(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 749 914**

(51) Int. CI.:

B41J 2/175 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **17.06.2016 PCT/US2016/038211**

(87) Fecha y número de publicación internacional: **21.12.2017 WO17218016**

(96) Fecha de presentación y número de la solicitud europea: **17.06.2016 E 16742058 (7)**

(97) Fecha y número de publicación de la concesión europea: **18.09.2019 EP 3297834**

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

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.03.2020

(73) Titular/es:

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

(72) Inventor/es:

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

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Autentificación de elemento reemplazable

Antecedentes

Los dispositivos que utilizan elementos reemplazables incluyen dispositivos de impresión, que incluyen impresoras, fotocopiadoras y dispositivos todo en uno (AIO) independientes que pueden realizar múltiples funciones, tal como imprimir, copiar, escanear y/o enviar faxes. Los elementos reemplazables de ejemplo para tales dispositivos de impresión incluyen tinta, tóner y/u otros tipos de colorante, incluido el colorante bidimensional (2D). Otros elementos de reemplazo de ejemplo, específicamente para dispositivos de impresión tridimensionales (3D), incluyen el agente de impresión 3D y el material de construcción de impresión 3D.

El documento US2006/008778 describe un sistema para verificar un cartucho de impresión comparando un número secreto almacenado en el cartucho con un número secreto para ese cartucho contenido en una base de datos. Se puede asociar una solicitud con un identificador de impresora y si una cantidad de solicitudes de verificación para un cartucho de impresión particular con diferentes identificadores de impresora asociados excede un umbral, se puede determinar que el número secreto ya no es secreto. El documento US2015/030818 describe un sistema de autentificación del cartucho de suministro de impresión en el que un servidor del cartucho emite un desafío de temporización criptográfica, en el que un desafío de cálculo matemático se debe completar correctamente en una ventana de tiempo esperada. El cálculo se puede realizar varias veces. El documento US2011109938 describe un componente de impresora reemplazable que incluye un primer dispositivo de memoria y un enlace de comunicación. El primer dispositivo de memoria se configura para almacenar un primer secreto. El enlace de comunicación se configura para vincular con capacidad de comunicación el primer dispositivo de memoria a un controlador de impresora cuando el componente de impresora reemplazable se instala en un sistema de impresión. El sistema de impresión comprende un segundo dispositivo de memoria que almacena un segundo secreto. El segundo dispositivo de memoria se vincula con capacidad de comunicación al controlador de impresora. El controlador de impresora se configura para determinar una autenticidad del componente de impresora reemplazable en función del primer secreto y el segundo secreto.

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 flujo de un método de ejemplo que puede realizar un cartucho de sustancia de impresión u otro elemento reemplazable para un dispositivo.

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 para implementar una parte del método de la FIG. 2.

La FIG. 4 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 para implementar una parte del método de la FIG. 2.

La FIG. 5 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 implementar una parte del método de la FIG. 2.

La FIG. 6 es un diagrama de flujo de un cuarto 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. 2.

Descripción detallada

Como se señaló en los antecedentes, los dispositivos que utilizan elementos reemplazables incluyen los 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 se agota, el cartucho se puede reemplazar por un cartucho que tenga un nuevo suministro de la sustancia de impresión en cuestión. Los cartuchos con diferentes tipos de sustancias de impresión también se pueden intercambiar según se desee. Como ejemplo, un cartucho que tiene tinta de uso general se puede cambiar por un cartucho que tiene tinta de calidad fotográfica en un dispositivo de impresión por inyección de tinta, según se desee.

Los fabricantes de dispositivos de impresión también suelen fabricar o suministrar de otro modo la sustancia de impresión utilizada en los dispositivos de impresión. Desde la perspectiva del usuario final, la utilización de cartuchos de sustancias de impresión suministrados o aprobados por el fabricante puede facilitar el resultado deseado por 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 el resultado del dispositivo de impresión o el funcionamiento del dispositivo de impresión si el dispositivo de impresión utiliza cartuchos de terceros. Una sustancia impresa de terceros está fuera del control del OEM. Por ejemplo, podría proporcionar diferentes resultados de impresión o implicar un riesgo evidente de acortar la vida útil del dispositivo de impresión. En algunos casos, tal como las 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, la utilización de una sustancia de impresión no aprobada puede afectar una garantía asociada con el dispositivo de impresión.

Por lo tanto, los fabricantes pueden inculcar cartuchos con seguridad de autentificación. 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 el OEM), entonces el dispositivo de impresión puede iniciar un determinado procedimiento, tal como, por ejemplo, informar al usuario final, tal como inmediatamente o poco después de la instalación.

Las técnicas descritas en la presente memoria proporcionan un esquema de autentificación novedoso e innovador para un cartucho de sustancia de impresión para un dispositivo de impresión, y más generalmente para un elemento reemplazable para un dispositivo (servidor) en el que se puede instalar el elemento (es decir, más generalmente, el dispositivo en el que el elemento se puede conectar). El cartucho de sustancia de impresión almacena varios valores de autentificación o contraseñas. El cartucho incluye lógica (tal como circuitos como un procesador y código de almacenamiento en memoria que ejecuta el procesador) para permitir la recuperación de solo un subconjunto de estos valores de autentificación. A medida que se solicitan diferentes valores de autentificación del cartucho, el cartucho puede rastrear el número de valores diferentes que se han devuelto. Una vez que el cartucho ha proporcionado el número máximo de dichos valores de autentificación únicos, no proporcionará ninguno de los otros valores de autentificación que se almacenaron originalmente en el cartucho. Sin embargo, el cartucho continúa proporcionando los valores de autentificación anteriores que se habían solicitado y devuelto.

Como ejemplo, un cartucho de sustancia de impresión puede almacenar sesenta y cuatro contraseñas diferentes o valores de autenticación. De estos sesenta y cuatro, el cartucho no puede generar más de dieciséis de las diferentes contraseñas. Una vez que el cartucho ha proporcionado dieciséis contraseñas diferentes, no proporcionará ninguna de las otras cuarenta y ocho contraseñas almacenadas 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 hash de los valores de autentificación o contraseñas. Los valores hash proporcionan una forma de determinar si un valor de autentificación determinado que el cartucho ha proporcionado es correcto. El cartucho puede proporcionar los valores hash de los valores de autentificación a solicitud, incluso para los valores que el cartucho no generará. En el ejemplo del párrafo anterior, por ejemplo, el cartucho puede proporcionar los valores hash para las sesenta y cuatro contraseñas, aunque el cartucho no proporcionará más de dieciséis de las sesenta y cuatro contraseñas.

