos (PO(s)) relacionado;

aplicar (250) una segunda función de comprobación aleatoria (HF2) criptográfica predeterminada a un conjunto de datos resultante de combinar, según un segundo esquema de combinación (CS2) predeterminado, el uno o más datos de identificación (IDD_k) respectivos obtenidos del conjunto de dicha al menos una característica discriminatoria (k) y los datos de contexto aleatorios (RCD) para obtener un valor de comprobación aleatoria original (Ho); detectar (210) por medio de uno o más sensores al menos una característica discriminatoria (k) de dicho objeto físico o grupo de objetos físicos (PO(s)) para obtener para cada característica discriminatoria (k) datos de identificación (IDD_k) respectivos que representan una identidad de dicho objeto físico o grupo de objetos físicos (PO(s)) relacionado; o

b) aplicar (220) a cada uno de dichos datos de identificación (IDD_k) una primera función de comprobación aleatoria ($HF_{1,k}$) criptográfica predeterminada respectiva para obtener un valor de comprobación aleatoria inicial (Hi_k) respectivo relacionado con la característica discriminatoria (k) respectiva; y

aplicar (250) una segunda función de comprobación aleatoria (HF2) criptográfica predeterminada a un conjunto de datos (H) resultante de combinar, según un segundo esquema de combinación (CS2) predeterminado, el uno o más valores de comprobación aleatoria iniciales (Hi_k) respectivos obtenidos del conjunto de dicha al menos una característica discriminatoria y los datos de contexto aleatorios (RCD) para obtener un valor de comprobación aleatoria original (Ho); o

(c) aplicar (330) una segunda función de comprobación aleatoria (HF2) criptográfica predeterminada a los datos de contexto aleatorios (RCD) para obtener un valor de comprobación aleatoria original (Ho); y

emitir (270, 280; 350, 360) datos de inicialización (IND) que representan dicho valor de comprobación aleatoria original (Ho) respectivo; y

- almacenar o hacer que se almacenen dichos datos de inicialización (IND) adicionales.

13. Un sistema (TC) de provisión de manera segura de un esquema de combinación (CS) variable en el tiempo para autenticar un objeto físico o grupo de objetos físicos (PO(s)) según un método de autenticación de un objeto físico o grupo de objetos físicos (PO(s)), el sistema (TC) que está configurado para realizar el método (600) de cualquiera de las reivindicaciones anteriores.

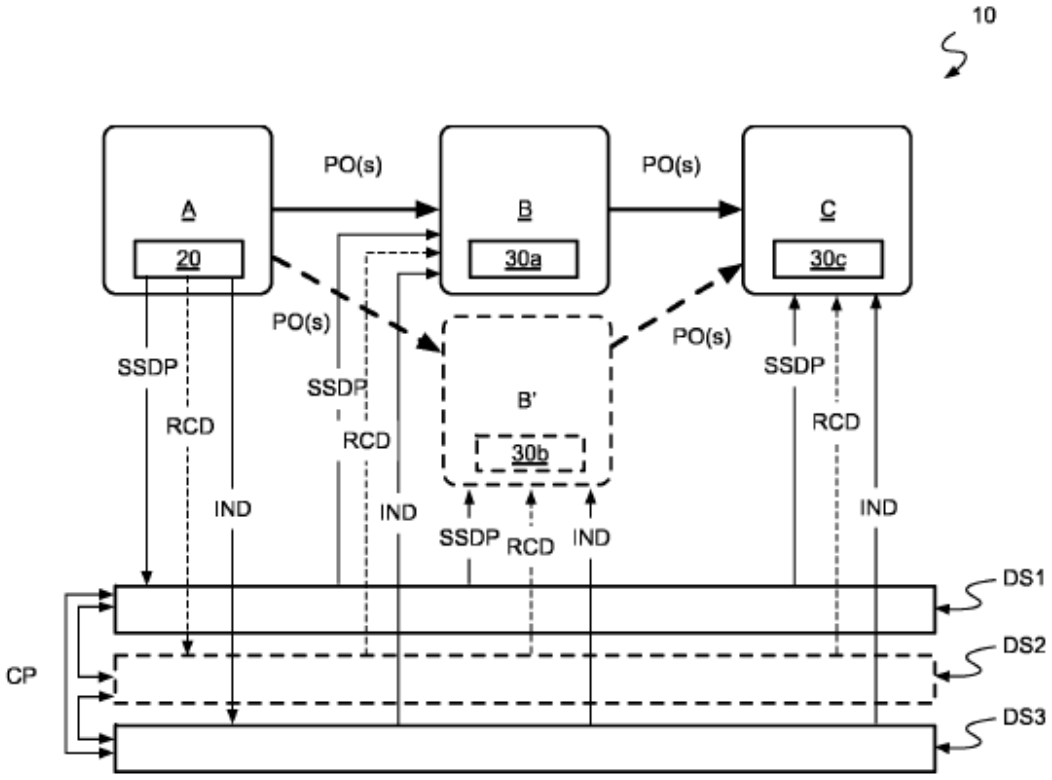
10
A
20
B
30a
C
30c
PO(s)
PO(s)
PO(s)
PO(s)
B'
30b
SSDP
RCD
IND
SSDP
RCD
IND
SSDP
RCD
IND
SSDP
RCD
IND
DS1
DS2
DS3
CP

