(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 716 739**

(51) Int. CI.:

G06F 3/12	(2006.01)	***H04L 29/06***	(2006.01)
B41J 2/175	(2006.01)	***H04N 1/44***	(2006.01)
B41J 29/38	(2006.01)		
G03G 15/08	(2006.01)		
G03G 21/18	(2006.01)		
G06F 21/44	(2013.01)		
G06F 21/57	(2013.01)		
G06F 21/60	(2013.01)		
H04L 9/08	(2006.01)		
H04L 9/32	(2006.01)		

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **27.10.2016 PCT/US2016/059107**

(87) Fecha y número de publicación internacional: **03.05.2018 WO18080495**

(96) Fecha de presentación y número de la solicitud europea: **27.10.2016 E 16797682 (8)**

(97) Fecha y número de publicación de la concesión europea: **20.02.2019 EP 3332318**

(54) Título: **Autenticación de elemento reemplazable**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.06.2019

(73) Titular/es:

HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P. (100.0%)
10300 Energy Drive
Spring TX 77389, US

(72) Inventor/es:

PANSHIN, STEPHEN D.;
WARD, JEFFERSON P. y
NESS, ERIK D.

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Autenticación de elemento reemplazable

Antecedentes

Dispositivos que usan elementos reemplazables incluyen dispositivos de impresión, incluyendo impresoras autónomas, máquinas copiadoras y dispositivos todo en uno (AIO) que pueden realizar múltiples funciones, tales como imprimir, copiar, escanear y/o enviar por fax. Ejemplos de elementos reemplazables para tales dispositivos de impresión incluyen tinta, tóner y/u otros tipos de colorante, incluyendo colorante bidimensional (2D). Otros ejemplos elementos de recambio, específicamente para dispositivos de impresión tridimensionales (3D), incluyen agente de impresión 3D y material de construcción de impresión 3D.

El documento US2007/077074 se refiere a consumibles para aparatos de impresión. Según los métodos descritos en el mismo, cuando se agota un consumible tal como un suministro de colorante, se puede establecer un código de autenticación en un valor predeterminado. El documento WO2006066270 se refiere a dispositivos de impresión operables exclusivamente con dispositivos consumibles respectivos, en donde otro dispositivo consumible almacena datos de identificación para ser operable con una serie de dispositivos de impresión.

Breve descripción de los dibujos

La FIG. 1 es un diagrama de un cartucho de sustancia de impresión de ejemplo para un dispositivo de impresión.

La FIG. 2 es un diagrama de una tabla de ejemplo de un conjunto reducido de contraseñas, o valores de autenticación, que se pueden almacenar para identidades de cartucho, o identidades de elementos reemplazables, dentro de un cartucho o elemento reemplazable.

La FIG. 3 es un diagrama de flujo de un método de ejemplo que puede realizar un cartucho de sustancia de impresión u otro elemento reemplazable para un dispositivo.

La FIG. 4 es un diagrama de flujo de un método de ejemplo que un puede realizar cartucho de sustancia de impresión u otro elemento reemplazable para un dispositivo para implementar una parte del método de la FIG. 3.

La FIG. 5 es un diagrama de flujo de otro método de ejemplo que puede realizar un cartucho de sustancia de impresión u otro elemento reemplazable para un dispositivo.

La FIG. 6 es un diagrama de flujo de un método de ejemplo que puede realizar un cartucho de sustancia de impresión u otro elemento reemplazable para un dispositivo para implementar una parte del método de la FIG. 5.

La FIG. 7 es un diagrama de flujo de un tercer método de ejemplo que puede realizar un cartucho de sustancia de impresión u otro elemento reemplazable para un dispositivo para seleccionar una identidad de elemento reemplazable, que es consistente con las descripciones de los métodos de las FIG. 4 y 6.

Descripción detallada

Como se ha señalado en los antecedentes, los dispositivos que usan elementos reemplazables incluyen dispositivos de impresión. Un suministro de sustancia de impresión, tal como colorante u otro tipo de sustancia de impresión, se almacena en un cartucho que se puede insertar en un dispositivo de impresión. Cuando el suministro llega a estar agotado, el cartucho se puede reemplazar por un cartucho que tiene un suministro nuevo de la sustancia de impresión en cuestión. Los cartuchos que tienen diferentes tipos de sustancias de impresión también se pueden intercambiar según se desee. Como ejemplo, un cartucho que tiene tinta de propósito general se puede intercambiar por un cartucho que tiene tinta de calidad fotográfica dentro de un dispositivo de impresión de inyección de tinta, según se desee.

Los fabricantes de dispositivos de impresión típicamente también fabrican o de otro modo suministran la sustancia de impresión usada en los dispositivos de impresión. Desde la perspectiva del usuario final, el uso de cartuchos de sustancias de impresión suministrados por el fabricante o aprobados por el fabricante puede facilitar la salida deseada de los dispositivos de impresión y/o inhibir el daño a los dispositivos de impresión. Para el fabricante de equipo original (OEM) puede ser difícil garantizar la salida del dispositivo de impresión o el funcionamiento del dispositivo de impresión si el dispositivo de impresión usa cartuchos de terceros. Una sustancia de impresión de terceros está fuera del control del OEM. Por ejemplo, podría proporcionar una salida de impresión diferente o conllevar un riesgo patente de acortamiento de la vida útil del dispositivo de impresión. En algunos casos, tales como impresoras 3D, incluso podría haber un riesgo de seguridad para un usuario cuando una sustancia de impresión es una sustancia de impresión no aprobada. En ciertos casos, el uso de una sustancia de impresión no aprobada puede afectar a una garantía asociada con el dispositivo de impresión.

Por lo tanto, los fabricantes pueden instilar cartuchos con seguridad de autenticación. Un dispositivo de impresión puede interrogar al cartucho para determinar si es auténtico. Si el cartucho no es auténtico (por ejemplo, no está aprobado por OEM), entonces el dispositivo de impresión puede iniciar un cierto procedimiento, tal como, por

ejemplo, informar al usuario final, tal como inmediatamente o inmediatamente después de la instalación.

En la solicitud de patente PCT presentada el 17 de junio de 2016, y la solicitud de patente PCT asignada nº PCT/US2016/38211, se describe un esquema de autenticación para un cartucho de sustancia de impresión para un dispositivo de impresión, y de manera más general para un elemento reemplazable para un dispositivo (anfitrión) en el que se puede instalar el elemento (es decir, de manera más general, el dispositivo al que se puede conectar el dispositivo). El cartucho de sustancia de impresión almacena una serie de valores de autenticación o contraseñas. El cartucho incluye una lógica (tal como circuitería como un procesador y una memoria que almacena el código que ejecuta el procesador) para permitir la recuperación de solo un subconjunto de estos valores de autenticación. A medida que se solicitan diferentes valores de autenticación desde el cartucho, el cartucho puede rastrear la serie de valores diferentes que se han devuelto. Una vez que el cartucho haya proporcionado el número máximo de tales valores de autenticación únicos, no proporcionará ninguno de los otros valores de autenticación que se almacenaron originalmente en el cartucho. Sin embargo, el cartucho continúa proporcionando los valores de autenticación previos que se habían solicitado y devuelto.

Como ejemplo, un cartucho de sustancia de impresión puede almacenar sesenta y cuatro contraseñas o valores de autenticación diferentes. De estos sesenta y cuatro, el cartucho puede emitir no más de dieciséis de las diferentes contraseñas. Una vez que el cartucho haya proporcionado dieciséis contraseñas diferentes, no proporcionará ninguna de las otras cuarenta y ocho contraseñas que se almacenaron en el cartucho. Sin embargo, el cartucho puede continuar respondiendo a las solicitudes de las dieciséis contraseñas diferentes que ya ha proporcionado.

El cartucho de sustancia de impresión también puede almacenar valores de comprobación aleatoria de los valores de autenticación o contraseñas. Los valores de comprobación aleatoria proporcionan una forma de determinar si es correcto un valor de autenticación dado que ha proporcionado el cartucho. El cartucho puede proporcionar los valores de comprobación aleatoria de los valores de autenticación bajo petición, incluso para los valores que el cartucho no emitirá. En el ejemplo del párrafo anterior, por ejemplo, el cartucho puede proporcionar los valores de comprobación aleatoria para las sesenta y cuatro contraseñas, aún cuando el cartucho no proporcionará más de dieciséis de las sesenta y cuatro contraseñas.

Un esquema de autenticación que usa tal cartucho de sustancia de impresión puede incluir un dispositivo de impresión anfitrión que podría solicitar cuatro contraseñas o valores de autenticación diferentes, almacenados en el cartucho. Diferentes dispositivos de impresión pueden solicitar y probablemente solicitarán contraseñas diferentes de un cartucho dado. De manera similar, un dispositivo de impresión determinado puede solicitar y probablemente solicitará diferentes contraseñas de diferentes cartuchos.

Tener un cartucho de sustancia de impresión que devuelve un número menor de valores de autenticación que el número total de valores de autenticación almacenados originalmente en el cartucho hace que sea mucho más difícil para un tercero frustrar tal esquema de autenticación. Incluso si un tercero supera otras medidas de seguridad para obtener los dieciséis valores de autenticación que el cartucho “cederá”, o emitirá o proporcionará, la probabilidad de que un cartucho de terceros que almacene solo estos dieciséis valores sea autenticado por un dispositivo de impresión es baja. En el esquema de autenticación de ejemplo que se ha presentado anteriormente, el dispositivo de impresión puede solicitar y probablemente solicitará al menos un valor de autenticación que no sea uno de los dieciséis valores que comparte el cartucho de terceros, haciendo improbable que cualquier dispositivo de impresión dado autenticase con éxito tal cartucho.

Sin embargo, en la presente memoria se describen técnicas para otro tipo de cartucho de sustancia de impresión para un dispositivo de impresión, y de manera más general para un elemento reemplazable para un dispositivo (anfitrión) en el que se puede instalar el elemento o de manera más general al cual se puede conectar el elemento, que puede ser capaz de pasar con éxito la autenticación en el esquema de autenticación que se ha descrito. El cartucho de sustancia de impresión almacena una serie de valores de autenticación o contraseñas, para una serie de identidades de cartuchos diferentes. Los valores de autenticación que almacena el cartucho de sustancia de impresión para cada identidad de cartucho, sin embargo, pueden no ser un conjunto completo de valores de autenticación.

Por ejemplo, en la solicitud de patente PCT de la técnica anterior, un cartucho puede almacenar sesenta y cuatro valores de autenticación, pero solo revelar dieciséis de estos valores de autenticación. Diferentes cartuchos que tienen diferentes identidades de cartucho pueden almacenar diferentes conjuntos de sesenta y cuatro valores de autenticación, con cada cartucho que revela dieciséis de los sesenta y cuatro valores de autenticación que almacena. De este modo, cada cartucho puede ser interrogado para identificar los dieciséis valores de autenticación que emitirá. Entonces se puede construir un nuevo cartucho que almacene los dieciséis valores de autenticación para cada uno de estos cartuchos, por sus identidades.

Por lo tanto, un cartucho según las técnicas descritas en la presente memoria puede no tener un conjunto completo de valores de autenticación para cualquier identidad de cartucho dada, sino más bien puede tener un conjunto incompleto de valores de autenticación para cada uno de los cuales puede ser un gran número de identidades de cartucho diferentes. Cuando tal cartucho se instala en un dispositivo de impresión, puede seleccionar una de sus identidades de cartucho a usar para la autenticación dentro del dispositivo de impresión. Si los valores de

autenticación que el cartucho almacena para la identidad seleccionada incluyen los que solicita el dispositivo de impresión, entonces el cartucho pasará con éxito la autenticación dentro del dispositivo.

Se puede considerar que una identidad de cartucho, y de manera más general una identidad de elemento reemplazable abarca los valores de comprobación aleatoria para un conjunto completo de valores de autenticación. En la solicitud de patente PCT referenciada, por ejemplo, aún cuando un cartucho solo revelará un número limitado de los valores de autenticación que almacena, el cartucho puede revelar los valores de comprobación aleatoria para todos los valores de autenticación que almacena. Los valores de comprobación aleatoria pueden ser valores de comprobación aleatoria unidireccionales, de modo que los valores de autenticación no se pueden determinar a partir de los valores de comprobación aleatoria. Cada valor de comprobación aleatoria se puede generar usando una función de comprobación aleatoria unidireccional de un valor de autenticación correspondiente y una identidad única del cartucho en cuestión, o está vinculado de otro modo a la identidad única del cartucho en cuestión. Por lo tanto, los valores de comprobación aleatoria que almacena el cartucho se pueden considerar como o como parte de la identidad del cartucho, dado que los valores de comprobación aleatoria codifican implícitamente la identidad única del cartucho.