Un esquema de autentificación que utiliza un cartucho de sustancia de impresión de este tipo puede incluir un dispositivo de impresión servidor que podría solicitar cuatro contraseñas diferentes, o valores de autenticación, almacenados en el cartucho. Diferentes dispositivos de impresión pueden y probablemente solicitarán diferentes contraseñas de un cartucho determinado. Del mismo modo, un dispositivo de impresión determinado puede y probablemente solicitará diferentes contraseñas de diferentes cartuchos.

Hacer que un cartucho de sustancia de impresión devuelva un número menor de valores de autentificación que el número total de valores de autentificación almacenados originalmente en el cartucho hace que sea mucho más difícil para un tercero frustrar dicho esquema de autenticación. Incluso si un tercero supera otras medidas de seguridad para obtener los dieciséis valores de autentificación que el cartucho "cederá", 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 autentificación de ejemplo que se ha presentado anteriormente, el dispositivo de impresión puede y probablemente solicitará al menos un valor de autentificación que no sea uno de los dieciséis valores que comparte el cartucho de terceros, lo que hace improbable que cualquier dispositivo de impresión determinado autentique con éxito un cartucho de este tipo.

La FIG. 1 muestra un cartucho de sustancia de impresión 100 de ejemplo para un dispositivo de impresión. El cartucho 100 incluye un suministro de sustancia de impresión 102. El cartucho 100 puede contener cualquier volumen de sustancia de impresión, tal como desde varios mililitros hasta decenas de litros. Los diferentes ejemplos de sustancia de impresión incluyen tinta para un dispositivo de impresión por chorro de tinta y tóner líquido o en polvo para un dispositivo de impresión láser. Dicha tinta y tóner son, en sí mismos, ejemplos de colorantes bidimensionales (2D), que es un colorante utilizado por un dispositivo de impresión adecuado para formar imágenes en medios como papel que, como mínimo, se extienden en una tercera dimensión perpendicular a las dos dimensiones que definen el plano de la superficie de los medios en los que se han formado las imágenes. Otros ejemplos de sustancia de impresión incluyen el agente de impresión tridimensional (3D) y el material de construcción de impresión 3D, que se utilizan por un dispositivo de impresión 3D adecuado para formar un objeto 3D que generalmente se puede retirar de cualquier sustrato sobre el cual se construye el objeto. Ciertas sustancias de impresión, tal como la tinta, se pueden usar tanto para la impresión 2D como 3D.

El cartucho de sustancia de impresión 100 incluye la 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 el código ejecutable por ordenador que ejecuta el procesador. A este respecto, entonces, en una implementación, la lógica 104 puede incluir un microprocesador y software integrado almacenado en el propio microprocesador, donde el medio de

almacenamiento de datos legible por computadora no volátil se integra en el microprocesador. En otra implementación, la lógica 104 puede incluir un microprocesador y un software integrado en un medio no volátil separado del microprocesador.

Como otro ejemplo, la lógica 104 puede ser o incluir un circuito integrado de aplicación específica (ASIC) o una matriz de puertas programable en campo (FPGA). Más generalmente a este respecto, la lógica 104 se puede implementar utilizando 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 de sustancia de impresión 100 incluye memoria no volátil 106. La memoria 106 puede ser memoria de semiconductores, y no es volátil, ya que cuando se corta la energía del cartucho 100, la memoria 106 aún retiene su contenido. La memoria 106 almacena las contraseñas 108, que también se denominan como valores de autentificación en la presente memoria. La memoria 106 puede almacenar valores hash 110 de, y que pueden corresponder individualmente a, las contraseñas 108. La memoria 106 puede almacenar una clave criptográfica 112 a partir de la cual se pueden generar las contraseñas 108.

La memoria 106 almacena un número de contraseñas 108, que se denomina como el número total de contraseñas 108. Las contraseñas 108, o valores de autenticación, son almacenados por el cartucho 100 de modo que el cartucho 100 pueda demostrar a un dispositivo de impresión servidor que es auténtico. Dicho de otra manera, las contraseñas 108 se utilizan para autenticar el cartucho 100 en el dispositivo de impresión. Las contraseñas 108 se pueden proteger de manera criptográfica cifrada, de modo que las contraseñas 108 sean, en esencia, irrecuperables del cartucho 100 fuera de los enfoques descritos en la presente memoria. Las contraseñas 108 pueden ser cada una, una serie de bits, tal como 256 bits.

La memoria 106 puede almacenar un valor hash 110 para cada contraseña 108. El cartucho 100 almacena los valores hash 110 para que el cartucho 100 pueda probar a un dispositivo de impresión servidor que las contraseñas 108 son correctas. Dicho de otra manera, los valores hash 110 se utilizan para verificar las contraseñas 108 proporcionadas por el cartucho 100 en el dispositivo de impresión. Los valores hash 110 pueden no estar protegidos criptográficamente por que se pueden recuperar libremente del cartucho 100, pero se pueden proteger criptográficamente por que los valores hash 110 no se pueden modificar. Los valores hash 110 pueden ser valores hash 110 unidireccionales de las contraseñas 108, lo que significa que una contraseña 108 no se puede determinar simplemente conociendo su valor hash 110 correspondiente, incluso si la función hash unidireccional utilizada para generar el valor hash 110 de la contraseña 108 es conocida.

El cartucho 100 puede proporcionar los valores hash 110 en una implementación de manera que un dispositivo servidor pueda validar los valores hash 110 como que han sido generados por una entidad (es decir, el fabricante o proveedor del cartucho 100) que la que el dispositivo servidor confía. Como ejemplo, los valores hash 110 se pueden firmar criptográficamente con una clave criptográfica privada antes del almacenamiento en el cartucho 100. El dispositivo servidor puede utilizar una clave criptográfica pública correspondiente para validar los valores hash 110. La clave privada no se puede almacenar en el cartucho 100 y no está disponible públicamente.