Fig. 1

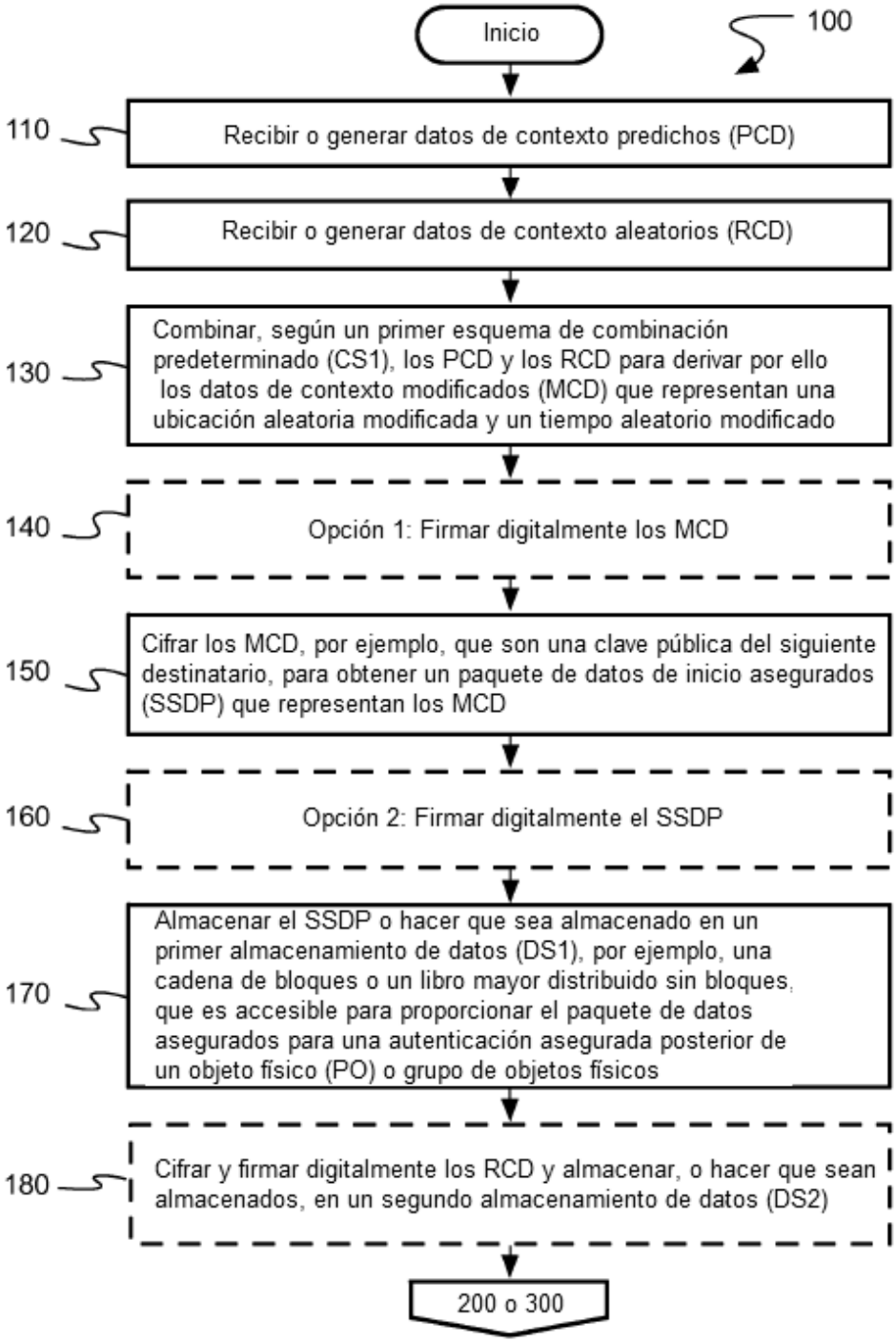
Inicio
100
110
Recibir o generar datos de contexto predichos (PCD)
120
Recibir o generar datos de contexto aleatorios (RCD)
130
Combinar, según un primer esquema de combinación predeterminado (CS1), los PCD y los RCD para derivar por ello los datos de contexto modificados (MCD) que representan una ubicación aleatoria modificada y un tiempo aleatorio modificado
140
Opción 1: Firmar digitalmente los MCD
150
Cifrar los MCD, por ejemplo, que son una clave pública del siguiente destinatario, para obtener un paquete de datos de inicio asegurados (SSDP) que representan los MCD
160
Opción 2: Firmar digitalmente el SSDP
170
Almacenar el SSDP o hacer que sea almacenado en un primer almacenamiento de datos (DS1), por ejemplo, una cadena de bloques o un libro mayor distribuido sin bloques, que es accesible para proporcionar el paquete de datos asegurados para una autenticación asegurada posterior de un objeto físico (PO) o grupo de objetos físicos
180
Cifrar y firmar digitalmente los RCD y almacenar, o hacer que sean almacenados, en un segundo almacenamiento de datos (DS2)
200 o 300

Fig. 2A

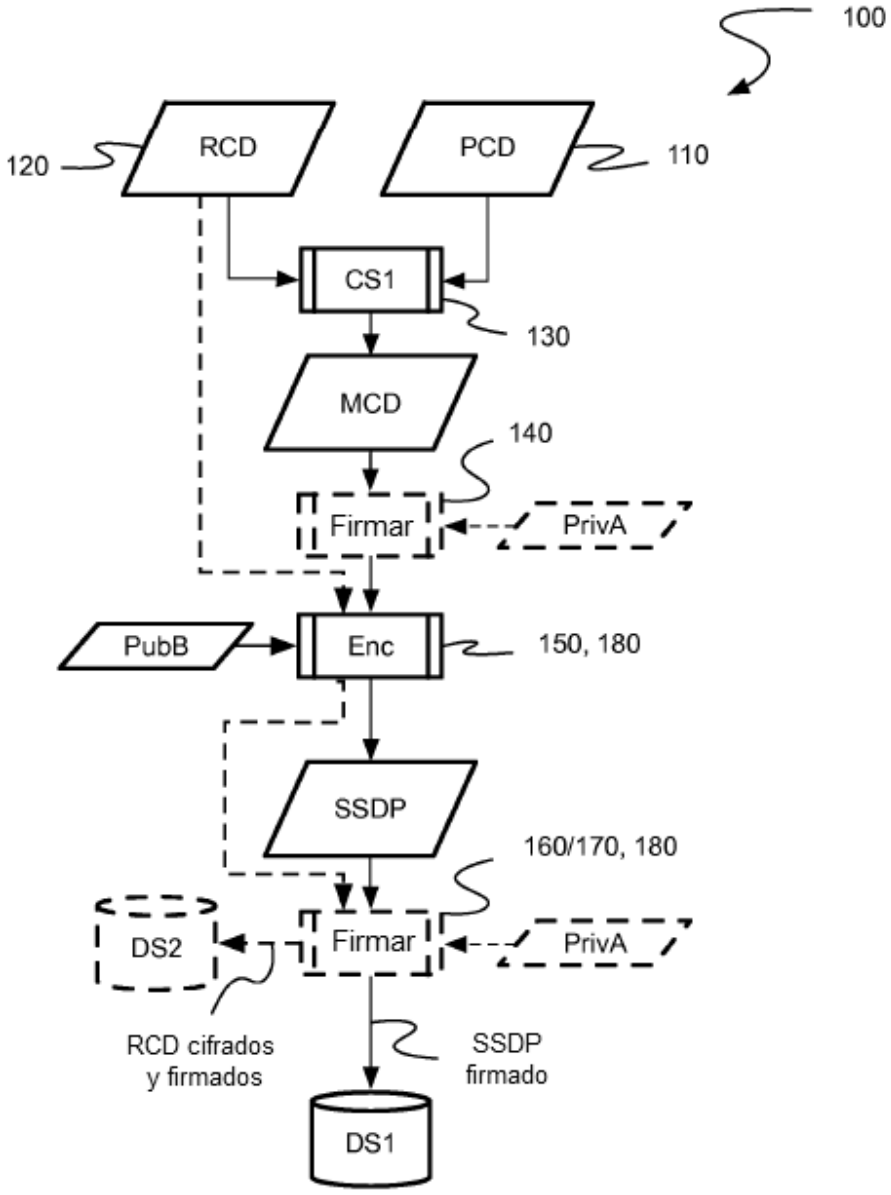
100
RCD
PCD
120
110
CS1
130
MCD
140
Firmar
PrivA
PubB
Enc
150, 180
SSDP
160/170, 180
DS2
Firmar
PrivA
RCD cifrados
y firmados
SSDP
firmado
DS1