Como tal, un cartucho según las técnicas descritas en la presente memoria puede almacenar los valores de comprobación aleatoria recuperados de un gran número de cartuchos diferentes de la solicitud de patente PCT referenciada como sus múltiples identidades de cartuchos. Para cada identidad de cartucho - es decir, para cada conjunto de valores de comprobación aleatoria de un conjunto completo correspondiente de valores de autenticación - el cartucho almacena una serie de valores de autenticación. Sin embargo, el número de valores de autenticación que el cartucho almacena para una identidad de cartucho puede ser menor que el número de valores de autenticación para los cuales hay valores de comprobación aleatoria. Como se ha señalado anteriormente, esto es debido a que un cartucho de la solicitud de patente PCT referenciada no revelará todos los valores de autenticación que almacena, pero puede revelar los valores de comprobación aleatoria para todos los valores de autenticación. De este modo, un cartucho según las técnicas descritas en la presente memoria puede incluir los conjuntos limitados de valores de autenticación que revelarán un número de tales cartuchos de la solicitud de patente PCT referenciada, junto con los valores de comprobación aleatoria para todos los valores de autenticación de esos cartuchos

La FIG. 1 muestra un cartucho 100 de sustancia de impresión de ejemplo para un dispositivo de impresión. El cartucho 100 incluye un suministro 102 de sustancia de impresión. El cartucho 100 puede contener cualquier volumen de sustancia de impresión, tal como desde varios mililitros hasta decenas de litros. Diferentes ejemplos de sustancia de impresión incluyen tinta para un dispositivo de impresión de inyección de tinta, y tóner líquido o en polvo para un dispositivo de impresión láser. Tales tinta y tóner son en sí mismos ejemplos de colorantes bidimensionales (2D), que es un colorante usado por un dispositivo de impresión adecuado para formar imágenes en medios como papel que mínimamente si es que se extienden en una tercera dimensión perpendicular a las dos dimensiones que definen el plano de la superficie del medio en el que se han formado las imágenes. Otros ejemplos de sustancia de impresión incluyen un agente de impresión tridimensional (3D) y material de construcción de impresión 3D, que se usan por un dispositivo de impresión 3D adecuado para formar un objeto 3D que típicamente se puede quitar de cualquier sustrato sobre el que se construye el objeto. Ciertas sustancias de impresión, tales como tinta, se pueden usar para impresión tanto 2D como 3D.

El cartucho 100 de sustancia de impresión incluye una lógica 104. La lógica 104 se puede implementar como circuitería dentro del cartucho 100. Por ejemplo, la lógica 104 puede incluir un procesador y un medio de almacenamiento de datos legible por ordenador no volátil que almacena código ejecutable por ordenador que ejecuta el procesador. A este respecto, entonces, en una implementación, la lógica 104 puede incluir un microprocesador y un software integrado almacenado en el microprocesador en sí mismo, donde el medio de almacenamiento de datos legible por ordenador no volátil se integra dentro del microprocesador. En otra implementación, la lógica 104 puede incluir un microprocesador y un software integrado dentro de un medio no volátil separado del microprocesador.

Como otro ejemplo, la lógica 104 puede ser o incluir un circuito integrado de aplicaciones específicas (ASIC) o una agrupación de puertas programables en campo (FPGA). De manera más general, a este respecto, la lógica 104 se puede implementar usando puertas lógicas. Como tercer ejemplo, la lógica 104 se puede implementar como cualquier combinación de un procesador, software almacenado dentro del procesador o en un medio separado del procesador, y puertas lógicas.

El cartucho 100 de sustancia de impresión incluye una memoria 106 no volátil. La memoria 106 puede ser una memoria de semiconductores, y es no volátil en que cuando se quita la alimentación del cartucho 100, la memoria 106 todavía conserva su contenido. La memoria 106 almacena identidades 110A, 110B, ..., 110M de cartuchos, que se conocen colectivamente como identidades 110 de cartucho. Las identidades 110 de cartucho también se pueden conocer como identidades de elementos reemplazables. Para cada identidad 110A, 110B, ..., 110M de cartucho, la memoria 106 almacena múltiples contraseñas 108A, 108B, ..., 108M, respectivamente, que se conocen colectivamente como contraseñas 108. Las contraseñas 108 también se conocen como valores de autenticación.

Las contraseñas 108, o valores de autenticación, se almacenan por el cartucho 100 de modo que el cartucho 100 pueda demostrar a un dispositivo de impresión anfitrión que es auténtico. Dicho de otra manera, las contraseñas 108

se usan para autenticar el cartucho 100 dentro del dispositivo de impresión. Las contraseñas 108 cada una puede ser una serie de bits, tal como 256 bits.

Cada identidad 110 de cartucho puede ser o incluir valores de comprobación aleatoria para al menos las contraseñas 108 que la memoria 106 no volátil almacena para la identidad 110 de cartucho en cuestión. Los valores de comprobación aleatoria se almacenan de modo que el cartucho 100 pueda demostrar a un dispositivo de impresión anfitrión que las contraseñas 108 de una identidad 110 de cartucho correspondiente son correctas. Dicho de otra manera, los valores de comprobación aleatoria que constituyen una identidad 110 de cartucho se usan para verificar las contraseñas 108 de esta misma identidad 110 proporcionadas por el cartucho 100. Los valores de comprobación aleatoria pueden ser valores de comprobación aleatoria unidireccionales de las contraseñas 108 de una identidad 110 de cartucho correspondiente, lo que significa que una contraseña 108 no se puede determinar solo conociendo su valor de comprobación aleatoria correspondiente, incluso si se conoce la función de comprobación aleatoria unidireccional usada para generar el valor de comprobación aleatoria a partir de la contraseña.

En el encendido del cartucho 100, tal como en el encendido del dispositivo de impresión en el que ha de ser instalado el cartucho 100, la lógica 104 puede tener que seleccionar una de las identidades 110 para asumir la autenticación del cartucho 100 dentro del dispositivo, hasta que el cartucho 100 se apague y entonces se encienda de nuevo. El encendido del cartucho 100 puede incluir el ciclo de alimentación del cartucho 100, tal como apagando y luego encendiendo el dispositivo de impresión en el que se ha instalado el cartucho 100 o realizando un reinicio por hardware o en frío del dispositivo. El encendido del cartucho 100 puede incluir insertar el cartucho 100 por primera vez en el dispositivo de impresión, después de la retirada del cartucho 100 de un recipiente en el que se ha proporcionado o después de la retirada del cartucho 100 de un dispositivo de impresión diferente en que se ha instalado. El encendido del cartucho 100 puede incluir quitar el cartucho 100 del dispositivo de impresión en el que se ha instalado, y reinstalar el cartucho 100 en este mismo dispositivo, mientras que el dispositivo de impresión permanece encendido. El encendido del cartucho 100 también puede ocurrir cuando se abre una puerta por la cual se accede al cartucho 100 dentro del dispositivo de impresión. El encendido del cartucho 100 puede incluir además encender solo la lógica 100 en sí misma, tal como cuando se ha completado la impresión de un trabajo de impresión usando el cartucho 100, y/o cuando se recibe un trabajo de impresión.

Una vez que la lógica 104 ha seleccionado una identidad 110 a asumir para la autenticación del cartucho 100 dentro del dispositivo de impresión en el que se ha instalado, puede no ser permitido por el dispositivo que cambie su identidad 110 hasta que el cartucho 100 haya sido encendido de nuevo. Esto es debido a que el dispositivo de impresión puede, después de solicitar y recibir los valores de comprobación aleatoria que constituyen la identidad 110, usar estos valores de comprobación aleatoria para validar cualquier contraseña 108 recibida previamente o posteriormente, y los valores de comprobación aleatoria que constituyen la identidad 110 asumida pueden ser correctos solo para verificar las contraseñas 108 de esta identidad 110. De este modo, una vez que la lógica 104 ha seleccionado su identidad 110, puede ofrecer solo las contraseñas 108 que la memoria 106 no volátil almacena para esta identidad 110 para autenticación, y no las contraseñas 108 que la memoria 106 almacena para cualquier otra identidad 110, hasta otro encendido del cartucho 100. Si el cartucho 100 falla en la autenticación – debido a que, por ejemplo, la memoria 106 almacena un conjunto limitado e incompleto de contraseñas 108 para la identidad 110 que se ha seleccionado, donde este conjunto no incluye la contraseña solicitada - el cartucho 100 de este modo puede ser incapaz de intentar la autenticación de nuevo hasta que se haya encendido de nuevo.

A continuación se describen diferentes técnicas en cuanto a cómo el cartucho 100 (y más específicamente la lógica 104 del mismo) puede seleccionar qué identidad 110 asumir para la autenticación con un dispositivo de impresión. Algunas técnicas se pueden emplear cuando un dispositivo de impresión solicita la identidad de cartucho 100 antes de solicitar cualquier contraseña del cartucho 100, donde la identidad en este sentido puede incluir los valores de comprobación aleatoria por los cuales las contraseñas solicitadas posteriormente se verificarán para su validez. Se pueden emplear otras técnicas cuando un dispositivo de impresión no solicita la identidad del cartucho 100 antes de solicitar una contraseña del cartucho 100, donde la identidad en este sentido puede incluir del mismo modo los valores de comprobación aleatoria mediante los cuales se verifican las contraseñas para su validez. Se pueden emplear otras técnicas cuando el cartucho 100 ha seleccionado previamente una identidad 110 que dio como resultado una autenticación con éxito del cartucho 100.

La FIG. 2 muestra una tabla 200 de ejemplo de un conjunto reducido de contraseñas, o valores de autenticación, que se pueden almacenar para identidades de cartuchos, o identidades de elementos reemplazables, dentro de un cartucho o elemento reemplazable. En la tabla 200 de ejemplo, las columnas 202 corresponden a identidades de cartucho únicas almacenadas dentro de un cartucho. En la FIG. 2, hay M de tales identidades de cartucho únicas. En la tabla 200 de ejemplo, las filas 204 corresponden a contraseñas únicas que se pueden solicitar para cualquier identidad de cartucho. En la FIG. 2, hay dieciséis de tales contraseñas únicas, pero en otra implementación, puede haber sesenta y cuatro o un número diferente de contraseñas únicas. El número de identidades M puede ser mayor que el número de contraseñas únicas que se pueden solicitar para cualquier identidad en un orden de 10, 100, 1000 o más. Por ejemplo, puede haber cientos, miles, decenas de miles, o más identidades de cartucho almacenadas dentro de un cartucho.

Las X en las celdas de la tabla 200 denotan las contraseñas únicas que el cartucho realmente almacena para cada

identidad de cartucho. Por ejemplo, para la identidad 1 de cartucho, el cartucho almacena las contraseñas 4, 5, 6 y 7. Para la identidad 2, el cartucho almacena las contraseñas 2, 8, 10 y 14; para la identidad 3, el cartucho almacena las contraseñas 5, 8, 10 y 14; y para la identidad 4, el cartucho almacena las contraseñas 4, 5, 9 y 16. Para la identidad 5, el cartucho almacena las contraseñas 3, 7, 11 y 14; y para la identidad M, el cartucho almacena las contraseñas 1, 12, 13 y 15.

La contraseña que el cartucho almacena para una identidad dada es generalmente y típicamente única para esa identidad, incluso si comparte el mismo número de contraseña que el de una contraseña que el cartucho almacena para otra identidad. Por ejemplo, la contraseña 5 para la identidad 1 es típicamente diferente de la contraseña 5 para la identidad 3. De manera similar, la contraseña 5 para cada una de las identidades 1 y 3 es típicamente diferente de la contraseña 5 de la identidad 4.

Un dispositivo de impresión en el que el cartucho de la FIG. 2 se ha instalado puede solicitar cualquier número de contraseñas desde 1 hasta 16. El dispositivo de impresión puede solicitar múltiples contraseñas. Cada identidad 1 hasta M de cartucho puede ser o incluir los valores de comprobación aleatoria por los cuales se pueden verificar todas las contraseñas 1 hasta 16 de esa identidad, aún cuando el cartucho solo almacena cuatro contraseñas para cada identidad.