La lógica 104 permite recuperar un número máximo predeterminado de las contraseñas 108, menor que el número total de las contraseñas 108 almacenadas en la memoria no volátil 106. La lógica 104 puede permitir la recuperación de este número menor de las contraseñas 108 (es decir, el número máximo predeterminado de las contraseñas 108), sin embargo, un número ilimitado de veces desde la memoria 106. En comparación, la lógica 104 prohíbe la recuperación de cualquier contraseña 108 que no sea el número máximo predeterminado de contraseñas, incluso una vez, de la memoria 106.

Cuales de las contraseñas 108 se seleccionan como el número máximo predeterminado de las contraseñas 108 de las cuales la lógica 104 permite la recuperación puede no especificarse a priori. Cualquier dispositivo de impresión servidor en el que el cartucho 100 está instalado actualmente o al que está conectado el cartucho 100 de otro modo solicita contraseñas 108 particulares, la lógica 104 puede devolver las contraseñas 108 solicitadas hasta que se haya alcanzado el número máximo predeterminado. Acto seguido, la lógica 104 solo devolverá las contraseñas 108 que ya se han solicitado, y no devolverá ninguna de las otras contraseñas 108, una vez que se haya seleccionado el número predeterminado de las contraseñas 108. Dicho de otra manera, la lógica 104 puede seleccionar el número máximo predeterminado particular de las contraseñas 108 a medida que las solicite cualquier dispositivo de impresión servidor, hasta que se haya alcanzado el número máximo.

Como ejemplo, la memoria no volátil 106 puede almacenar dieciséis contraseñas 108, numeradas del uno al dieciséis, y la lógica 104 puede devolver solo cuatro de estas contraseñas 108. El cartucho 100 se puede insertar en un primer dispositivo de impresión servidor, que puede solicitar y recibir contraseñas con los números uno y trece. Por lo tanto, la lógica 104 ha seleccionado de forma efectiva dos de las cuatro contraseñas 108 que revelará el cartucho 100, las numeradas uno y trece. A continuación, el cartucho se puede retirar de este dispositivo de impresión servidor y se puede insertar en otro dispositivo de impresión servidor que solicite y reciba contraseñas con los números seis y trece. Por lo tanto, ahora la lógica 104 ha seleccionado de forma efectiva tres de las cuatro contraseñas 108 que revelará el cartucho 100, las numeradas uno, seis y trece.

El cartucho se puede retirar del dispositivo de impresión servidor en el que está instalado actualmente y se puede insertar en un tercer dispositivo de impresión servidor, que puede solicitar y recibir contraseñas con los números siete y trece. Por lo tanto, ahora la lógica 104 ha seleccionado de forma efectiva todas las cuatro de las cuatro contraseñas 108 que revelará el cartucho 100, las numeradas uno, seis, siete y trece. La lógica 104 puede continuar devolviendo estas cuatro contraseñas 108, pero no devolverá ninguna otra contraseña 108. Es decir, la lógica 104 no devolverá ninguna contraseña 108 a menos que tenga un número de uno, seis, siete o trece.

La memoria no volátil 106 utilizada para el almacenamiento de las contraseñas 108 puede ser una memoria de escritura limitada y lectura limitada. Las contraseñas 108 se escriben en la memoria 106 solo una vez, tal como durante un proceso de fabricación seguro. Se puede leer un número máximo predeterminado del número total de las contraseñas 108 un número ilimitado de veces. Las contraseñas 108 distintas de este número máximo predeterminado se vuelven ilegibles una vez que se ha seleccionado específicamente el número máximo predeterminado de las contraseñas 108. Por lo tanto, cada contraseña 108 se puede recuperar un número ilimitado de veces o puede ser irrecuperable, pero la lógica 104 no determina de antemano qué contraseñas 108 son cuáles.

Por lo tanto, las contraseñas 108 distintas del número máximo predeterminado de las contraseñas 108 se borran al menos funcionalmente una vez que se ha seleccionado específicamente el número máximo predeterminado de las contraseñas 108. Se pueden borrar completa e indeleblemente de la memoria 108 mediante la lógica 104, por ejemplo, de manera que el "desborrado" o la recuperación de las contraseñas borradas 108 se considere imposible. Las contraseñas 108 en cuestión se pueden borrar funcionalmente porque estas contraseñas 108 permanecen almacenadas en la memoria 108, pero son irrecuperables. Por ejemplo, los enlaces de fusible a las partes físicas de la memoria 108 donde se almacenan las contraseñas 108 en cuestión se pueden cortar, haciendo que las contraseñas 108 sean irrecuperables y, por lo tanto, borradas funcionalmente, aunque en realidad las contraseñas 108 permanecen en la memoria.

La memoria 106 puede almacenar la clave criptográfica 112 en lugar de las contraseñas 108 cuando se fabrica el cartucho 100. En esta implementación, antes de la primera utilización del cartucho 100, no se pueden almacenar contraseñas 108 en el cartucho 108. Más bien, cuando se solicita una contraseña 108, el cartucho 100 genera la contraseña 108 "sobre la marcha", si el cartucho 100 todavía no ha generado y proporcionado el número máximo predeterminado de contraseñas únicas 108. Una vez que se ha generado el número máximo predeterminado de contraseñas únicas 108, la clave criptográfica 112 se puede borrar al menos funcionalmente, de la manera descrita en el párrafo anterior.

La FIG. 2 muestra un método de ejemplo 200 que puede realizar un elemento reemplazable para un dispositivo, tal como el cartucho de sustancia de impresión 100 para un dispositivo de impresión. El método 200 se puede implementar como 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 200, por ejemplo. El elemento reemplazable realiza el método 200 una vez que se ha instalado en un dispositivo servidor.

El elemento reemplazable recibe una solicitud del dispositivo servidor para un valor de autentificación particular de varios valores de autentificación que el elemento puede almacenar (202). La solicitud se puede firmar con una clave criptográfica digital, o se puede proteger de otra manera. El elemento reemplazable determina si ha enviado previamente el valor de autentificación en cuestión a cualquier dispositivo servidor (203), incluido el dispositivo servidor en el que el elemento está instalado actualmente, así como a cualquier otro dispositivo servidor. Si el elemento reemplazable ha enviado previamente el valor de autentificación solicitado (204), el elemento devuelve el valor solicitado al dispositivo servidor (206).