Fig. 2B

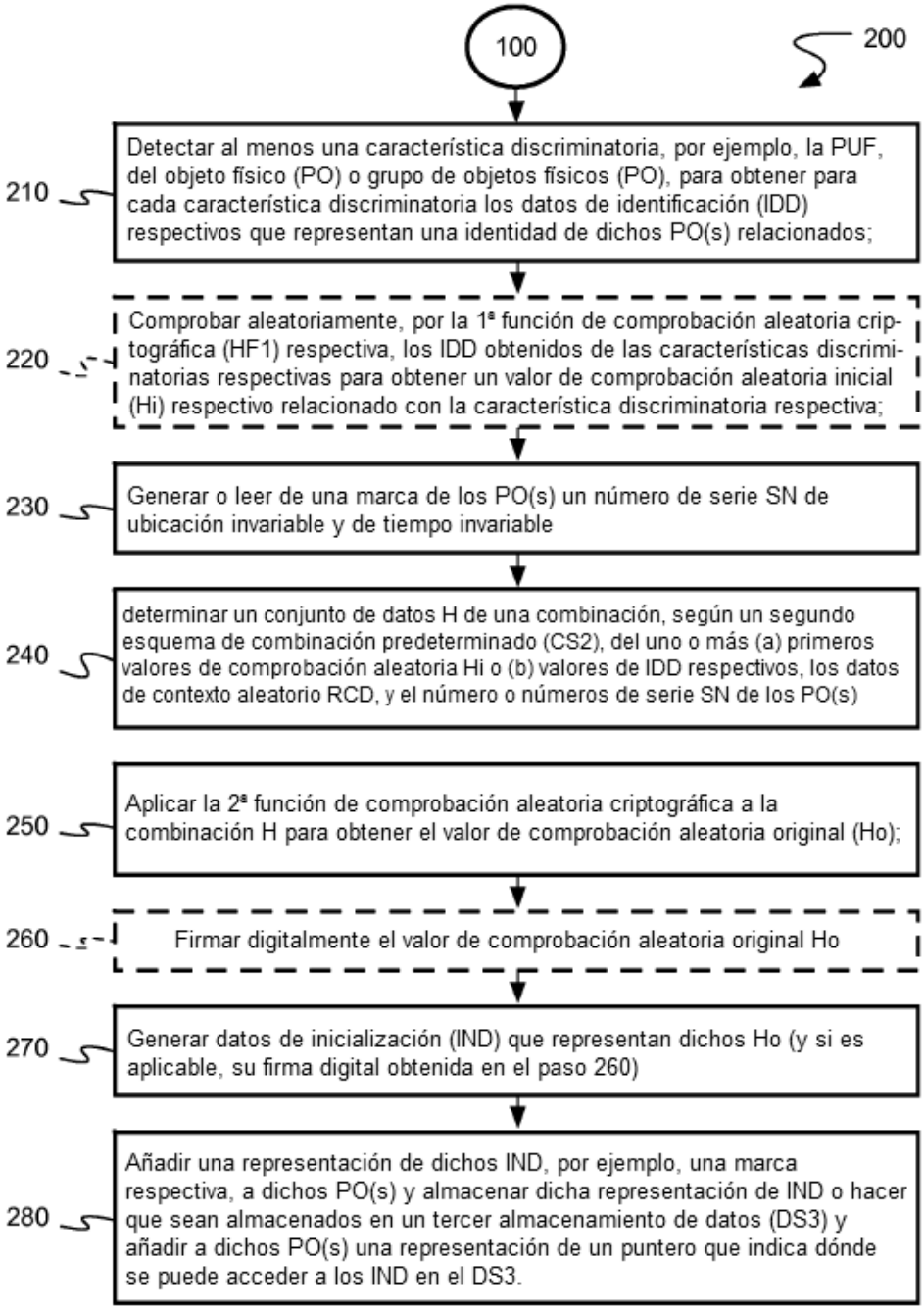
100
200
210
Detectar al menos una característica discriminatoria, por ejemplo, la PUF, del objeto físico (PO) o grupo de objetos físicos (PO), para obtener para cada característica discriminatoria los datos de identificación (IDD) respectivos que representan una identidad de dichos PO(s) relacionados;
220
Comprobar aleatoriamente, por la 1ª función de comprobación aleatoria criptográfica (HF1) respectiva, los IDD obtenidos de las características discriminatorias respectivas para obtener un valor de comprobación aleatoria inicial (Hi) respectivo relacionado con la característica discriminatoria respectiva;
230
Generar o leer de una marca de los PO(s) un número de serie SN de ubicación invariable y de tiempo invariable
240
determinar un conjunto de datos H de una combinación, según un segundo esquema de combinación predeterminado (CS2), del uno o más (a) primeros valores de comprobación aleatoria Hi o (b) valores de IDD respectivos, los datos de contexto aleatorio RCD, y el número o números de serie SN de los PO(s)
250
Aplicar la 2ª función de comprobación aleatoria criptográfica a la combinación H para obtener el valor de comprobación aleatoria original (Ho);
260
Firmar digitalmente el valor de comprobación aleatoria original Ho
270
Generar datos de inicialización (IND) que representan dichos Ho (y si es aplicable, su firma digital obtenida en el paso 260)
280
Añadir una representación de dichos IND, por ejemplo, una marca respectiva, a dichos PO(s) y almacenar dicha representación de IND o hacer que sean almacenados en un tercer almacenamiento de datos (DS3) y añadir a dichos PO(s) una representación de un puntero que indica dónde se puede acceder a los IND en el DS3.

Fig. 3A

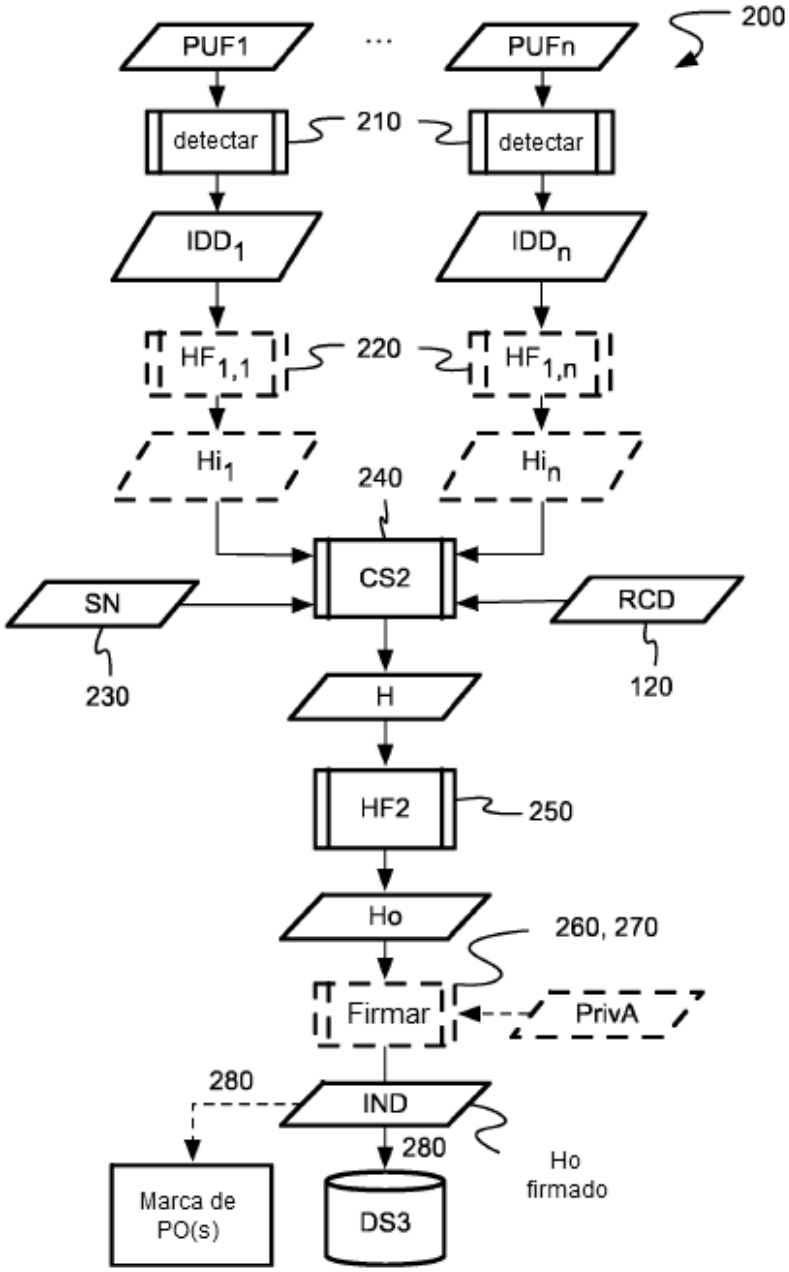
200
PUF1
...
PUFn
detectar
210
detectar
IDD1
IDDn
HF1,1
220
HF1,n
Hi1
Hin
240
CS2
SN
RCD
230
120
H
HF2
250
Ho
260, 270
Firmar
PrivA
280
IND
280
Ho
firmado
Marca de
PO(s)
DS3