Por ejemplo, si el cartucho ha asumido la identidad 2 de cartucho, será capaz de ser autenticado con éxito si se solicitan solo una o más de las contraseñas 2, 8, 10 y 14. Esto es debido a que para la identidad 2 de cartucho, el cartucho almacena las contraseñas 2, 8, 10 y 14. Si el cartucho ha asumido la identidad 2 de cartucho y se solicita cualquier contraseña distinta de 2, 8, 10 o 14, el cartucho no será capaz de ser autenticado con éxito. Esto es debido a que el cartucho no almacena ninguna contraseña distinta de las contraseñas 2, 8, 10 y 14 para la identidad 2 de cartucho.

En la solicitud de patente PCT referenciada, un cartucho puede almacenar un conjunto completo de contraseñas 1 hasta 16 y un conjunto correspondiente de valores de comprobación aleatoria - es decir, una identidad - para estas contraseñas. Sin embargo, el cartucho puede revelar solo cuatro de las contraseñas, tales como las primeras cuatro contraseñas solicitadas desde el cartucho. Por lo tanto, un cartucho según las técnicas descritas en la presente memoria, tal como el cartucho de la FIG. 2, se puede programar interrogando múltiples de tales cartuchos de la solicitud de patente PCT referenciada, para obtener sus conjuntos de valores de comprobación aleatoria tales como las identidades de cartuchos únicas, y las cuatro contraseñas que cada cartucho revelará como las cuatro contraseñas que se almacenan con el conjunto de comprobaciones aleatorias proporcionado por ese cartucho.

Por ejemplo, un primer cartucho de la solicitud de patente PCT referenciada puede corresponder a la identidad 1 de cartucho. La identidad 1 de cartucho puede ser o incluir los valores de comprobación aleatoria para todas las contraseñas 1 hasta 16 de este cartucho, como se recuperan desde el cartucho. Sin embargo, el cartucho puede emitir solo las contraseñas 4, 5, 6 y 7 (es decir, como las cuatro primeras contraseñas solicitadas desde el cartucho). Por lo tanto, las contraseñas 4, 5, 6 y 7 se recuperan y almacenan como correspondientes a la identidad 1. Un segundo cartucho de la solicitud de patente PCT referenciada puede corresponder a la identidad 2 de cartucho, que puede ser o incluir los valores de comprobación aleatoria para todas las contraseñas 1 hasta 16 de este cartucho, como se recuperan desde el cartucho. Sin embargo, el cartucho puede emitir solo las contraseñas 2, 8, 10 y 14 (es decir, como las primeras cuatro contraseñas solicitadas desde el cartucho). Por lo tanto, las contraseñas 2, 8, 10 y 14 se recuperan y almacenan como correspondientes a la identidad 2. Este proceso se puede repetir entonces para los cartuchos tercero, cuarto, quinto y, en última instancia, hasta el de orden m de la solicitud de patente PCT referenciada.

La FIG. 3 muestra un método 300 de ejemplo que puede realizar un elemento reemplazable para un dispositivo, tal como el cartucho 100 de sustancia de impresión para un dispositivo de impresión. El método 300 se puede implementar como un código legible por ordenador almacenado en un medio de almacenamiento de datos legible por ordenador no transitorio y que ejecuta un procesador. Como tal, la lógica 104 del cartucho 100 puede realizar el método 300, por ejemplo. El elemento reemplazable realiza el método 300 tras la instalación o conexión a un dispositivo anfitrión y en el encendido del elemento reemplazable.

El método 300 se refiere a un escenario en el que el elemento reemplazable recibe una solicitud de una identidad antes de recibir una solicitud de un valor de autenticación desde el dispositivo anfitrión. Por lo tanto, el elemento reemplazable tiene que seleccionar y asumir una identidad para su uso con el dispositivo anfitrión antes de que el elemento sea capaz de aprender los valores de autenticación que el dispositivo estará solicitando. De este modo, el elemento reemplazable recibe una solicitud de su identidad desde el dispositivo (302) anfitrión y selecciona una identidad a asumir a partir de las identidades de elementos reemplazables que almacena (304). El elemento reemplazable envía la identidad seleccionada al dispositivo (306) anfitrión. Por ejemplo, el elemento reemplazable puede enviar los valores de comprobación aleatoria que pueden constituir la identidad seleccionada.

El elemento reemplazable recibe una solicitud de un valor de autenticación desde el dispositivo (308) anfitrión. El elemento reemplazable almacena información que indica qué valor de autenticación solicitó el dispositivo (310) anfitrión. Por ejemplo, si el dispositivo anfitrión solicita el valor de autenticación número n, el elemento reemplazable almacena que el dispositivo anfitrión ha solicitado el valor de autenticación número n. El elemento reemplazable

puede almacenar la dirección del dispositivo anfitrión que puede ser determinable a partir de la solicitud recibida en la parte 302 o la parte 308 como parte de esta información. Por ejemplo, el elemento reemplazable puede almacenar la dirección del controlador de acceso al medio (MAC) del dispositivo anfitrión.

Si el elemento reemplazable no tiene el valor de autenticación solicitado almacenado para la identidad (312) seleccionada, entonces el elemento almacena información que indica que la autenticación de la identidad seleccionada ha sido sin éxito para o con el dispositivo (314) anfitrión, que puede incluir almacenar la dirección del dispositivo anfitrión. El elemento reemplazable no puede enviar ninguna respuesta al dispositivo anfitrión. De este modo, el elemento reemplazable tiene que esperar a ser encendido de nuevo de modo que se pueda hacer otro intento de autenticación, tal como realizando el método 300 de nuevo.

Sin embargo, si el elemento reemplazable tiene el valor de autenticación solicitado almacenado para la identidad (312) seleccionada, entonces el elemento envía el valor de autenticación solicitado al dispositivo (316) anfitrión. El método 300 entonces procede de una de dos formas. En primer lugar, el elemento reemplazable puede recibir otra solicitud de valor de autenticación desde el dispositivo anfitrión (es decir, para un valor de autenticación diferente), en cuyo caso el método pasa desde la parte 316 de vuelta a la parte 308.

En segundo lugar, el elemento reemplazable puede determinar que la identidad seleccionada que ha asumido el elemento dio como resultado implícita o explícitamente la autenticación con éxito del elemento dentro del dispositivo anfitrión. En este caso, el elemento reemplazable almacena información que indica que la autenticación de la identidad seleccionada fue con éxito para el dispositivo (318) anfitrión, que puede incluir el almacenamiento de la dirección del dispositivo anfitrión. Por ejemplo, si el elemento reemplazable es un cartucho de impresión y el dispositivo anfitrión es un dispositivo de impresión, si el dispositivo de impresión comienza a usar el cartucho de impresión para formar imágenes en medios, entonces el elemento puede concluir que ha ocurrido una autenticación con éxito implícita. Como otro ejemplo, el dispositivo anfitrión puede indicar explícitamente al elemento reemplazable que el elemento se ha autenticado con éxito.

La FIG. 4 muestra un método 400 de ejemplo que puede realizar un elemento reemplazable para un dispositivo para seleccionar una identidad a asumir dentro del dispositivo en el encendido del método 300. Por ejemplo, un elemento reemplazable puede realizar el método 400 para implementar la parte 304 del método 300, después de que el elemento haya recibido una solicitud de una identidad desde el dispositivo anfitrión en la parte 302 y antes de que el elemento haya recibido una solicitud de un valor de autenticación en la parte 306. El elemento reemplazable determina si se ha conectado previamente al dispositivo (402) anfitrión.

Por ejemplo, cuando el elemento reemplazable almacena los valores de autenticación solicitados desde el dispositivo anfitrión en la parte 310, y cuando el elemento almacena si se autenticó sin éxito o con éxito en la parte 314 o 318, respectivamente, el elemento reemplazable almacena la dirección u otra información de identificación del dispositivo anfitrión recibida en la parte 302 o 308 del método 300. Por lo tanto, el elemento reemplazable puede comparar la dirección, por ejemplo, del dispositivo anfitrión desde el cual el elemento acaba de recibir la solicitud en la parte 302, y compararla con las direcciones del dispositivo anfitrión que almacenó cuando se realizaron previamente las partes 310, 314 y/o 318. Si la dirección del dispositivo anfitrión desde el cual el elemento reemplazable acaba de recibir la solicitud en la parte 302 coincide con cualquiera de las almacenadas previamente, entonces el elemento reemplazable se ha conectado previamente al dispositivo anfitrión. Si la dirección no coincide con ninguna dirección del dispositivo anfitrión almacenada previamente, entonces el elemento reemplazable no se ha conectado previamente al dispositivo anfitrión en cuestión.

Si el elemento reemplazable no se ha conectado previamente al dispositivo (404) anfitrión, entonces en una implementación el elemento reemplazable selecciona aleatoriamente una identidad de elemento reemplazable a partir de las identidades de elementos reemplazables que almacena (406). En otras implementaciones, el elemento reemplazable puede seleccionar una identidad de elemento reemplazable en la parte 406 de una manera diferente. Por ejemplo, si las identidades de elementos reemplazables se almacenan de una manera ordenada, el elemento reemplazable puede seleccionar la primera identidad en el orden en que se almacenan. Como otro ejemplo, la identidad de elemento reemplazable puede seleccionar una identidad que aún no ha enviado a ningún dispositivo anfitrión, seleccionando aleatoriamente una identidad a partir de las identidades no seleccionadas previamente, o seleccionando la primera identidad que aún no ha sido seleccionada en el orden en que se almacenan las identidades.

Como tercer ejemplo, si durante el encendido inmediatamente anterior del elemento reemplazable el elemento se autenticó con éxito por el dispositivo anfitrión al cual se conectó en ese momento, entonces el elemento reemplazable puede seleccionar la identidad de elemento reemplazable que había seleccionado durante esta autenticación con éxito. Por ejemplo, el elemento reemplazable puede haber sido conectado a un primer dispositivo anfitrión y, en el momento de la desconexión del primer dispositivo anfitrión el elemento se autenticó con éxito con el primer dispositivo anfitrión usando una identidad dada. El elemento reemplazable se conecta entonces a un segundo dispositivo anfitrión, al que nunca se ha conectado antes, y se realiza la parte 406 para seleccionar una identidad a asumir con el segundo dispositivo anfitrión. En esta implementación, el elemento reemplazable puede seleccionar de nuevo la identidad dada que asumió con éxito con el primer dispositivo anfitrión, a asumir con el segundo dispositivo anfitrión.

Si el elemento reemplazable ha sido conectado previamente al dispositivo (404) anfitrión, entonces el elemento reemplazable puede determinar si el elemento reemplazable se autentificó con éxito previamente con este dispositivo (408) anfitrión. Si el elemento reemplazable se autenticó con éxito previamente con el dispositivo (410) anfitrión, entonces el elemento puede seleccionar la identidad de elemento reemplazable que asumió durante esta autenticación (412) anterior. En una implementación, la parte 408 comprueba solo si el elemento reemplazable se autenticó con éxito previamente con el dispositivo anfitrión durante el encendido inmediatamente anterior cuando se conectó al dispositivo. Es decir, en esta implementación, la parte 408 comprueba si la última vez que el elemento reemplazable se conectó al dispositivo anfitrión y se encendió, se autenticó con éxito el elemento reemplazable.

Tal implementación puede asegurar que el elemento reemplazable no seleccione repetidamente una identidad de elemento reemplazable que en el pasado dio como resultado que el elemento se autenticase con éxito con el dispositivo anfitrión, pero más recientemente no lo hizo. Esta implementación significa que el elemento reemplazable seleccionará la misma identidad a asumir con un dispositivo anfitrión si el momento inmediatamente anterior en que el elemento se conectó al dispositivo anfitrión y se encendió el elemento reemplazable se autenticó con éxito. Sin embargo, si el elemento reemplazable no se autentica con éxito después de seleccionar esta misma identidad, entonces el elemento no seleccionará automáticamente la identidad la próxima vez que el elemento se conecte al dispositivo anfitrión y se encienda.

Si el elemento reemplazable se autenticó sin éxito previamente con el dispositivo (410) anfitrión - o bien solo durante el último intento de autenticación o bien que nunca se ha autenticado con éxito, dependiendo de cómo se implementa la parte 408 como se ha señalado anteriormente - entonces el elemento puede seleccionar una identidad de elemento reemplazable que el elemento reemplazable no ha enviado previamente al dispositivo (414) anfitrión. Como tal, en esta implementación, el elemento reemplazable puede seleccionar aleatoriamente o de una manera ordenada una identidad a partir de las identidades de elementos reemplazables que el elemento no ha asumido antes con el dispositivo anfitrión. En una segunda implementación, el elemento reemplazable puede seleccionar aleatoriamente o de una manera ordenada una identidad a partir de las identidades de elementos reemplazables que almacena, independientemente de si la identidad se autenticó sin éxito previamente con el dispositivo anfitrión.