Sin embargo, si el elemento reemplazable no ha enviado previamente el valor de autentificación solicitado (206), el elemento determina si ya ha enviado el número máximo de valores de autentificación únicos (208). Por ejemplo, de sesenta y cuatro valores de autentificación que el elemento reemplazable puede almacenar, el elemento no puede enviar más de dieciséis de estos valores. Si el elemento de reemplazo ya ha enviado el número máximo de valores de autentificación únicos (210), el elemento no envía el valor de autentificación que ha solicitado el dispositivo servidor en el que está instalado el elemento (212).

Sin embargo, si el elemento reemplazable aún no ha enviado el número máximo de valores de autentificación únicos, entonces el elemento envía el valor de autentificación solicitado al dispositivo servidor (214). A continuación, el elemento reemplazable puede determinar nuevamente si se ha enviado el número máximo de valores de autentificación (216), incluido el valor de autentificación que el elemento acaba de enviar en la parte 214. Por ejemplo, si se permite que el elemento envíe solo dieciséis de sus sesenta y cuatro valores de autenticación, si se enviaron quince valores antes de la ejecución de la parte 214, entonces se envía un decimosexto valor de autentificación diferente en la parte 214, de tal manera que el número máximo de dieciséis valores de autentificación diferentes ahora haya sido enviado.

Si ahora se ha enviado el número máximo de valores de autentificación únicos (218), entonces el elemento reemplazable puede al menos borrar funcionalmente los valores de autentificación que almacena y que no se han enviado (220). Como tal, en el ejemplo en curso, una vez que se han enviado dieciséis valores de autentificación

diferentes, se borran los otros cuarenta y ocho valores de autenticación. Tenga en cuenta que cada vez que se realiza el método 200 de la FIG. 2, entonces, el elemento reemplazable puede enviar cualquier valor de autentificación que envió previamente, y puede enviar cualquier valor de autentificación que no haya enviado previamente siempre que el número máximo de valores de autentificación diferentes que el elemento enviará aún no haya sido alcanzado.

Desde las partes 206, 212 y 220, y desde la parte 218 cuando aún no se ha alcanzado el número máximo de valores de autentificación enviados únicos, o como un punto de entrada al método 200, el elemento reemplazable puede recibir del dispositivo servidor una solicitud de uno o más valores hash correspondientes a uno o más valores de autentificación (222). Por ejemplo, el elemento reemplazable puede recibir una solicitud para todos los valores hash correspondientes a todos los valores de autenticación, para solo uno de los valores hash correspondientes a solo uno de los valores de autenticación, y así sucesivamente. El elemento reemplazable puede recibir una solicitud de uno o más valores hash incluso después de que los valores de autentificación que nunca se hayan enviado se borren en la parte 220, después de que se haya alcanzado el número máximo de valores de autentificación únicos que el elemento enviará en la parte 218. Es decir, el elemento reemplazable puede no borrar los valores hash para los valores de autentificación que borra, por ejemplo. La parte 222 se puede considerar como un punto de entrada al método 200 por que la solicitud de los valores hash se puede recibir antes de recibir una solicitud de un valor de autenticación.

La FIG. 3 muestra un método 300 de ejemplo que es un ejemplo de una implementación particular de las partes 202 a la parte 220 del método 200. Las partes numeradas de idéntica forma en las Fig. 2 y 3 se realizan en el método 300 al menos, en esencia, según se describió anteriormente en relación con el método 200. Los números entre paréntesis indican que una parte dada del método 300 está implementando una parte correspondiente del método 200. Es decir, Y(X) en la FIG. 3 significa que la parte Y del método 300 está implementando la parte X del método 200.

En la Fig. 3, los valores de autentificación pueden tener identificadores, tal como identificadores únicos correspondientes, que también se pueden denominar direcciones. Por ejemplo, si el elemento reemplazable almacena sesenta y cuatro valores de autenticación, los identificadores pueden ser uno, dos, tres, y así sucesivamente, hasta sesenta y cuatro. El elemento reemplazable recibe una solicitud del dispositivo servidor en el que está instalado para un valor de autentificación por identificador (302). Por ejemplo, el dispositivo servidor puede solicitar el valor de autentificación que tiene el identificador ABCD, puede solicitar el sexto valor de autenticación, de tal manera que el identificador del valor de autentificación solicitado sea seis, y así sucesivamente.

En la Fig. 3, el elemento reemplazable puede tener dos tablas. La primera tabla tiene un número de entradas igual al número máximo de diferentes valores de autentificación que el elemento reemplazable devolverá a cualquier dispositivo servidor. Cuando el elemento reemplazable aún no se ha utilizado en ningún dispositivo servidor, todas las entradas pueden estar vacías. Es decir, las entradas de la primera tabla están inicialmente vacías. La primera tabla almacena al menos los identificadores de los valores de autentificación que el elemento reemplazable ha enviado a cualquier dispositivo servidor. La primera tabla también puede almacenar los propios valores de autenticación. El elemento reemplazable puede almacenar la primera tabla de forma criptográfica segura.

La segunda tabla tiene un número de entradas igual al número de valores de autentificación que almacena el elemento reemplazable, tal como antes de que el elemento reemplazable aún no se haya utilizado en ningún dispositivo servidor. Cada entrada incluye al menos un valor de autenticación. Cada entrada puede almacenar además el identificador del valor de autenticación. Si los identificadores no se almacenan en la segunda tabla, entonces se pueden determinar por referencia. Por ejemplo, si hay sesenta y cuatro entradas, la primera entrada puede almacenar el valor de autentificación con el identificador más bajo, la segunda entrada puede almacenar el valor de autentificación con el identificador igual al identificador más bajo más un valor de incremento, y la tercera entrada puede almacenar el valor de autentificación con el identificador igual al identificador más bajo más dos veces el valor de incremento, y así sucesivamente. Por lo tanto, la sexagésima cuarta entrada puede almacenar el valor de autentificación que tiene el identificador igual al identificador más bajo más sesenta y tres veces el valor de incremento. Si el identificador más bajo es BASE y el valor de incremento es INC, el identificador del enésimo valor de autenticación, donde n es un valor de uno (el primer valor de autenticación) a N (el último valor de autenticación) es BASE + INC x (n-1).