Fig. 3B

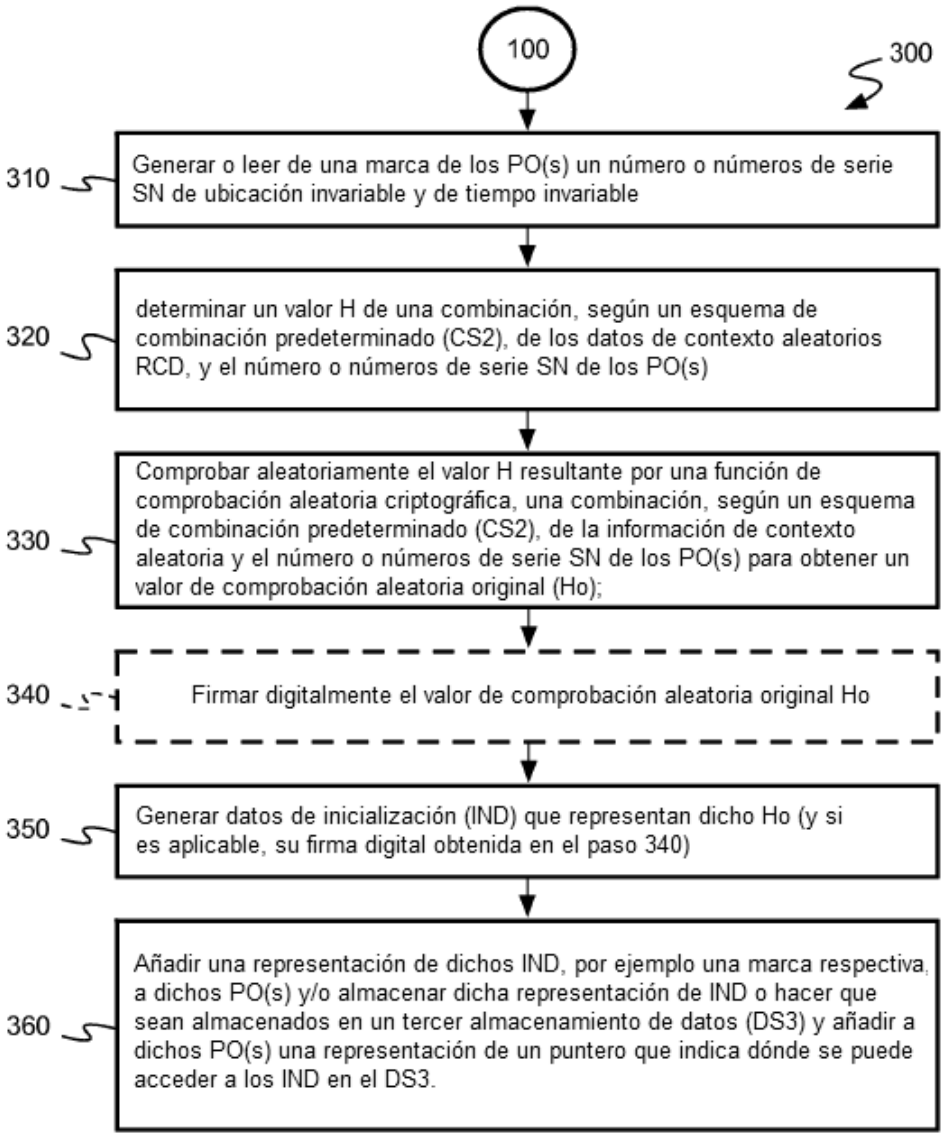
100
300
310
Generar o leer de una marca de los PO(s) un número o números de serie SN de ubicación invariable y de tiempo invariable
320
determinar un valor H de una combinación, según un esquema de combinación predeterminado (CS2), de los datos de contexto aleatorios RCD, y el número o números de serie SN de los PO(s)
330
Comprobar aleatoriamente el valor H resultante por una función de comprobación aleatoria criptográfica, una combinación, según un esquema de combinación predeterminado (CS2), de la información de contexto aleatoria y el número o números de serie SN de los PO(s) para obtener un valor de comprobación aleatoria original (Ho);
340
Firmar digitalmente el valor de comprobación aleatoria original Ho
350
Generar datos de inicialización (IND) que representan dicho Ho (y si es aplicable, su firma digital obtenida en el paso 340)
360
Añadir una representación de dichos IND, por ejemplo una marca respectiva, a dichos PO(s) y/o almacenar dicha representación de IND o hacer que sean almacenados en un tercer almacenamiento de datos (DS3) y añadir a dichos PO(s) una representación de un puntero que indica dónde se puede acceder a los IND en el DS3.

Fig. 4A

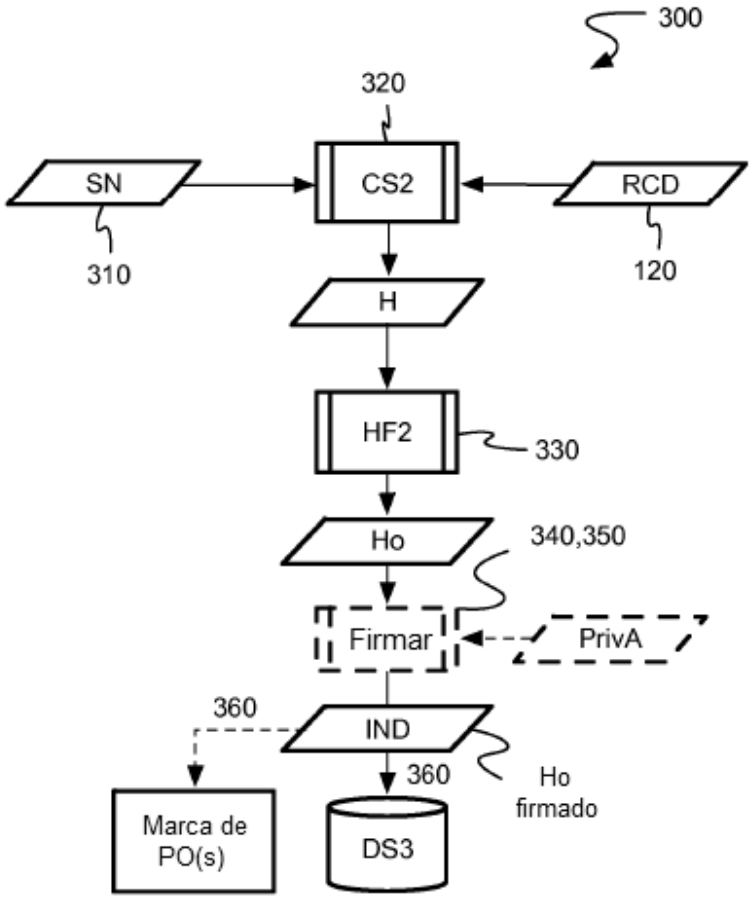
300
320
SN
CS2
RCD
310
120
H
HF2
330
Ho
340,350
Firmar
PrivA
360
IND
360
Ho
firmado
Marca de
PO(s)
DS3