Sin embargo, se puede emplear una tercera implementación de la parte 414 cuando se asume que es probable que el dispositivo anfitrión solicite los mismos valores de autenticación del elemento reemplazable como lo hizo durante las solicitudes de autenticación anteriores. En esta implementación, el elemento reemplazable puede seleccionar aleatoriamente o de una manera ordenada una identidad a partir de las identidades de elementos reemplazables para las que almacena los valores de autenticación que el dispositivo anfitrión solicitó previamente. Consideremos el siguiente ejemplo en relación con la FIG. 2. En el primer encendido del elemento reemplazable, el elemento puede seleccionar la identidad 3, y el dispositivo anfitrión puede solicitar el valor 5 de autenticación. El elemento reemplazable tiene este valor de autenticación solicitado para la identidad 3 y, por lo tanto, es capaz de devolver el valor de autentificación solicitado. El dispositivo anfitrión puede solicitar entonces el valor 4 de autenticación. El elemento reemplazable no tiene un valor 4 de autenticación y, por lo tanto, la autenticación falla.

En el segundo encendido del elemento reemplazable, el elemento puede seleccionar la identidad 1, debido a que asume que el dispositivo anfitrión solicitará los valores 4 y 5 de autenticación como lo hizo durante el último encendido. Si el dispositivo anfitrión solicita los valores 4 y 5 de autenticación (en cualquier orden), entonces el elemento reemplazable es capaz de devolver ambos valores de autenticación. El dispositivo anfitrión puede solicitar entonces un valor 9 de autenticación. El elemento reemplazable no almacena el valor 9 de autenticación para la identidad 1 y, por lo tanto, la autenticación falla de nuevo.

Sin embargo, en el tercer encendido, el elemento reemplazable selecciona la identidad 4, debido a que asume que el dispositivo anfitrión solicitará los valores 4, 5 y 9 de autenticación (en cualquier orden), como lo hizo en el segundo encendido. Si el dispositivo anfitrión solicita los valores 4, 5 y 9 de autenticación durante el tercer encendido, entonces el elemento reemplazable es capaz de devolver todos de los tres valores de autenticación. El dispositivo anfitrión puede solicitar entonces el valor 16 de autenticación. El elemento reemplazable almacena el valor 16 de autenticación para la identidad 4 y, de este modo, también puede devolver este valor de autenticación. Si el dispositivo anfitrión no solicita ningún valor de autenticación adicional, la autenticación ha tenido éxito.

El elemento reemplazable puede seleccionar una identidad de elemento reemplazable en la parte 414 en una cuarta implementación que combina dos o más de las tres implementaciones que se han descrito para la parte 414. Como ejemplo, el elemento reemplazable puede seleccionar primero una identidad de elemento reemplazable a partir de las identidades para las que el elemento almacena los valores de autenticación que el dispositivo anfitrión ha solicitado previamente. Después de un número predeterminado de intentos de autenticación sin éxito en una fila, o después de concluir a través de una técnica estadística, de aprendizaje por máquina u otra técnica que el dispositivo anfitrión probablemente no está seleccionando los mismos valores de autenticación, el elemento reemplazable puede seleccionar entonces una identidad de elemento reemplazable a partir de las identidades que el elemento no ha seleccionado previamente con el dispositivo anfitrión. Después de otro número predeterminado de intentos de autenticación sin éxito en una fila, el elemento reemplazable puede seleccionar entonces una identidad de todas las identidades que almacena, sin considerar si el elemento ha asumido previamente la identidad con el dispositivo anfitrión.

Tal implementación de combinación puede ser útil debido a que el elemento reemplazable puede no tener conocimiento anterior en cuanto al número de valores de autenticación que un dispositivo anfitrión puede solicitar, si el dispositivo anfitrión solicitase los mismos valores de autenticación y/o el orden en el que se solicitan los valores de autenticación, en su caso. Por ejemplo, un dispositivo anfitrión puede solicitar tres valores de autenticación, y otro dispositivo anfitrión puede solicitar cuatro. Un tercer dispositivo anfitrión puede solicitar entre dos y cuatro valores de autenticación. Un dispositivo anfitrión puede solicitar los valores de autenticación números a, b, c, d o puede que no. Un dispositivo anfitrión puede solicitar los valores de autenticación números a, b, c, d en un orden aleatorio, o puede solicitar siempre a seguido por b, seguido por c, seguido por d. La implementación de combinación, por lo tanto, permite que el elemento reemplazable cambie las estrategias cuando la estrategia actual parece poco probable que tenga éxito.

La FIG. 5 muestra otro método 500 de ejemplo que puede realizar un elemento reemplazable para un dispositivo, tal como el cartucho 100 de sustancia de impresión para un dispositivo de impresión. Como el método 300 de la FIG. 3, el método 500 se puede implementar como un código legible por ordenador almacenado en un medio de almacenamiento de datos legible por ordenador no transitorio y que ejecuta un procesador. Como tal, la lógica 104 del cartucho 100 puede realizar el método 500, por ejemplo. El elemento reemplazable realiza el método 500 tras la instalación o conexión a un dispositivo anfitrión y en el encendido del elemento reemplazable.

El método 500 se refiere a un escenario en el que el elemento reemplazable recibe una solicitud de una identidad después de recibir una solicitud de un valor de autenticación desde el dispositivo anfitrión. Por lo tanto, el elemento reemplazable no tiene que seleccionar y asumir una identidad para su uso con el dispositivo anfitrión antes de que el elemento aprenda el primer valor de autenticación que está solicitando el dispositivo. El elemento reemplazable recibe de este modo una solicitud de un valor de autenticación desde el dispositivo (502) anfitrión. La primera vez que parte 502 se realiza durante el método 500, se realiza antes de que el elemento reemplazable haya seleccionado una identidad. Como tal, si el elemento reemplazable aún no ha asumido una identidad (504), entonces el elemento reemplazable selecciona una identidad a asumir a partir de las identidades de elementos reemplazables que almacena (506). El elemento reemplazable selecciona una de las identidades de elementos reemplazables para las que almacena el valor de autenticación solicitado. La parte 506 se realiza de este modo solo una vez cada vez que se realiza el método 500.

Si el elemento reemplazable ya ha asumido una identidad (504), o después de que el elemento haya seleccionado una identidad a asumir (506), el elemento reemplazable almacena información que indica qué valor de autentificación solicitó el dispositivo anfitrión (508). Como se ha descrito anteriormente en relación con la parte 308, si el dispositivo anfitrión solicita el valor de autenticación número n, el elemento reemplazable almacena que el dispositivo anfitrión ha solicitado el valor de autenticación número n. El dispositivo anfitrión puede almacenar la dirección del dispositivo anfitrión que se puede determinar a partir de la solicitud recibida en la parte 502.

El elemento reemplazable tendrá el primer valor de autenticación solicitado para la identidad seleccionada, debido a que el elemento selecciona una identidad para la que verdaderamente almacena el valor de autenticación solicitado la primera vez que se realiza la parte 502. Sin embargo, el elemento reemplazable puede no tener un valor de autenticación solicitado posteriormente para la identidad seleccionada. Si el elemento reemplazable no tiene el valor de autenticación solicitado almacenado para la identidad (510) seleccionada, el elemento almacena información que indica que la autenticación de la identidad seleccionada ha sido sin éxito para o con el dispositivo (512) anfitrión, que puede incluir el almacenamiento de la dirección del dispositivo anfitrión. Como se ha descrito anteriormente en relación con la parte 314 del método 300, el elemento reemplazable puede no enviar ninguna respuesta al dispositivo anfitrión y, además, el elemento ha de esperar a que se encienda de nuevo de modo que se pueda hacer otro intento de autenticación, tal como realizando el método 500 de nuevo.

Sin embargo, si el elemento reemplazable tiene el valor de autenticación solicitado almacenado para la identidad (510) seleccionada, entonces el elemento envía el valor de autenticación solicitado al dispositivo (514) anfitrión. El método 500 puede proceder entonces de una de dos formas. El elemento reemplazable puede recibir otra solicitud de valor de autenticación desde el dispositivo anfitrión (es decir, para un valor de autenticación diferente), en cuyo caso el método 500 procede desde la parte 514 de vuelta a la parte 502.

Sin embargo, en algún punto, el elemento reemplazable recibirá una solicitud de su identidad desde el dispositivo (516) anfitrión, y en respuesta el elemento envía la identidad seleccionada en la parte 506 al dispositivo (518) anfitrión, tal como los valores de comprobación aleatoria de los valores de autenticación para la identidad seleccionada que pueden constituir la identidad seleccionada. Las partes 516 y 518 se representan como que se realizan después de la parte 514 por conveniencia ilustrativa. De manera más general, la parte 516 se realiza en el método 500 en cualquier momento después de que se haya realizado la parte 502 la primera vez, y la parte 518 se realiza en el método 500 en cualquier momento después de que se haya realizado la parte 506.

El elemento reemplazable puede determinar de este modo que la identidad seleccionada que ha asumido dio como resultado implícita o explícitamente una autenticación con éxito del elemento dentro del dispositivo anfitrión. En este caso, el elemento reemplazable almacena información que indica que la autenticación de la identidad seleccionada fue con éxito para el dispositivo (520) anfitrión, que puede incluir el almacenamiento de la dirección del dispositivo anfitrión. Si el elemento reemplazable es un cartucho de impresión y el dispositivo anfitrión es un dispositivo de

impresión, por ejemplo, si el dispositivo de impresión comienza usando el cartucho para formar imágenes en medios, entonces el elemento puede concluir que ha ocurrido una autenticación con éxito implícita. Como otro ejemplo, el dispositivo anfitrión puede indicar explícitamente al elemento reemplazable que el elemento se ha autenticado con éxito. La parte 520 se realiza después de que se hayan realizado las partes 516 y 518 si el dispositivo anfitrión autentica la identidad seleccionada que el elemento reemplazable envió en la parte 518 en respuesta a la solicitud del dispositivo de que el elemento se recibió en la parte 516.

La FIG. 6 muestra un método 600 de ejemplo que puede realizar un elemento reemplazable para un dispositivo para seleccionar una identidad a asumir dentro del dispositivo en el encendido en el método 500. Por ejemplo, un elemento reemplazable puede realizar el método 600 para implementar la parte 506 del método 500, después de que el elemento haya recibido una solicitud de un valor de autenticación desde el dispositivo anfitrión en la parte 502 y antes de que el elemento haya recibido una solicitud de su identidad en la parte 516. El elemento reemplazable determina si se ha conectado previamente al dispositivo (602) anfitrión, como se ha descrito en relación con la parte 402 del método 400.

Si el elemento reemplazable no se ha conectado previamente al dispositivo (604) anfitrión, entonces, en una implementación, el elemento de recambio selecciona aleatoriamente una identidad de elemento reemplazable de las identidades de elementos reemplazables que almacena (606), como se ha descrito en relación con la parte 406 del método 400, pero con la condición añadida de que el elemento reemplazable selecciona una identidad para la que almacena el valor de autenticación solicitado. Además, en otras implementaciones, el elemento reemplazable puede seleccionar una identidad de elemento reemplazable en la parte 606 de una manera diferente. El elemento reemplazable puede seleccionar una identidad de elemento reemplazable en la parte 606 de otra manera, como se ha descrito en relación con la parte 406 del método 400, pero también con la condición añadida de que el elemento reemplazable selecciona una identidad para la cual almacena el valor de autenticación requerido.

Esta condición añadida representa el conocimiento que tiene el elemento reemplazable en la realización del método 500 (y, de este modo, del método 600) que no tiene en la realización del método 300 (y, de este modo, del método 400). Cuando el elemento reemplazable realiza el método 600, el elemento ya ha recibido una solicitud de un valor de autenticación desde el dispositivo anfitrión por la parte 502 del método 500. En comparación, cuando el elemento reemplazable realiza el método 400, el elemento aún no ha recibido una solicitud de un valor de autenticación desde el dispositivo anfitrión. Por lo tanto, en la parte 606, aún cuando el elemento reemplazable no se ha conectado previamente al dispositivo anfitrión, el elemento aún conoce ya el primer valor de autenticación que está solicitando el dispositivo anfitrión y, como tal, selecciona una identidad para la cual el elemento almacena el valor de autenticación solicitado.