Por lo tanto, el elemento reemplazable busca el identificador solicitado en la primera tabla (303). Es decir, si el elemento reemplazable recibió una solicitud del dispositivo servidor en la parte 302 para el valor de autentificación que tiene un identificador determinado, el elemento reemplazable busca el identificador determinado en la primera tabla. Si el elemento reemplazable recibió una solicitud en la parte 302 para el quinto valor de autenticación, el identificador de este valor de autentificación puede ser cinco, o se puede determinar como se describió anteriormente, en el cual entonces el elemento busca en la primera tabla. Si el identificador solicitado está en la primera tabla, entonces esto significa que el elemento reemplazable envió previamente el valor de autentificación que tiene este identificador. Si el identificador solicitado no está en la primera tabla, entonces esto significa que el elemento no ha enviado previamente el valor de autentificación que tiene este identificador.

Si el identificador está en la primera tabla, el elemento reemplazable envía el valor de autentificación que tiene este

identificador (206). Por ejemplo, si la primera tabla almacena valores de autentificación así como sus identificadores, entonces el elemento reemplazable puede recuperar el valor de autentificación en cuestión de la primera tabla. Si la primera tabla solo almacena identificadores y no los propios valores de autenticación, entonces el elemento reemplazable puede recuperar el valor de autentificación que tiene el identificador en cuestión de la segunda tabla para devolver al dispositivo servidor.

Si el identificador no está en la primera tabla, entonces el elemento reemplazable determina si hay entradas vacías en la primera tabla (306). Si hay entradas vacías en la primera tabla, entonces esto significa que el elemento reemplazable aún no ha enviado el número máximo de valores de autentificación diferentes. Si no hay entradas vacías en la primera tabla, entonces esto significa que el elemento reemplazable ya ha enviado el número máximo de valores de autentificación diferentes. Por lo tanto, si no hay entradas vacías (308), el elemento reemplazable rechaza enviar el valor de autentificación solicitado (212).

Sin embargo, si hay entradas vacías en la primera tabla (308), entonces el elemento reemplazable recupera el valor de autentificación que tiene el identificador solicitado de la segunda tabla (310). El elemento localiza un identificador vacío en la primera tabla (312) y almacena al menos el identificador del valor de autentificación recuperado en esta entrada vacía (314). Por ejemplo, el elemento puede almacenar el valor de autentificación en la entrada, así como el identificador de este valor. El elemento reemplazable a continuación envía el valor de autentificación de vuelta al dispositivo servidor que solicitó el valor (214).

El elemento reemplazable a continuación determina si la primera tabla ahora tiene entradas vacías (316). Si no hay más entradas vacías después de que la entrada vacía situada en la parte 312 se haya llenado en la parte 314, entonces esto significa que se ha alcanzado el número máximo de valores de autentificación diferentes que puede proporcionar el elemento reemplazable. Si todavía hay al menos una entrada vacía en la primera tabla después de que la entrada vacía situada en la parte 312 fuese llenada en la parte 314, entonces esto significa que aún no se ha alcanzado el número máximo de valores de autentificación diferentes que el elemento reemplazable puede proporcionar. Por lo tanto, si quedan entradas vacías en la primera tabla (318), el método 300 se termina (320).

Si no quedan entradas vacías en la primera tabla (318), el elemento reemplazable borra los valores de autentificación de la segunda tabla (220). El elemento reemplazable puede borrar de la segunda tabla solo los valores de autentificación que no ha proporcionado, que son aquellos valores de autentificación que tienen identificadores que no están almacenados en la primera tabla. Si la primera tabla almacena tanto identificadores como valores de autenticación, en lugar de solo identificadores, entonces el elemento reemplazable puede borrar todos los valores de autentificación de la segunda tabla. Por ejemplo, el elemento reemplazable puede eliminar la segunda tabla por completo. El elemento reemplazable puede borrar la segunda tabla porque el elemento almacena los valores de autentificación que aún responderá a las solicitudes adecuadas de los dispositivos servidor en la primera tabla. En otra implementación, el elemento reemplazable responde a las solicitudes de valores de autentificación de la primera tabla, y si un valor de autentificación solicitado no se almacena en la primera tabla, puede recuperar el valor de la segunda tabla para almacenarlo en la primera tabla solo si hay una entrada vacía disponible en la primera tabla en la que almacenar el valor solicitado.

La FIG. 4 muestra un método 400 de ejemplo que es otro ejemplo de una implementación particular de las partes 202 a 220 del método 200. Las partes numeradas de idéntica forma en las Fig. 2 y 4 se realizan en el método 400 al menos como se ha descrito en relación con el método 200. Los números entre paréntesis indican que una parte determinada del método 400 está implementando una parte correspondiente del método 200. Es decir, Y(X) en la FIG. 4 significa que la parte Y del método 400 está implementando la parte X del método 200.

El elemento reemplazable recibe una solicitud de un valor de autentificación del dispositivo servidor en el que está instalado (202). El elemento reemplazable determina si el valor de autentificación fue enviado previamente (203). Si el valor de autentificación fue enviado previamente (204), entonces el elemento reemplazable envía el valor de autentificación que se ha solicitado de vuelta al dispositivo servidor (206).

El elemento reemplazable mantiene un contador del número de valores de autentificación únicos que el elemento ha proporcionado a cualquier dispositivo servidor en la implementación de la FIG. 4. El contador puede ser un contador de solo incremento, que se puede aumentar y no se puede disminuir. El contador se almacena en una memoria no volátil, tal como la memoria no volátil 106, y se puede proteger criptográficamente.

El elemento reemplazable determina si el contador es igual al número máximo de valores de autentificación únicos que el elemento proporcionará a cualquier dispositivo servidor si se solicita correctamente (402). Si el contador es igual a este número máximo de valores de autentificación únicos, entonces esto significa que el elemento reemplazable ya ha proporcionado el número máximo de valores de autentificación diferentes que proporcionará a cualquier dispositivo servidor. Por lo tanto, si el contador es igual al número máximo de valores de autentificación únicos (404), entonces el elemento reemplazable no envía el valor de autentificación solicitado al dispositivo servidor (212).

Si el contador no es igual al número máximo de valores de autentificación únicos (es decir, el contador es menor que este número), entonces esto significa que el elemento reemplazable aún no ha proporcionado el número máximo de

valores de autentificación diferentes que proporcionará a cualquier dispositivo servidor. Por lo tanto, el elemento reemplazable envía el valor de autentificación solicitado de vuelta al dispositivo servidor (214). El elemento reemplazable también incrementa el contador (406).