Fig. 4B

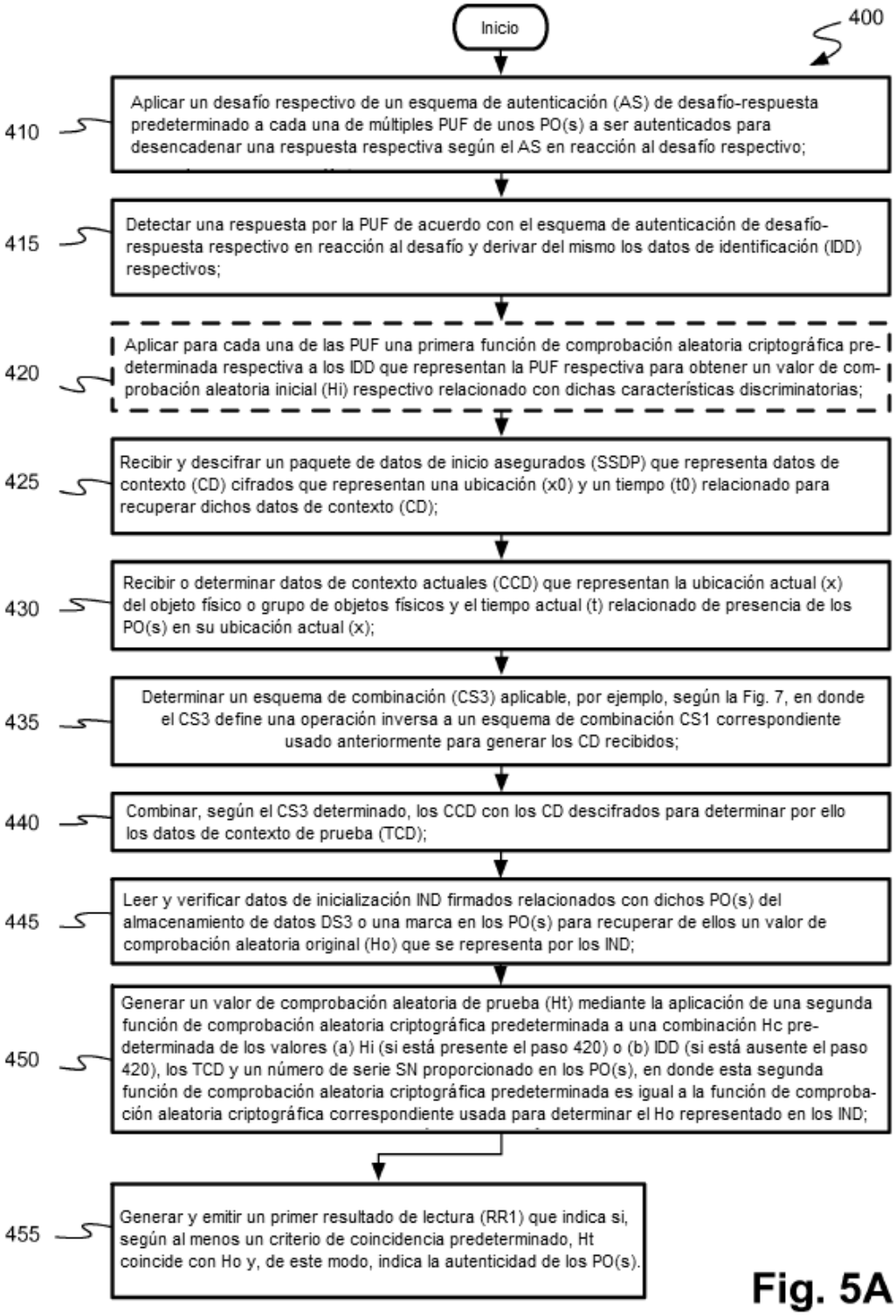
Inicio
400
410
Aplicar un desafío respectivo de un esquema de autenticación (AS) de desafío-respuesta predeterminado a cada una de múltiples PUF de unos PO(s) a ser autenticados para desencadenar una respuesta respectiva según el AS en reacción al desafío respectivo;
415
Detectar una respuesta por la PUF de acuerdo con el esquema de autenticación de desafío-respuesta respectivo en reacción al desafío y derivar del mismo los datos de identificación (IDD) respectivos;
420
Aplicar para cada una de las PUF una primera función de comprobación aleatoria criptográfica predeterminada respectiva a los IDD que representan la PUF respectiva para obtener un valor de comprobación aleatoria inicial (Hi) respectivo relacionado con dichas características discriminatorias;
425
Recibir y descifrar un paquete de datos de inicio asegurados (SSDP) que representa datos de contexto (CD) cifrados que representan una ubicación (x0) y un tiempo (t0) relacionado para recuperar dichos datos de contexto (CD);
430
Recibir o determinar datos de contexto actuales (CCD) que representan la ubicación actual (x) del objeto físico o grupo de objetos físicos y el tiempo actual (t) relacionado de presencia de los PO(s) en su ubicación actual (x);
435
Determinar un esquema de combinación (CS3) aplicable, por ejemplo, según la Fig. 7, en donde el CS3 define una operación inversa a un esquema de combinación CS1 correspondiente usado anteriormente para generar los CD recibidos;
440
Combinar, según el CS3 determinado, los CCD con los CD descifrados para determinar por ello los datos de contexto de prueba (TCD);
445
Leer y verificar datos de inicialización IND firmados relacionados con dichos PO(s) del almacenamiento de datos DS3 o una marca en los PO(s) para recuperar de ellos un valor de comprobación aleatoria original (Ho) que se representa por los IND;
450
Generar un valor de comprobación aleatoria de prueba (Ht) mediante la aplicación de una segunda función de comprobación aleatoria criptográfica predeterminada a una combinación Hc predeterminada de los valores (a) Hi (si está presente el paso 420) o (b) IDD (si está ausente el paso 420), los TCD y un número de serie SN proporcionado en los PO(s), en donde esta segunda función de comprobación aleatoria criptográfica predeterminada es igual a la función de comprobación aleatoria criptográfica correspondiente usada para determinar el Ho representado en los IND;
455
Generar y emitir un primer resultado de lectura (RR1) que indica si, según al menos un criterio de coincidencia predeterminado, Ht coincide con Ho y, de este modo, indica la autenticidad de los PO(s).