Si el elemento reemplazable se ha conectado previamente al dispositivo (604) anfitrión, entonces el elemento determina si se autenticó con éxito previamente con el dispositivo (608) anfitrión. Como es el caso con la parte 408 del método 400, la parte 608 puede probar solo si el elemento reemplazable se autenticó con éxito previamente con el dispositivo anfitrión durante el encendido inmediatamente anterior cuando se conectó al dispositivo. Es decir, en una implementación, la parte 608 comprueba si la última vez que el elemento reemplazable se conectó al dispositivo anfitrión y se encendió, el elemento reemplazable se autenticó con éxito.

Si el elemento reemplazable se autenticó con éxito previamente con el dispositivo (610) anfitrión y si el elemento reemplazable almacena el valor de autenticación solicitado para una identidad de elemento reemplazable que el dispositivo anfitrión autenticó (612), entonces el elemento reemplazable selecciona de nuevo tal identidad (614). Como se ha señalado anteriormente, en la realización del método 600, el elemento reemplazable ya tiene conocimiento del primer valor de autenticación que está solicitando el dispositivo anfitrión. Por lo tanto, incluso si el elemento reemplazable se autenticó con éxito previamente con el dispositivo anfitrión, si el elemento se autenticó con éxito usando una identidad dada para la cual el elemento no almacena el valor de autenticación solicitado, entonces la identidad dada no dará como resultado de nuevo la autenticación del elemento. Como mínimo, en otras palabras, el elemento reemplazable en el método 600 selecciona una identidad para la cual el elemento almacena el valor de autenticación solicitado.

Se señala que cuando el elemento reemplazable selecciona una identidad en la parte 614, puede haber múltiples identidades con las cuales el elemento se autenticó con éxito previamente con el dispositivo anfitrión. En este caso, el elemento reemplazable puede seleccionarse aleatoriamente a partir de una de estas identidades. En otra implementación, el elemento reemplazable puede seleccionar la identidad con la que el elemento se autenticó con éxito más recientemente con el dispositivo anfitrión.

Si el elemento reemplazable no se autenticó con éxito previamente con el dispositivo (610) anfitrión, o si el elemento reemplazable se autentificó con éxito previamente (610) pero el elemento no almacena el elemento de autenticación solicitado para una identidad que el dispositivo anfitrión autenticado (612), entonces el elemento reemplazable puede seleccionar una identidad de elemento reemplazable que el elemento no ha enviado previamente al dispositivo (616) anfitrión. Tal identidad es también una para la cual el elemento reemplazable almacena el valor de autenticación solicitado del cual tiene conocimiento el elemento. En esta implementación, el elemento reemplazable puede seleccionar aleatoriamente o de una manera ordenada una identidad a partir de las identidades de elementos reemplazables que el elemento no ha asumido antes con el dispositivo anfitrión y que almacena el valor de

autenticación solicitado. En una segunda implementación, el elemento reemplazable puede seleccionar aleatoriamente o de una manera ordenada una identidad a partir de las identidades de elementos reemplazables para las cuales el elemento almacena el valor de autenticación solicitado, independientemente de si la identidad se autentificó sin éxito previamente con el dispositivo anfitrión.

Una tercera implementación de la parte 616, sin embargo, se puede emplear cuando se asume que es probable que el dispositivo anfitrión solicite los mismos valores de autenticación del elemento reemplazable como lo hizo durante las solicitudes de autenticación anterior. En esta implementación, el elemento reemplazable puede seleccionar aleatoriamente o de una manera ordenada una identidad a partir de las identidades de elementos reemplazables para la cual almacena los valores de autenticación que el dispositivo anfitrión solicitó previamente, así como el valor de autenticación que está solicitando actualmente el dispositivo. Esta tercera implementación corresponde a la tercera implementación de la parte 414 del método 400 descrito anteriormente, con la condición añadida de que el elemento reemplazable también almacena para la identidad seleccionada el valor de autenticación que está solicitando actualmente el dispositivo. Como en la parte 414, se puede usar además una implementación adicional que combine dos o más de las tres implementaciones que se han descrito.

Los métodos 400 y 600 que se han descrito proporcionan de este modo diversas formas mediante las cuales un elemento reemplazable para un dispositivo anfitrión puede seleccionar una identidad a ofrecer al dispositivo para la autenticación del elemento con el dispositivo. La diferencia entre los métodos 400 y 600 es el conocimiento que tiene el elemento reemplazable cuando se selecciona una identidad a asumir con el dispositivo anfitrión. En el método 400, el elemento reemplazable aún no ha recibido una solicitud de un valor de autenticación desde el dispositivo anfitrión, mientras que en el método 600, el elemento ya ha recibido una primera solicitud de un valor de autenticación. Por lo tanto, siendo iguales todas las otras cosas, el elemento reemplazable es más probable que seleccione una identidad que dará como resultado una autentificación con éxito en el método 600 que en el método 400.

La FIG. 7 muestra otro método 700 de ejemplo que puede realizar un elemento reemplazable para un dispositivo anfitrión, tal como el cartucho 100 de sustancia de impresión para un dispositivo de impresión, para seleccionar una identidad a asumir con propósitos de autenticación con el dispositivo. El método 700 es un caso particular de cada uno de los métodos 400 y 600. Como los otros métodos que se han descrito, el método 700 se puede implementar como un código legible por ordenador almacenado en un medio de almacenamiento de datos legible por ordenador no transitorio y que ejecuta un procesador. Por lo tanto, la lógica 104 del cartucho 100 puede realizar el método 700.

El método 700 asume el siguiente escenario. Un elemento reemplazable se conecta a un primer dispositivo anfitrión y se enciende. El elemento puede o no haber sido autenticado con éxito usando la identidad de elemento reemplazable que asumió en este encendido. El elemento reemplazable se enciende una segunda vez. En el segundo encendido, el elemento aún puede estar conectado al primer dispositivo anfitrión, o ahora se puede conectar a un segundo dispositivo anfitrión diferente del primer dispositivo anfitrión.

El elemento reemplazable determina si se autenticó con éxito en el (primer) encendido antes del (segundo) encendido actual (702). Si el elemento reemplazable se autenticó con éxito en el encendido anterior (704), entonces el elemento selecciona de nuevo o asume la identidad de elemento reemplazable que usó en el encendido anterior (706). El elemento reemplazable selecciona esta identidad independientemente de si está instalado en un (segundo) dispositivo anfitrión diferente o en el mismo (primer) dispositivo anfitrión en el encendido actual en comparación con el encendido anterior. En el caso en que el elemento reemplazable ya haya recibido una solicitud de un valor de autenticación desde el dispositivo anfitrión - como en los métodos 500 y 600 de las FIG. 5 y 6 - sin embargo, el elemento selecciona la identidad autenticada con éxito previamente solo si el elemento también almacena el valor de autenticación solicitado para esta identidad.

Sin embargo, si el elemento reemplazable no se autenticó con éxito en el encendido anterior (704), entonces el elemento selecciona o asume una identidad de elemento reemplazable diferente de la que usó en el encendido anterior (708). Cómo se selecciona esta identidad de elemento reemplazable diferente se puede determinar como se ha descrito anteriormente en relación con los métodos 400 y 600. Por lo tanto, el método 700 anterior prioriza el uso de la identidad de elemento reemplazable seleccionada más recientemente, si esa identidad se autenticó con éxito.

Las técnicas descritas en la presente memoria proporcionan un elemento reemplazable para un dispositivo anfitrión, tal como un cartucho de sustancia de impresión para un dispositivo de impresión, que también puede pasar la autenticación dentro del dispositivo. Tal elemento reemplazable, en otras palabras, puede emplear dentro de un dispositivo anfitrión que solicita valores de autenticación del elemento y autentica el elemento en base a los valores que devuelve el elemento. En lugar de almacenar un conjunto completo de valores de autenticación, el elemento reemplazable puede almacenar múltiples conjuntos parciales de valores de autenticación, donde cada conjunto parcial está unido a una identidad de elemento de recambio diferente. Los diferentes conjuntos parciales se pueden obtener interrogando a otros elementos reemplazables que almacenan cada uno un conjunto completo de valores de autenticación, pero que solo proporcionará cada uno un subconjunto limitado de sus valores.

REIVINDICACIONES

1. Un medio de almacenamiento de datos legible por ordenador no transitorio que almacena un código ejecutable por ordenador ejecutable por un elemento reemplazable para que los dispositivos de impresión realicen un método que comprende:

en respuesta a la recepción de una solicitud de una identidad (110) del elemento reemplazable desde un dispositivo anfitrión al que se ha conectado el elemento reemplazable, seleccionar la identidad de una pluralidad de identidades de elementos reemplazables almacenadas dentro del elemento reemplazable, el elemento reemplazable que almacena una pluralidad de valores de autenticación para cada identidad (110) de elemento reemplazable;

enviar la identidad (110) seleccionada al dispositivo anfitrión;

después de enviar la identidad (110) seleccionada, y en respuesta a recibir una solicitud de un valor de autenticación desde el dispositivo anfitrión, determinar si el elemento reemplazable almacena el valor de autenticación solicitado para la identidad (110) seleccionada; y

en respuesta a la determinación de que el elemento reemplazable almacena el valor de autenticación solicitado para la identidad (110) seleccionada, enviar el valor de autenticación requerido para la identidad (110) seleccionada al dispositivo anfitrión; caracterizado por que: seleccionar la identidad (110) a partir de las identidades (110) de elementos reemplazables almacenadas dentro del elemento reemplazable comprende:

determinar si el elemento reemplazable se autenticó sin éxito previamente con el dispositivo anfitrión; y

en respuesta a la determinación de que el elemento reemplazable se autenticó sin éxito previamente con el dispositivo anfitrión, seleccionar aleatoriamente una de las identidades (110) de elementos reemplazables que el elemento reemplazable no envió cuando el elemento reemplazable se autenticó sin éxito previamente.

2. El medio de almacenamiento de datos legible por ordenador no transitorio de la reivindicación 1, en donde el método comprende además:

después de enviar el valor de autenticación solicitado para la identidad (110) seleccionada al dispositivo anfitrión, y en respuesta a la recepción de una solicitud de un segundo valor de autenticación desde el dispositivo anfitrión, determinar si el elemento reemplazable almacena el segundo valor de autenticación solicitado para la identidad seleccionada; y

en respuesta a la determinación de que el elemento reemplazable almacena el segundo valor de autenticación solicitado para la identidad (110) seleccionada, enviar el segundo valor de autenticación solicitado para la identidad (110) seleccionada al dispositivo anfitrión.

3. El medio de almacenamiento de datos legible por ordenador no transitorio de la reivindicación 1, en donde seleccionar la identidad a partir de las identidades (110) de elementos reemplazables almacenadas dentro del elemento reemplazable comprende:

determinar si el elemento reemplazable se ha conectado previamente al dispositivo anfitrión; y

en respuesta a la determinación de que el elemento reemplazable no se ha conectado previamente al dispositivo anfitrión, seleccionar aleatoriamente la identidad (110) a partir de las identidades (110) de elementos reemplazables almacenadas dentro del elemento reemplazable.

4. El medio de almacenamiento de datos legible por ordenador no transitorio de la reivindicación 1, en donde seleccionar la identidad (110) a partir de las identidades de elementos reemplazables almacenados dentro del elemento reemplazable comprende:

determinar si el elemento reemplazable se autenticó con éxito previamente con el dispositivo anfitrión; y

en respuesta a la determinación de que el elemento reemplazable se autenticó con éxito previamente con el dispositivo anfitrión, seleccionar la identidad (110) que se autenticó con éxito previamente con el dispositivo anfitrión.

5. El medio de almacenamiento de datos legible por ordenador no transitorio de la reivindicación 1, en donde seleccionar la identidad a partir de las identidades de elementos reemplazables almacenadas dentro del elemento reemplazable comprende:

determinar si el elemento reemplazable se autenticó sin éxito previamente con el dispositivo anfitrión; y

en respuesta a la determinación de que el elemento reemplazable fue autentificado sin éxito previamente con

el dispositivo anfitrión, seleccionar una de las identidades (110) de elementos reemplazables para las cuales el elemento reemplazable almacena los valores de autenticación que el dispositivo anfitrión solicitó previamente cuando el elemento reemplazable se autenticó sin éxito previamente.