El elemento reemplazable determina si el contador ahora es igual al número máximo de valores de autentificación únicos que proporcionará a cualquier dispositivo servidor (408). Si el contador aún no es igual al número máximo de valores de autentificación únicos (410), entonces el método 400 se termina (412). Sin embargo, si el contador ahora es igual a este número (410), entonces esto significa que el elemento reemplazable ahora ha enviado el número máximo de diferentes valores de autentificación que proporcionará y, como tal, puede borrar los valores de autentificación que no se han proporcionado o enviado a cualquier dispositivo servidor (220).

La FIG. 5 muestra un método 500 de ejemplo que es un tercer ejemplo de una implementación particular de las partes 202 a 220 del método 200. Las partes numeradas de idéntica forma en las Fig. 2 y 5 se realizan en el método 500 al menos como se ha descrito en relación con el método 200. Los números entre paréntesis indican que una parte determinada del método 500 está implementando una parte correspondiente del método 200. Es decir, Y(X) en la FIG. 5 significa que la parte Y del método 500 está implementando la parte X del método 200.

El elemento reemplazable recibe una solicitud de un valor de autentificación del dispositivo servidor en el que está instalado (202). El elemento reemplazable determina si el valor de autentificación fue enviado previamente (203). Si el valor de autentificación fue enviado previamente a cualquier dispositivo servidor (204), entonces el elemento reemplazable envía el valor de autentificación de vuelta al dispositivo servidor en el que está instalado (206).

El elemento reemplazable mantiene un indicador correspondiente a si el elemento ha proporcionado el número máximo de valores de autentificación únicos a cualquier dispositivo servidor en la implementación de la FIG. 5. El indicador puede ser un indicador solo ajustable, que se puede establecer pero que no se puede borrar. El indicador se almacena en la memoria no volátil, tal como la memoria no volátil 106, y se puede proteger criptográficamente.

El elemento reemplazable determina si el indicador se ha establecido (502). Si se ha establecido el indicador, esto significa que el elemento reemplazable ya ha proporcionado el número máximo de diferentes valores de autentificación que proporcionará a cualquier dispositivo servidor. Por lo tanto, si se establece el indicador (504), entonces el elemento reemplazable no envía el valor de autentificación solicitado al dispositivo servidor (212). Si el indicador no está establecido, entonces esto significa que el elemento reemplazable aún no ha proporcionado el número máximo de valores de autentificación diferentes que proporcionará a cualquier servidor. Por lo tanto, el elemento reemplazable envía el valor de autentificación solicitado de vuelta al dispositivo servidor (214).

El elemento reemplazable determina si ahora se ha enviado el número máximo de valores de autentificación únicos (216). Si todavía no se ha enviado el número máximo de valores de autentificación diferentes (218), entonces el método 500 se termina. Sin embargo, si ahora se ha enviado el número máximo de diferentes valores de autentificación (218), el elemento reemplazable establece el indicador (508) y puede borrar los valores de autentificación que aún no se han proporcionado o enviado a ningún dispositivo servidor (220).

En una implementación diferente, el indicador se establece antes de enviar el valor de autenticación. Es decir, en esta implementación, se determina si el número máximo de autenticaciones se habrá enviado ahora con el envío de un valor de autenticación, y si es así, entonces se establece el indicador, y después de que el indicador se haya establecido, se envía el valor de autenticación. Los valores de autentificación que no se hayan enviado también se pueden borrar en esta implementación antes de enviar el valor de autentificación en cuestión. De manera más general, cualquier acción que se realice debido al envío del último valor de autentificación único que proporcionará el elemento reemplazable, tal como incrementar un contador, establecer un indicador, almacenar un valor en una tabla, etc., se puede realizar antes de enviar este último valor de autentificación único. Se observa a este respecto que, aún más generalmente, cualquier acción de este tipo que se realice junto con el envío de un valor de autentificación (y no el último valor de autenticación) se puede realizar antes de que el valor de autentificación se envíe realmente.

La FIG. 6 muestra un método 600 de ejemplo que es un cuarto ejemplo de una implementación particular de las partes 202 a 220 del método 200. Las partes numeradas de idéntica forma en las Fig. 2 y 6 se realizan en el método 600 al menos como se ha descrito en relación con el método 200. Los números entre paréntesis indican que una parte determinada del método 600 está implementando una parte correspondiente del método 200. Es decir, Y(X) en la FIG. 6 significa que la parte Y del método 600 está implementando la parte X del método 200.

El elemento reemplazable recibe una solicitud de un valor de autentificación de un dispositivo servidor (202). El elemento reemplazable determina si el valor de autentificación fue enviado previamente (203). Si el valor de autentificación fue enviado previamente a cualquier dispositivo servidor (204), entonces el elemento reemplazable envía el valor de autentificación de vuelta al dispositivo servidor solicitante (206).

Si el elemento reemplazable no ha enviado previamente el valor de autentificación solicitado (206), entonces el elemento determina si ya ha enviado el número máximo de valores de autentificación únicos (208). Si el elemento de reemplazo ya ha enviado el número máximo de valores de autentificación únicos (210), entonces el elemento no envía el valor de autentificación que el dispositivo servidor en cuestión ha solicitado (212). Por lo tanto, el método

600 se termina.

Sin embargo, si el elemento reemplazable aún no ha enviado el número máximo de valores de autentificación únicos (210), entonces el elemento genera el valor de autentificación a partir de una clave criptográfica (602), tal como la clave criptográfica 112 del cartucho de sustancia de impresión 100 de la FIG. 1. En la implementación de la FIG. 6, entonces, las contraseñas 108 se pueden no generar y almacenar a priori en el cartucho 100 en el momento de la fabricación del cartucho 100. Un cartucho de impresión 100 nunca utilizado puede no tener contraseñas 108 almacenadas en el mismo, sino que simplemente almacena la clave criptográfica 112 a partir de la cual se pueden generar las contraseñas 108. El elemento reemplazable, por lo tanto, envía el valor de autentificación que se ha solicitado y que el elemento acaba de generar al dispositivo servidor (214). A este respecto, se observa que la implementación de la FIG. 6 se puede emplear junto con al menos una parte de la implementación de la FIG. 3, en la que los valores enviados se almacenan en una primera tabla. Como tal, una vez que se ha generado el valor de autenticación, se puede almacenar en la primera tabla, de modo que el valor no se tenga que regenerar más tarde, y si o cuando la clave criptográfica se borre al menos funcionalmente, el valor de autentificación se pueda devolver.