Fig. 5A

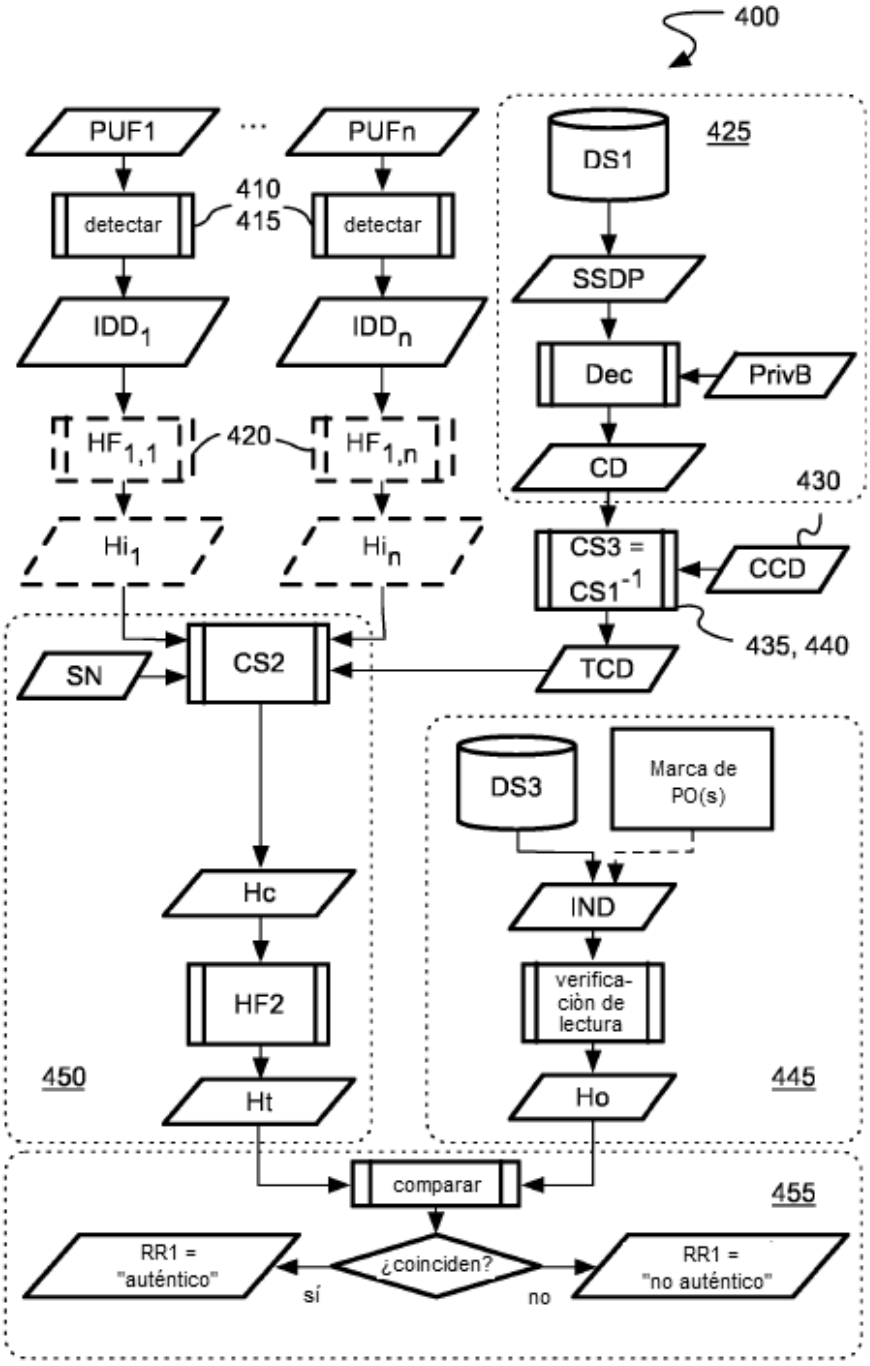
400
PUF1
PUFn
410
415
detectar
detectar
IDD1
IDDn
HF1,1
HF1,n
420
Hi1
Hin
425
DS1
SSDP
Dec
PrivB
CD
430
CS3 = CS1-1
CCD
435, 440
TCD
SN
CS2
Hc
HF2
Ht
450
DS3
Marca de PO(s)
IND
verifica-ción de lectura
Ho
445
comparar
455
RR1 = "auténtico"
¿coinciden?
sí
no
RR1 = "no auténtico"

Fig. 5B

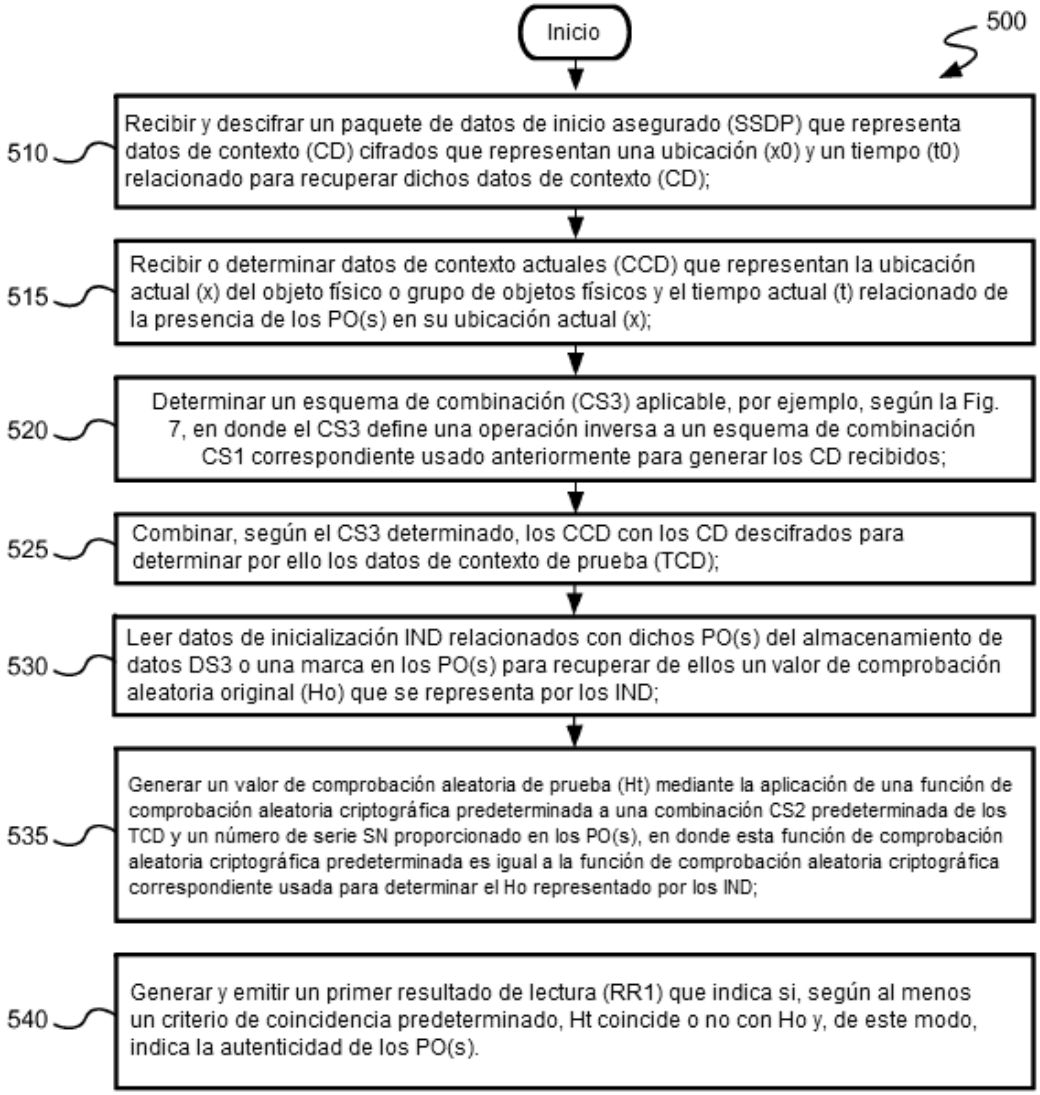
Inicio
500
510
Recibir y descifrar un paquete de datos de inicio asegurado (SSDP) que representa datos de contexto (CD) cifrados que representan una ubicación (x0) y un tiempo (t0) relacionado para recuperar dichos datos de contexto (CD);
515
Recibir o determinar datos de contexto actuales (CCD) que representan la ubicación actual (x) del objeto físico o grupo de objetos físicos y el tiempo actual (t) relacionado de la presencia de los PO(s) en su ubicación actual (x);
520
Determinar un esquema de combinación (CS3) aplicable, por ejemplo, según la Fig. 7, en donde el CS3 define una operación inversa a un esquema de combinación CS1 correspondiente usado anteriormente para generar los CD recibidos;
525
Combinar, según el CS3 determinado, los CCD con los CD descifrados para determinar por ello los datos de contexto de prueba (TCD);
530
Leer datos de inicialización IND relacionados con dichos PO(s) del almacenamiento de datos DS3 o una marca en los PO(s) para recuperar de ellos un valor de comprobación aleatoria original (Ho) que se representa por los IND;
535
Generar un valor de comprobación aleatoria de prueba (Ht) mediante la aplicación de una función de comprobación aleatoria criptográfica predeterminada a una combinación CS2 predeterminada de los TCD y un número de serie SN proporcionado en los PO(s), en donde esta función de comprobación aleatoria criptográfica predeterminada es igual a la función de comprobación aleatoria criptográfica correspondiente usada para determinar el Ho representado por los IND;
540
Generar y emitir un primer resultado de lectura (RR1) que indica si, según al menos un criterio de coincidencia predeterminado, Ht coincide o no con Ho y, de este modo, indica la autenticidad de los PO(s).