6. El medio de almacenamiento de datos legible por ordenador no transitorio de la reivindicación 1, que comprende además:

en respuesta a la recepción de la solicitud del valor de autenticación desde el dispositivo anfitrión, almacenar información que indica que el dispositivo anfitrión solicitó el valor de autenticación;

en respuesta a la determinación de que el elemento reemplazable se ha autenticado con éxito con el dispositivo anfitrión, almacenar información que indica que el elemento reemplazable se ha autenticado con éxito con el dispositivo anfitrión; y

en respuesta a la determinación de que el elemento reemplazable se ha autenticado sin éxito con el dispositivo anfitrión, almacenar información que indica que el elemento reemplazable se ha autenticado sin éxito con el dispositivo anfitrión.

7. Un método que comprende:

antes de que un elemento reemplazable para el dispositivo de impresión que recibe una solicitud de una identidad (110) del elemento reemplazable desde un dispositivo anfitrión al que se haya conectado el elemento reemplazable, y en respuesta al elemento reemplazable que recibe una solicitud de un valor de autenticación desde el dispositivo anfitrión, seleccionar, por el elemento reemplazable, la identidad a partir de una pluralidad de identidades (110) de elementos reemplazables almacenadas dentro del elemento reemplazable, el elemento reemplazable que almacena una pluralidad de valores de autenticación para cada identidad (110) de elemento reemplazable, la identidad seleccionada como una de las identidades de elementos reemplazables para las cuales el elemento reemplazable almacena el valor de autenticación solicitado; y

después de seleccionar la identidad (110), enviar, por el elemento reemplazable, el valor de autenticación solicitado para la identidad seleccionada al dispositivo anfitrión; caracterizado por que: seleccionar la identidad (110) a partir de las identidades (110) de elementos reemplazables almacenadas dentro del elemento reemplazable comprende:

determinar si el elemento reemplazable se autenticó sin éxito previamente con el dispositivo anfitrión; y en respuesta a la determinación de que el elemento reemplazable se autenticó sin éxito previamente con el dispositivo anfitrión, seleccionar aleatoriamente una de las identidades (110) de elementos reemplazables para las cuales el elemento reemplazable almacena el valor de autenticación solicitado y que no seleccionó el elemento reemplazable cuando el elemento reemplazable se autenticó sin éxito previamente.

8. El método de la reivindicación 7, que comprende además:

en respuesta a que el elemento reemplazable que recibe una solicitud de la identidad (110) del elemento reemplazable desde el dispositivo anfitrión, enviar, mediante el elemento reemplazable, la identidad (110) seleccionada al dispositivo anfitrión.

9. El método de la reivindicación 7, que comprende además:

antes de que el elemento reemplazable que recibe la solicitud de la identidad (110) del elemento reemplazable desde el dispositivo anfitrión, después de enviar el valor de autenticación solicitado para la identidad (110) seleccionada al dispositivo anfitrión, y en respuesta a recibir una solicitud de un segundo valor de autentificación desde el dispositivo anfitrión, determinar, mediante el elemento reemplazable, si el elemento reemplazable almacena el segundo valor de autenticación solicitado para la identidad (110) seleccionada; y

en respuesta a la determinación de que el elemento reemplazable almacena el segundo valor de autenticación solicitado para la identidad (110) seleccionada, enviar, mediante el elemento reemplazable, el segundo valor de autenticación solicitado para la identidad (110) seleccionada al dispositivo anfitrión.

10. El método de la reivindicación 7, en donde seleccionar la identidad a partir de las identidades de elementos reemplazables almacenadas dentro del elemento reemplazable comprende:

determinar si el elemento reemplazable se ha conectado previamente al dispositivo anfitrión; y

en respuesta a la determinación de que el elemento reemplazable no se ha conectado previamente al dispositivo anfitrión, seleccionar aleatoriamente la identidad (110) a partir de las identidades (110) de elementos reemplazables para las cuales el elemento reemplazable almacena el valor de autenticación requerido.

11. El método de la reivindicación 7, en donde seleccionar la identidad a partir de las identidades de elementos reemplazables almacenadas dentro del elemento reemplazable comprende:

determinar si el elemento reemplazable se autenticó con éxito previamente con el dispositivo anfitrión; y

en respuesta a la determinación de que el elemento reemplazable se autenticó con éxito previamente con el dispositivo anfitrión, seleccionar la identidad que se autenticó con éxito previamente con el dispositivo anfitrión si el elemento reemplazable almacena el valor de autenticación solicitado para la identidad que se autenticó previamente con el dispositivo anfitrión.

12. El método de la reivindicación 7, en donde seleccionar la identidad a partir de las identidades de elementos reemplazables almacenadas dentro del elemento reemplazable comprende:

determinar si el elemento reemplazable se autenticó sin éxito previamente con el dispositivo anfitrión; y

en respuesta a la determinación de que el elemento reemplazable se autenticó sin éxito previamente con el dispositivo anfitrión, seleccionar una de las identidades (110) de elementos reemplazables para las cuales el elemento reemplazable almacena el valor de autenticación solicitado y para las cuales el elemento reemplazable también almacena los valores de autenticación que el dispositivo anfitrión solicitó previamente cuando el elemento reemplazable se autenticó sin éxito previamente.

13. El método de la reivindicación 7, que comprende además:

en respuesta al elemento reemplazable que recibe la solicitud del valor de autenticación desde el dispositivo anfitrión, almacenar información que indica que el dispositivo anfitrión solicitó el valor de autenticación;

en respuesta al elemento reemplazable que determina que el elemento reemplazable se ha autenticado con éxito con el dispositivo anfitrión, almacenar información que indica que el elemento reemplazable se ha autentificado con éxito con el dispositivo anfitrión; y

en respuesta al elemento reemplazable que determina que el elemento reemplazable se ha autenticado sin éxito con el dispositivo anfitrión, almacenar información que indica que el elemento reemplazable se ha autenticado sin éxito con el dispositivo anfitrión.

14. Un cartucho (100) de sustancia de impresión para un dispositivo de impresión, que comprende:

un suministro (102) de sustancia de impresión para el dispositivo de impresión;

una memoria (106) no volátil que almacena una pluralidad de identidades (110) de cartucho, y para cada identidad una pluralidad de contraseñas (108); y

lógica (104) para, en el encendido del cartucho (100), asumir como identidad (110) del cartucho (100) para su uso para autenticación de la identidad (110) del cartucho que la lógica (104) asumió antes del encendido si el cartucho (100) se autenticó con éxito con la identidad (110) de cartucho que la lógica (100) asumió antes del encendido;

en donde la identidad de cartucho que la lógica (104) asumió antes del encendido es una identidad (110) del cartucho anterior, caracterizado por que la lógica (104) es además para, en el encendido, asumir como la identidad del cartucho (100) a usar para autenticación mediante una selección aleatoria una identidad (110) de cartucho diferente de la identidad (110) de cartucho anterior si el cartucho (100) se autentificó sin éxito con la identidad (110) de cartucho anterior.

15. El cartucho de sustancia de impresión de la reivindicación 14, en donde la identidad de cartucho que la lógica (104) asumió antes del encendido es una identidad (110) de cartucho anterior, y en donde la lógica (104) es además para, en el encendido, asumir como la identidad (110) del cartucho (100) a usar para autenticación la identidad (110) de cartucho anterior si el cartucho fue autenticado con éxito con la identidad (110) de cartucho anterior y si el cartucho (100) almacena una contraseña (108) solicitada para la identidad (110) de cartucho anterior.

16. El cartucho de sustancia de impresión de la reivindicación 14, en donde la lógica es además para, en respuesta a una solicitud del dispositivo de impresión de una contraseña (108):

determinar si la memoria (106) no volátil almacena la contraseña (108) solicitada para la identidad (110) asumida; y

si la memoria no volátil almacena la contraseña (108) solicitada para la identidad (110) asumida, enviar la contraseña (108) solicitada para la identidad (110) asumida.

17. El cartucho de sustancia de impresión de la reivindicación 14, en donde la sustancia de impresión es una o más de: tinta, tóner, colorante bidimensional (2D), agente de impresión tridimensional (3D) y material de construcción de impresión 3D.

FIG 1

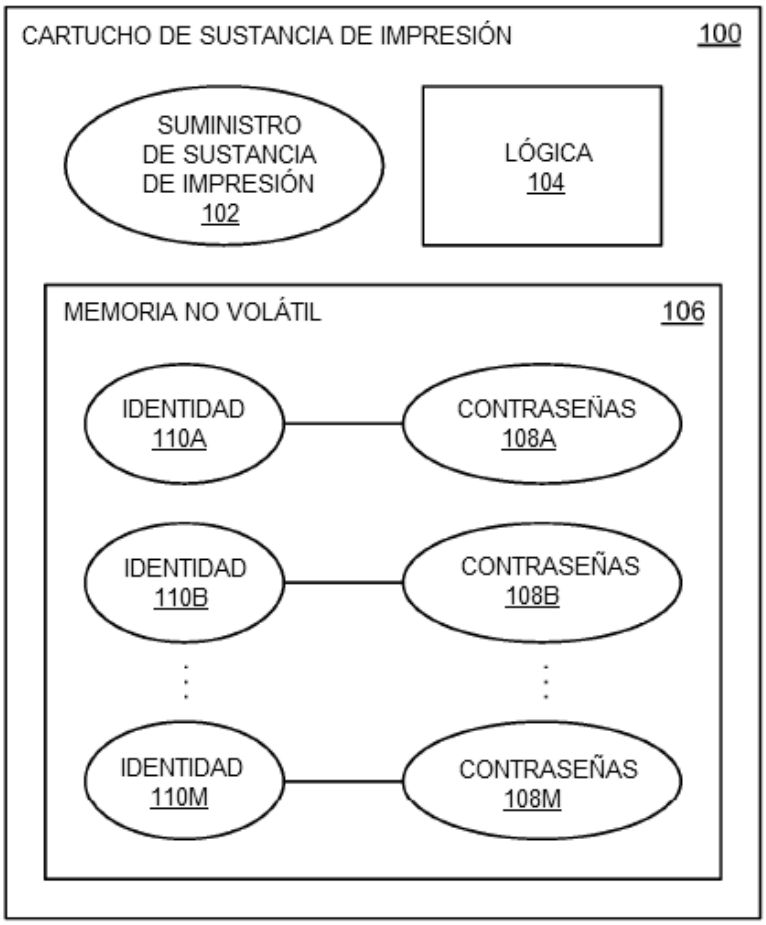
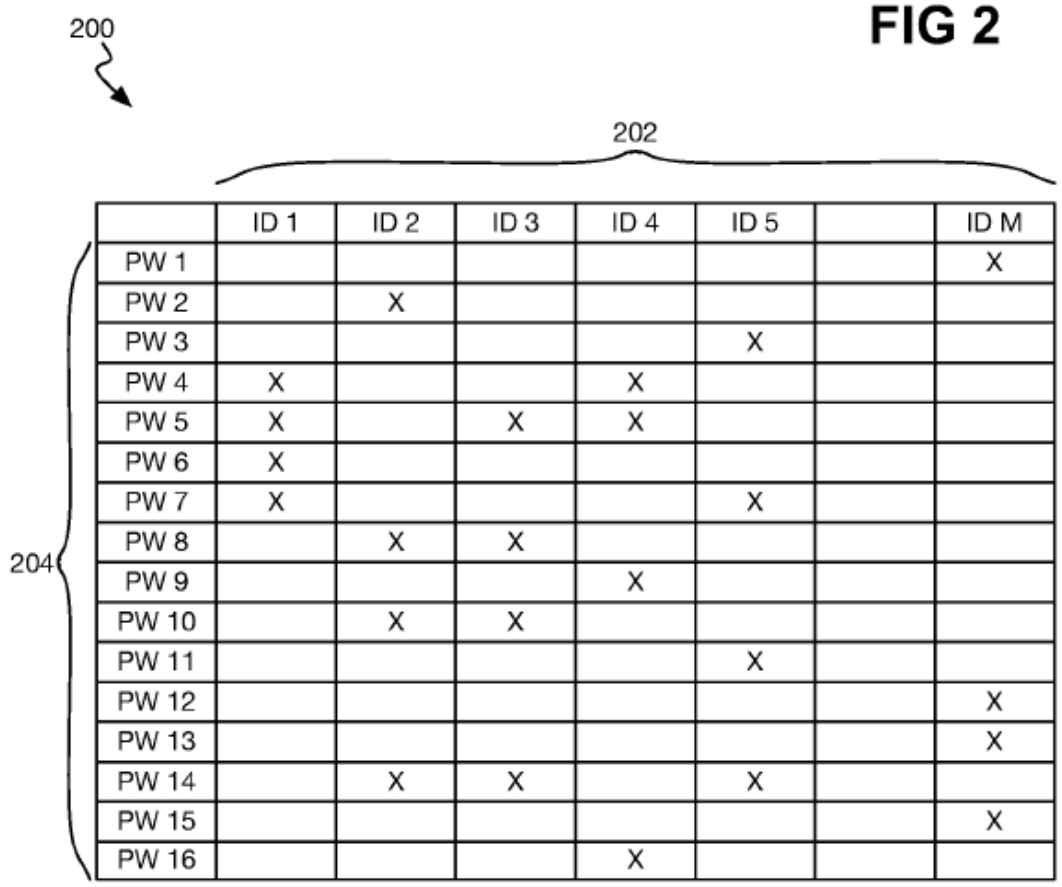