El elemento reemplazable puede determinar nuevamente si se ha enviado el número máximo de valores de autentificación (216), incluido el valor de autentificación que el elemento acaba de enviar en la parte 214. Si aún no se ha enviado el número máximo de valores de autentificación (218), entonces el método 600 se termina. Sin embargo, si ahora se ha enviado el número máximo de valores de autentificación (218), entonces el elemento reemplazable puede al menos borrar funcionalmente la clave criptográfica (606), de modo que no se puedan generar valores de autentificación adicionales. La clave criptográfica se puede borrar al menos funcionalmente una vez que se ha generado el valor de autentificación en la parte 602, y antes de enviar realmente el valor de autentificación en la parte 214 en una implementación.

Las diferentes implementaciones de partes del método 200 que se han descrito en relación con los métodos 300, 400, 500 y 600 se pueden combinar o modificar de diferentes maneras. Por ejemplo, solo se puede emplear la primera tabla del método 300. Se pueden emplear una o más tablas del método 300 junto con el contador del método 400 y/o el indicador del método 500. El contador del método 400 se puede utilizar junto con el indicador del método 500 sin tampoco ninguna tabla del método 300. La primera tabla del método 300, el contador del método 400 y/o el indicador del método 500 se pueden utilizar junto con el enfoque del método 600.

Las técnicas descritas en la presente memoria pueden mejorar o proporcionar otro esquema para la seguridad criptográfica de un elemento reemplazable para un dispositivo, tal como un cartucho de suministro de impresión para un dispositivo de impresión. Un elemento reemplazable proporciona un número limitado de valores de autorización, o contraseñas, que almacena. Una vez que se haya proporcionado el número máximo de valores de autorización diferentes, no se atenderán las solicitudes de los otros valores de autorización, incluso si permanecen almacenados en el elemento reemplazable. Un enfoque de este tipo puede disminuir la probabilidad de que un tercero que intente recuperar todos los valores de autorización del elemento reemplazable tenga éxito. Además, la probabilidad de que la posesión de solo el número máximo de valores de autorización únicos de como resultado una autentificación exitosa es muy baja.

REIVINDICACIONES

1. Un medio de almacenamiento de datos legible por ordenador no transitorio que almacena código ejecutable por ordenador que, cuando se ejecuta mediante la lógica (104) de un elemento reemplazable, hace que la lógica (104) realice un método **caracterizado por** comprender:

en respuesta a la recepción de una solicitud de un valor de autentificación particular (108) de varios valores de autentificación (108) del elemento reemplazable de al menos un dispositivo servidor al que se ha conectado el elemento reemplazable, determinar si el elemento reemplazable envió previamente el valor de autentificación (108);

en respuesta a la determinación de que el valor de autentificación (108) se envió previamente, enviar el valor de autentificación (108) al dispositivo servidor;

en respuesta a la determinación de que el valor de autentificación (108) no se envió previamente, determinar si el elemento reemplazable envió previamente un número máximo de valores de autentificación únicos de los valores de autentificación (108) en respuesta a una solicitud de cualquier dispositivo servidor, siendo menor el número máximo de valores de autentificación únicos (108) que un número total de valores de autentificación (108);

en respuesta a la determinación de que no se ha enviado el número máximo de valores de autentificación únicos (108), enviar el valor de autentificación (108) al dispositivo servidor; y

en respuesta a la determinación de que se ha enviado el número máximo de valores de autentificación únicos (108), rechazar enviar el valor de autentificación (108) al dispositivo servidor.

2. El medio de almacenamiento de datos legible por ordenador no transitorio de la reivindicación 1, en donde cada valor de autentificación (108) tiene un identificador diferente, en donde la solicitud del valor de autentificación (108) comprende un identificador solicitado del valor de autentificación (108), en donde se determina si el elemento reemplazable que envió previamente el valor de autentificación comprende:

buscar el identificador solicitado en una tabla de al menos los diferentes identificadores de los valores de autentificación (108) que se han enviado previamente, en donde determinar que el valor de autentificación (108) fue enviado previamente comprende:

determinar que el identificador solicitado es uno de los diferentes identificadores en la tabla, en donde determinar que el valor de autentificación (108) no fue enviado previamente comprende:

determinar que el identificador solicitado no es uno de los diferentes identificadores en la tabla, y en donde el método comprende además, en respuesta a determinar que no se ha enviado el número máximo de valores de autentificación únicos (108):

recuperar el valor de autentificación (108) de una tabla diferente de todos los valores de autentificación mediante el identificador solicitado; y

almacenar al menos el identificador diferente del valor de autentificación (108) en la tabla de al menos los diferentes identificadores de los valores de autentificación (108) que se han enviado previamente.

3. El medio de almacenamiento de datos legible por ordenador no transitorio de la reivindicación 2, en donde la tabla de al menos los diferentes identificadores de los valores de autentificación (108) que se han enviado previamente tiene un número predeterminado de entradas que inicialmente están vacías, el número predeterminado de entradas igual al número máximo de valores de autentificación únicos (108) que se permite enviar al elemento de reemplazo, en donde almacenar al menos el identificador diferente del valor de autentificación (108) en la tabla de al menos los diferentes identificadores de los valores de autentificación (108) que se han enviado previamente comprende:

localizar una entrada vacía de la tabla de al menos los diferentes identificadores de los valores de autentificación (108) que se han enviado previamente; y

almacenar al menos el identificador diferente del valor de autentificación (108) en la entrada vacía, y en donde determinar si el elemento reemplazable envió previamente el número máximo de valores de autentificación únicos (108) comprende:

determinar si la tabla de al menos los diferentes identificadores de los valores de autentificación (108) que se han enviado previamente tiene entradas vacías.

4. El medio de almacenamiento de datos legible por ordenador no transitorio de la reivindicación 1, en donde determinar si el elemento reemplazable envió previamente el número máximo de valores de autentificación únicos (108) comprende:

determinar si un contador de un número único de los valores de autentificación (108) que el elemento reemplazable ha enviado previamente es igual al número máximo de valores de autentificación únicos (108), y en donde el método comprende además, en respuesta a determinar que no se ha enviado el número de valores de autentificación únicos (108):

incrementar el contador.