Fig. 6A

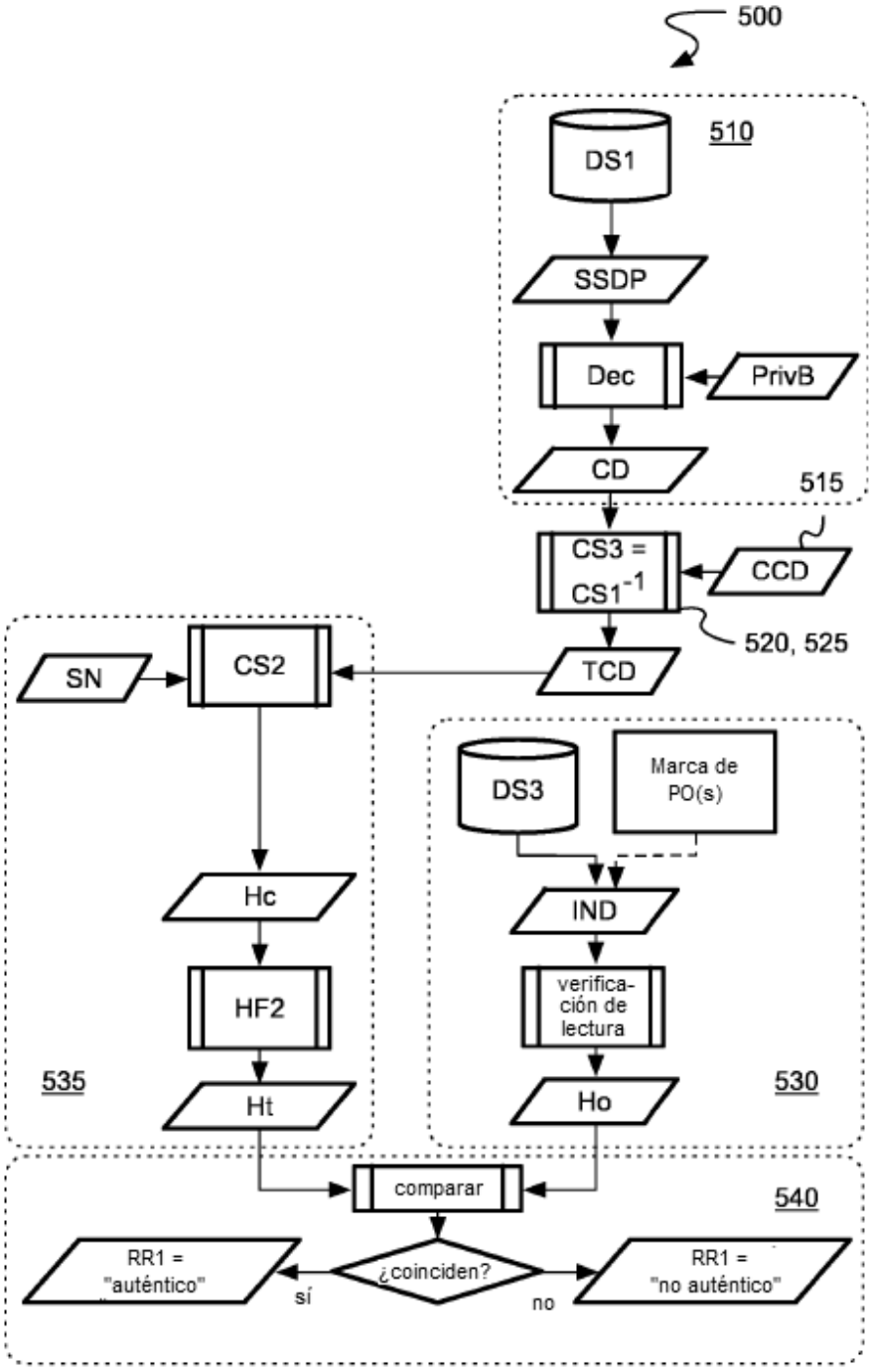
500
510
DS1
SSDP
Dec
PrivB
CD
515
CS3 = CS1-1
CCD
520, 525
TCD
SN
CS2
DS3
Marca de PO(s)
Hc
IND
HF2
verifica-ción de lectura
535
Ht
Ho
530
comparar
540
RR1 = "auténtico"
¿coinciden?
sí
no
RR1 = "no auténtico"