CARTUCHO DE SUSTANCIA DE IMPRESIÓN
100
SUMINISTRO DE SUSTANCIA DE IMPRESIÓN
102
LÓGICA
104
MEMORIA NO VOLÁTIL
106
IDENTIDAD
110A
CONTRASEÑAS
108A
IDENTIDAD
110B
CONTRASEÑAS
108B
IDENTIDAD
110M
CONTRASEÑAS
108M

FIG 2



	ID 1	ID 2	ID 3	ID 4	ID 5		ID M
PW 1							X
PW 2		X					
PW 3					X		
PW 4	X			X			
PW 5	X		X	X			
PW 6	X						
PW 7	X				X		
PW 8		X	X				
PW 9				X			
PW 10		X	X				
PW 11					X		
PW 12							X
PW 13							X
PW 14		X	X		X		
PW 15							X
PW 16				X			

FIG 3

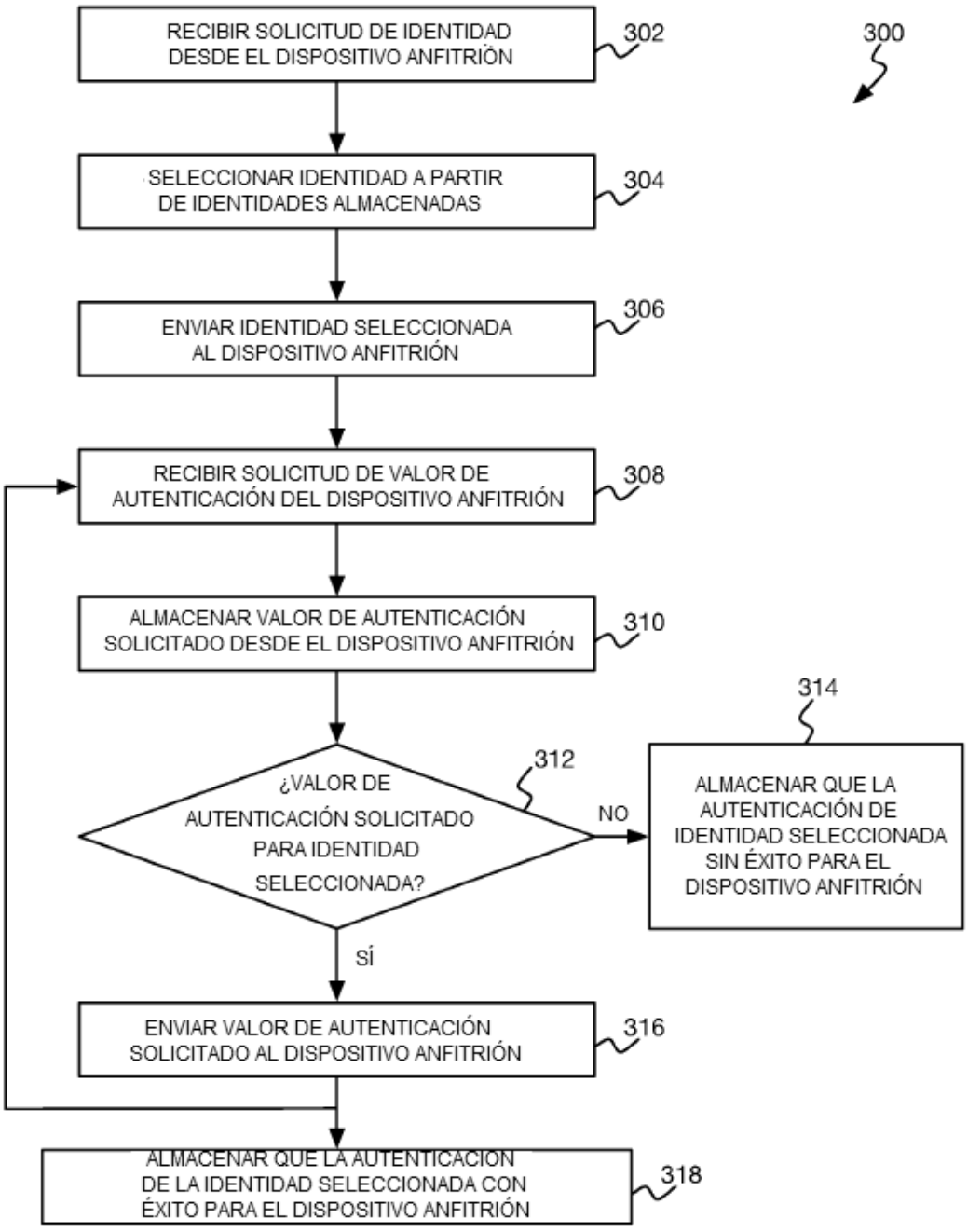

300
RECIBIR SOLICITUD DE IDENTIDAD DESDE EL DISPOSITIVO ANFITRIÓN
302
SELECCIONAR IDENTIDAD A PARTIR DE IDENTIDADES ALMACENADAS
304
ENVIAR IDENTIDAD SELECCIONADA AL DISPOSITIVO ANFITRIÓN
306
RECIBIR SOLICITUD DE VALOR DE AUTENTICACIÓN DEL DISPOSITIVO ANFITRIÓN
308
ALMACENAR VALOR DE AUTENTICACIÓN SOLICITADO DESDE EL DISPOSITIVO ANFITRIÓN
310
¿VALOR DE AUTENTICACIÓN SOLICITADO PARA IDENTIDAD SELECCIONADA?
312
NO
314
ALMACENAR QUE LA AUTENTICACIÓN DE IDENTIDAD SELECCIONADA SIN ÉXITO PARA EL DISPOSITIVO ANFITRIÓN
SÍ
ENVIAR VALOR DE AUTENTICACIÓN SOLICITADO AL DISPOSITIVO ANFITRIÓN
316
ALMACENAR QUE LA AUTENTICACIÓN DE LA IDENTIDAD SELECCIONADA CON ÉXITO PARA EL DISPOSITIVO ANFITRIÓN
318

FIG 4

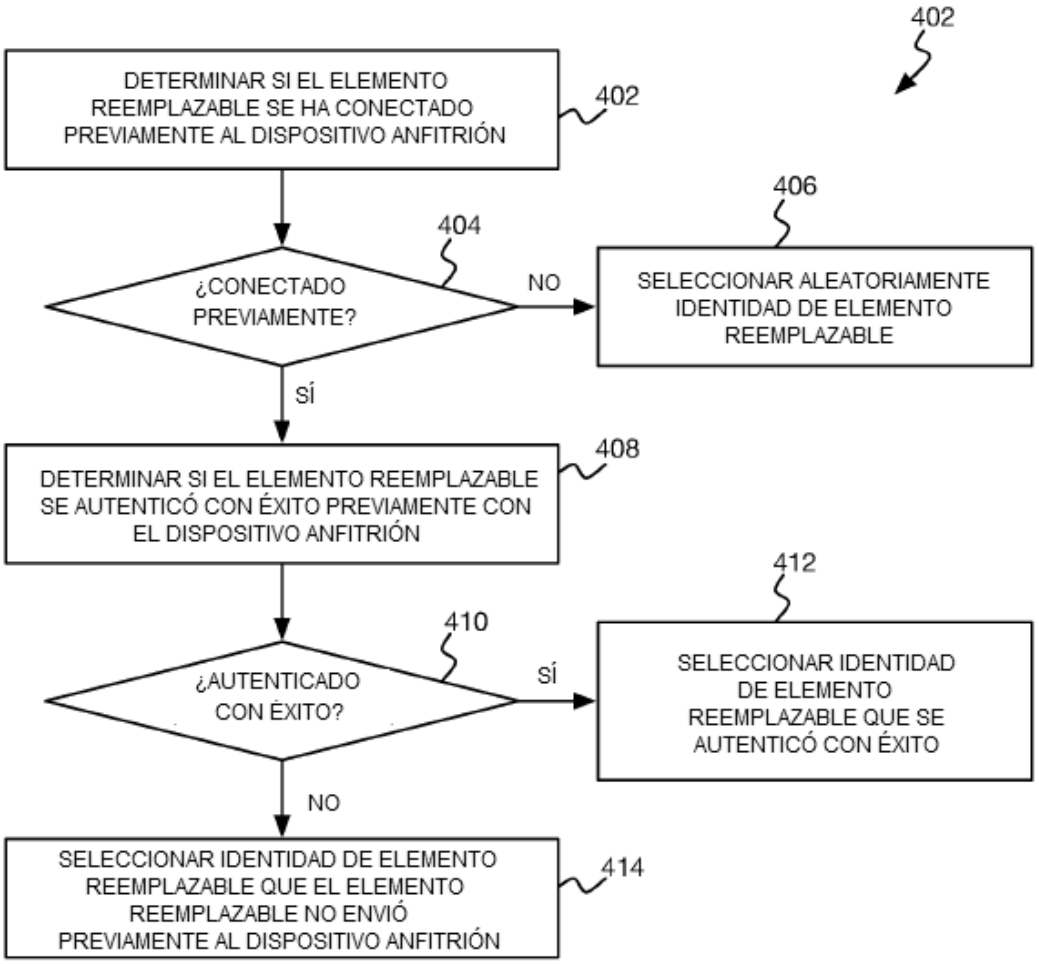
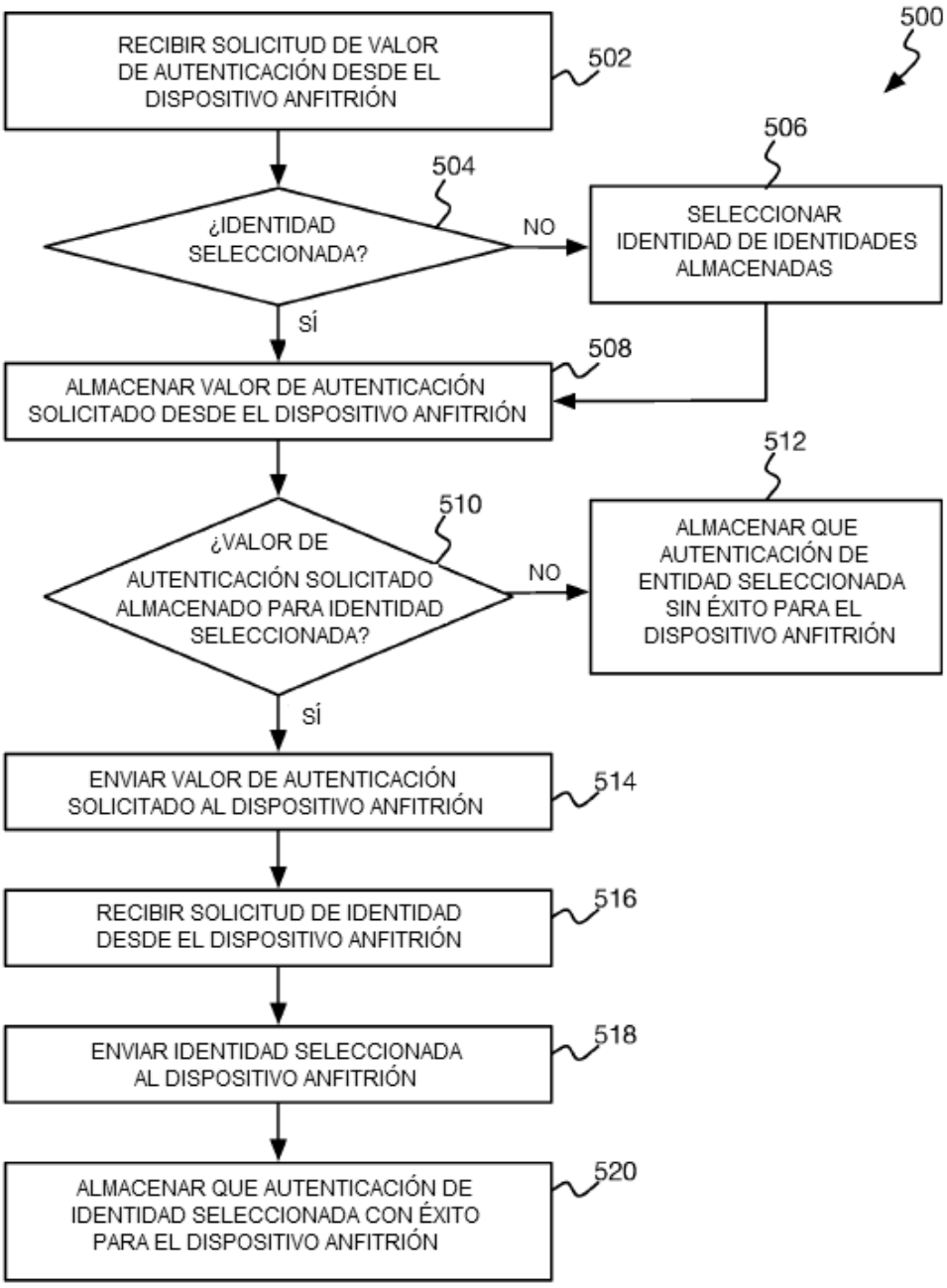

402
DETERMINAR SI EL ELEMENTO REEMPLAZABLE SE HA CONECTADO PREVIAMENTE AL DISPOSITIVO ANFITRIÓN
402
404
¿CONECTADO PREVIAMENTE?
NO
406
SELECCIONAR ALEATORIAMENTE IDENTIDAD DE ELEMENTO REEMPLAZABLE
SÍ
DETERMINAR SI EL ELEMENTO REEMPLAZABLE SE AUTENTICÓ CON ÉXITO PREVIAMENTE CON EL DISPOSITIVO ANFITRIÓN
408
410
¿AUTENTICADO CON ÉXITO?
SÍ
412
SELECCIONAR IDENTIDAD DE ELEMENTO REEMPLAZABLE QUE SE AUTENTICÓ CON ÉXITO
NO
SELECCIONAR IDENTIDAD DE ELEMENTO REEMPLAZABLE QUE EL ELEMENTO REEMPLAZABLE NO ENVIÓ PREVIAMENTE AL DISPOSITIVO ANFITRIÓN
414

FIG 5


500
RECIBIR SOLICITUD DE VALOR DE AUTENTICACIÓN DESDE EL DISPOSITIVO ANFITRIÓN
502
¿IDENTIDAD SELECCIONADA?
504
NO
SÍ
SELECCIONAR IDENTIDAD DE IDENTIDADES ALMACENADAS
506
ALMACENAR VALOR DE AUTENTICACIÓN SOLICITADO DESDE EL DISPOSITIVO ANFITRIÓN
508
¿VALOR DE AUTENTICACIÓN SOLICITADO ALMACENADO PARA IDENTIDAD SELECCIONADA?
510
NO
SÍ
ALMACENAR QUE AUTENTICACIÓN DE ENTIDAD SELECCIONADA SIN ÉXITO PARA EL DISPOSITIVO ANFITRIÓN
512
ENVIAR VALOR DE AUTENTICACIÓN SOLICITADO AL DISPOSITIVO ANFITRIÓN
514
RECIBIR SOLICITUD DE IDENTIDAD DESDE EL DISPOSITIVO ANFITRIÓN
516
ENVIAR IDENTIDAD SELECCIONADA AL DISPOSITIVO ANFITRIÓN
518
ALMACENAR QUE AUTENTICACIÓN DE IDENTIDAD SELECCIONADA CON ÉXITO PARA EL DISPOSITIVO ANFITRIÓN
520

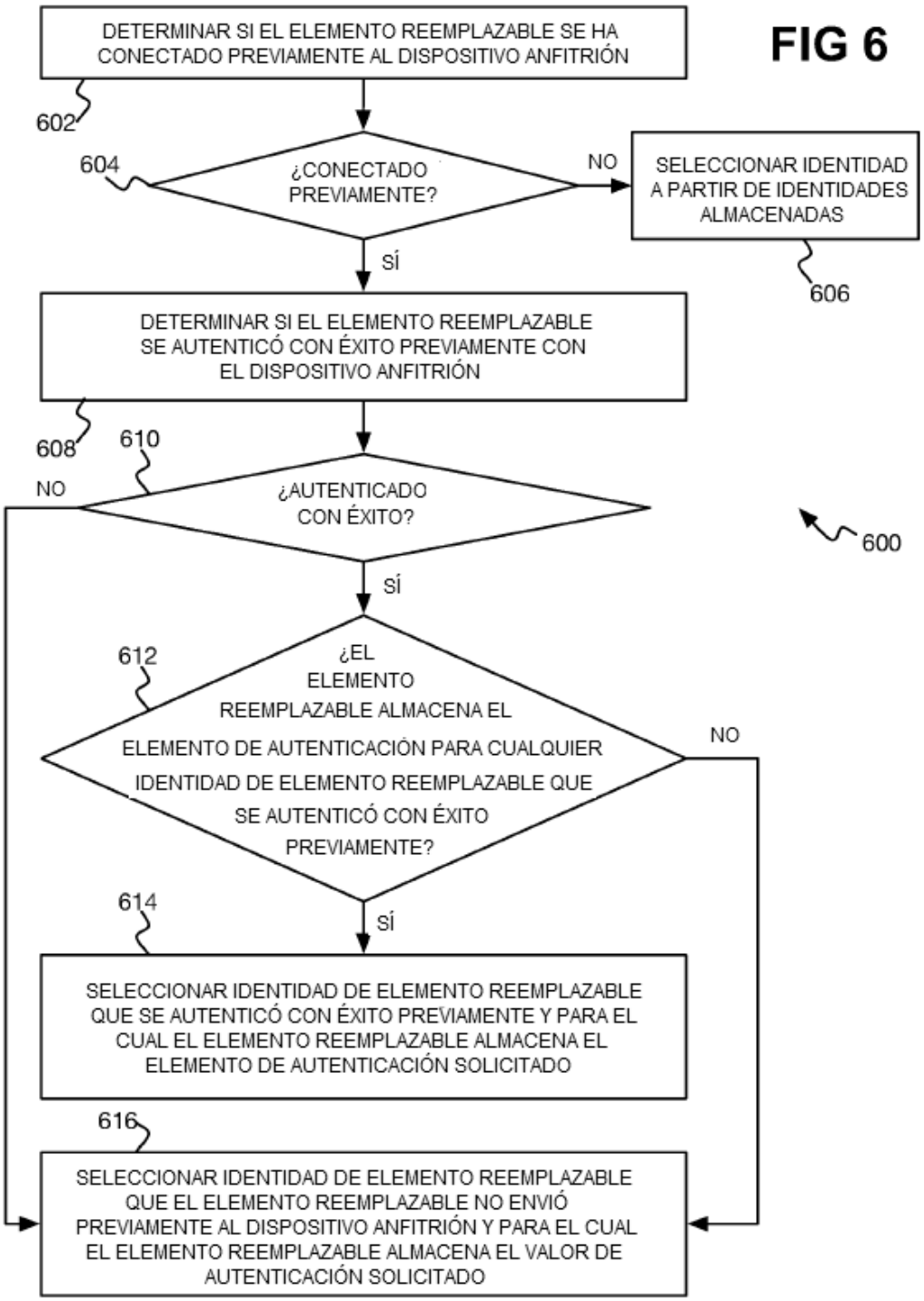
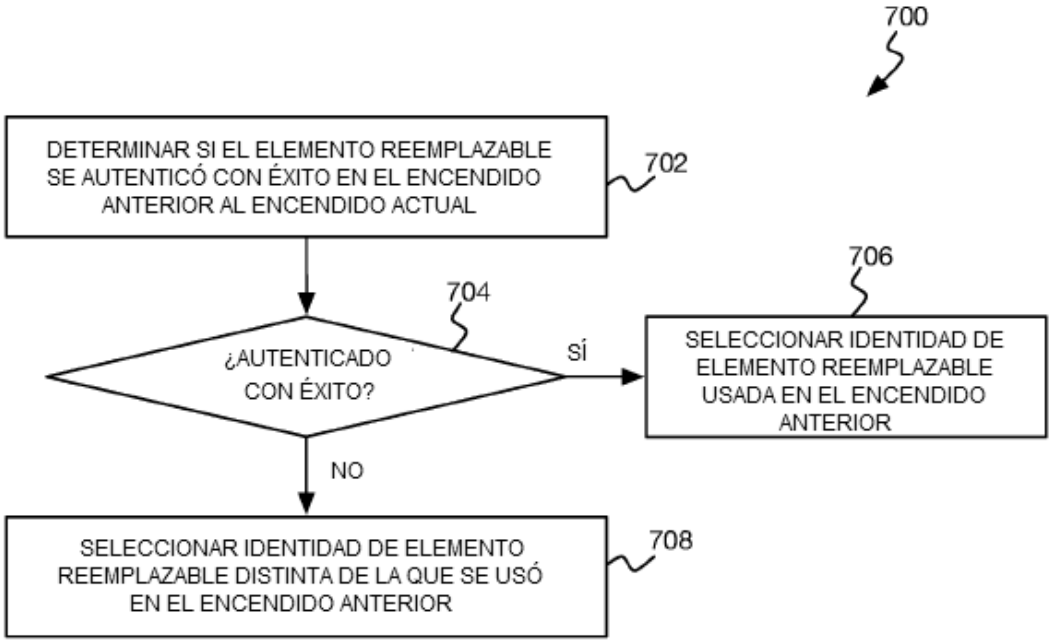

DETERMINAR SI EL ELEMENTO REEMPLAZABLE SE HA CONECTADO PREVIAMENTE AL DISPOSITIVO ANFITRIÓN
602
604
¿CONECTADO PREVIAMENTE?
NO
SELECCIONAR IDENTIDAD A PARTIR DE IDENTIDADES ALMACENADAS
606
SÍ
DETERMINAR SI EL ELEMENTO REEMPLAZABLE SE AUTENTICÓ CON ÉXITO PREVIAMENTE CON EL DISPOSITIVO ANFITRIÓN
608
610
NO
¿AUTENTICADO CON ÉXITO?
600
SÍ
612
¿EL ELEMENTO REEMPLAZABLE ALMACENA EL ELEMENTO DE AUTENTICACIÓN PARA CUALQUIER IDENTIDAD DE ELEMENTO REEMPLAZABLE QUE SE AUTENTICÓ CON ÉXITO PREVIAMENTE?
NO
614
SÍ
SELECCIONAR IDENTIDAD DE ELEMENTO REEMPLAZABLE QUE SE AUTENTICÓ CON ÉXITO PREVIAMENTE Y PARA EL CUAL EL ELEMENTO REEMPLAZABLE ALMACENA EL ELEMENTO DE AUTENTICACIÓN SOLICITADO
616
SELECCIONAR IDENTIDAD DE ELEMENTO REEMPLAZABLE QUE EL ELEMENTO REEMPLAZABLE NO ENVIÓ PREVIAMENTE AL DISPOSITIVO ANFITRIÓN Y PARA EL CUAL EL ELEMENTO REEMPLAZABLE ALMACENA EL VALOR DE AUTENTICACIÓN SOLICITADO

FIG 6

FIG 7


700
DETERMINAR SI EL ELEMENTO REEMPLAZABLE SE AUTENTICÓ CON ÉXITO EN EL ENCENDIDO ANTERIOR AL ENCENDIDO ACTUAL
702
704
¿AUTENTICADO CON ÉXITO?
SÍ
706
SELECCIONAR IDENTIDAD DE ELEMENTO REEMPLAZABLE USADA EN EL ENCENDIDO ANTERIOR
NO
SELECCIONAR IDENTIDAD DE ELEMENTO REEMPLAZABLE DISTINTA DE LA QUE SE USÓ EN EL ENCENDIDO ANTERIOR
708