Fig. 6B

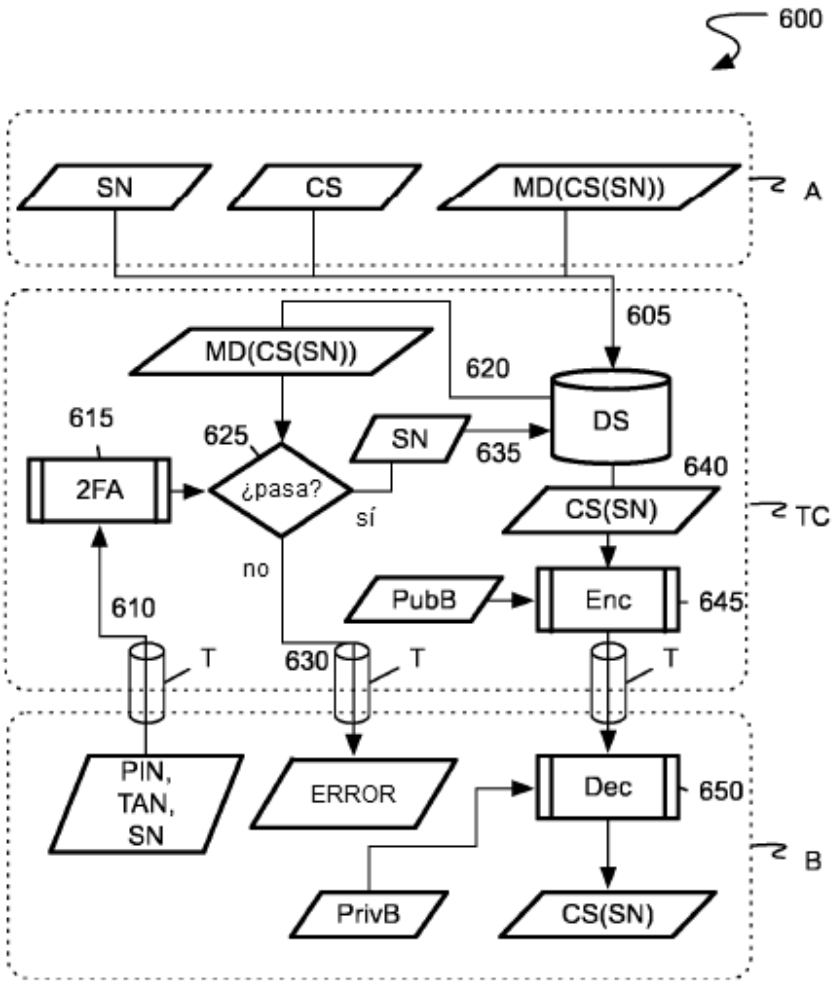
600
SN
CS
MD(CS(SN))
A
605
MD(CS(SN))
620
DS
615
625
SN
635
640
2FA
¿pasa?
sí
CS(SN)
TC
no
PubB
Enc
645
610
T
630
T
T
PIN,
TAN,
SN
ERROR
Dec
650
B
PrivB
CS(SN)

Fig. 7

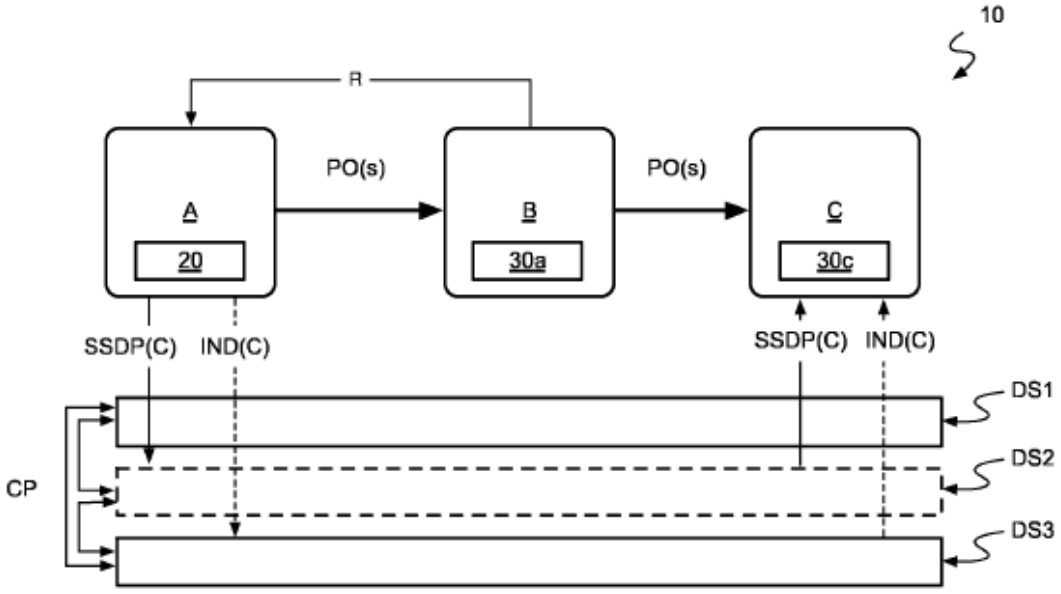
10
R
A
20
PO(s)
B
30a
PO(s)
C
30c
SSDP(C)
IND(C)
SSDP(C)
IND(C)
DS1
DS2
DS3
CP

Fig. 8A

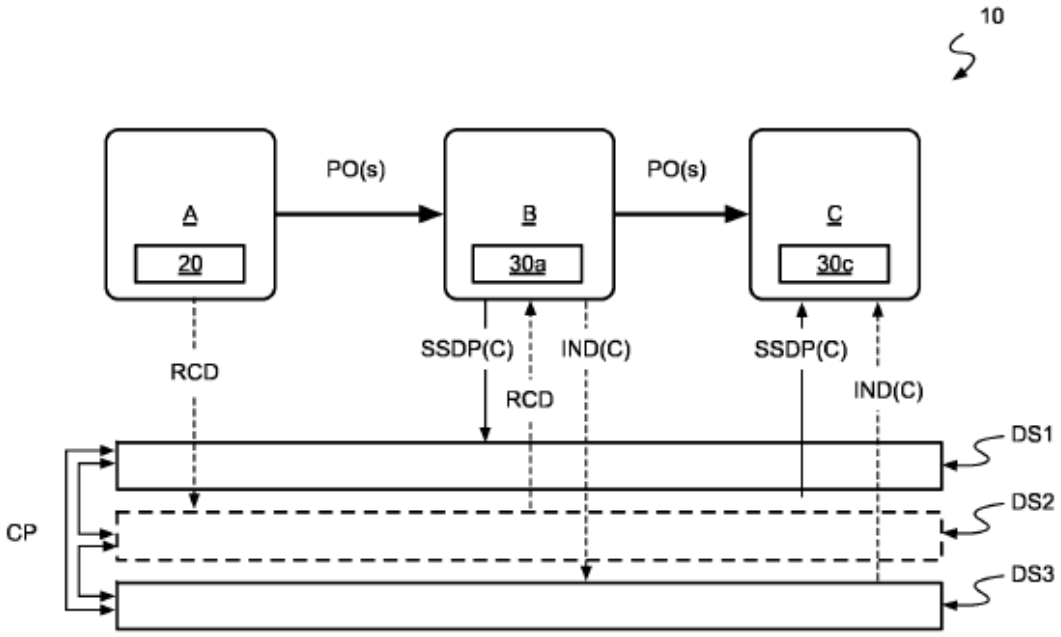
10
A
20
PO(s)
B
30a
PO(s)
C
30c
RCD
SSDP(C)
IND(C)
RCD
SSDP(C)
IND(C)
DS1
DS2
DS3
CP

Fig. 8B