5. El medio de almacenamiento de datos legible por ordenador no transitorio de la reivindicación 1, en donde determinar si el elemento reemplazable envió previamente el número máximo de valores de autentificación únicos (108) comprende:

determinar si se ha establecido un indicador correspondiente al número máximo de valores de autentificación únicos (108) que se han enviado previamente, y en donde el método comprende además, en respuesta a determinar que el número máximo de valores de autentificación únicos (108) no se ha enviado:

determinar si el número máximo de valores de autentificación únicos (108) se ha enviado ahora o se hará enviar ahora;

en respuesta a la determinación de que el número máximo de valores de autentificación únicos (108) se ha enviado ahora o se hará enviar ahora, establecer el indicador.

6. El medio de almacenamiento de datos legible por ordenador no transitorio de la reivindicación 1, en donde el método comprende además, en respuesta a la determinación de que no se ha enviado el número máximo de valores de autentificación únicos (108):

una vez que se ha enviado el valor de autentificación (108) o se habrá enviado al dispositivo servidor, determinar si se ha enviado ahora el número máximo de valores de autentificación únicos (108);

en respuesta a la determinación de que el número máximo de valores de autentificación únicos (108) se ha enviado o se hará enviar ahora, borrar funcionalmente al menos los valores de autentificación (108) del elemento reemplazable que no se han enviado.

7. El medio de almacenamiento de datos legible por ordenador no transitorio de la reivindicación 1, en donde el método comprende además, en respuesta a la determinación de que el número máximo de valores de autentificación (108) no se ha enviado:

generar el valor de autentificación (108) a partir de una clave criptográfica (112) almacenada en el elemento reemplazable.

8. El medio de almacenamiento de datos legible por ordenador no transitorio de la reivindicación 7, en donde el método comprende además, en respuesta a la determinación de que el número máximo de valores de autentificación (108) no se ha enviado:

una vez que el valor de autentificación (108) se ha enviado o se hará enviar al dispositivo servidor, determinar si se ha enviado ahora el número máximo de valores de autentificación únicos (108);

en respuesta a la determinación de que el número máximo de valores de autentificación únicos (108) se ha enviado o se hará enviar ahora, borrar funcionalmente la clave criptográfica del elemento reemplazable de modo que los valores de autentificación (108) que no se hayan enviado no se puedan generar.

9. El medio de almacenamiento de datos legible por ordenador no transitorio de la reivindicación 1, en donde la solicitud es una primera solicitud, y el método comprende además:

recibir una segunda solicitud, mediante el elemento de reemplazo del dispositivo servidor, para un valor hash unidireccional (110) del valor de autentificación (108); y

enviar el valor hash unidireccional (110) mediante el elemento de reemplazo al dispositivo servidor, en donde la primera solicitud se recibe antes o después de que se reciba la segunda solicitud.

10. El medio de almacenamiento de datos legible por ordenador no transitorio de la reivindicación 1, en donde el dispositivo servidor es un dispositivo de impresión, y el elemento reemplazable es un cartucho de sustancia de impresión (100) para el dispositivo de impresión.

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

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

una memoria no volátil (106) que almacena varias contraseñas (108) y/o una clave criptográfica (112) a partir de la cual se pueden generar las contraseñas (108); y

caracterizado por comprender la lógica (104) para:

permitir la recuperación de un número máximo predeterminado de las contraseñas (108), menor que un número total de las contraseñas (108), de la memoria no volátil (106), para autenticar el cartucho de sustancia de impresión (100) en el dispositivo de impresión; y

seleccionar el número máximo predeterminado de las contraseñas (108) cuando cualquier dispositivo solicita una contraseña particular (108) de las contraseñas (108) de la memoria no volátil (106), hasta que se haya alcanzado el número máximo predeterminado de las contraseñas (108).

12. El cartucho de sustancia de impresión (100) de la reivindicación 11, en donde la lógica (104) es además para:

permitir la recuperación del número máximo predeterminado de las contraseñas (108) un número ilimitado de veces desde la memoria no volátil (106); y

prohibir la recuperación de cualquier contraseña (108) de las contraseñas (108) que no sea el número máximo predeterminado de las contraseñas (108) incluso una vez desde la memoria no volátil (106).

13. El cartucho de sustancia de impresión (100) de la reivindicación 11, en donde la memoria no volátil (106) es una memoria limitada de lectura y de solo escritura en la que el número máximo predeterminado de las contraseñas (108) es legible un número ilimitado de veces y las contraseñas (108) distintas del número máximo predeterminado de las contraseñas (108) no se pueden leer una vez que se ha seleccionado el número máximo predeterminado de las contraseñas (108).

14. El cartucho de sustancia de impresión (100) de la reivindicación 11, en donde la lógica (104) es además para:

al menos borrar funcionalmente al menos las contraseñas (108) que no sean el número máximo predeterminado de las contraseñas (108) una vez que se haya seleccionado el número máximo predeterminado de las contraseñas (108).

15. El cartucho de sustancia de impresión (100) de la reivindicación 11, en donde la lógica (104) es además, en respuesta a la recepción de una solicitud de una contraseña particular (108) de las contraseñas (108), para:

si la contraseña particular (108) ha sido enviada previamente, devolver la contraseña particular (108);

si la contraseña particular (108) no se ha enviado previamente y el número máximo predeterminado de las contraseñas (108) no se ha enviado, generar la contraseña particular (108) a partir de la clave criptográfica (112) y devolver la contraseña particular (108); y

si la contraseña particular (108) no se ha enviado previamente y se ha enviado el número máximo predeterminado de las contraseñas (108), rechazar generar y devolver la contraseña particular (108).

16. El cartucho de sustancia de impresión (100) de la reivindicación 15, en donde la lógica (104) es además, después de generar la contraseña particular (108) a partir de la clave criptográfica (112), para:

al menos borrar funcionalmente la clave criptográfica (112) si el número máximo predeterminado de las contraseñas se ha enviado o se hará enviar ahora.

17. El cartucho de sustancia de impresión (100) de la reivindicación 11, que comprende además:

una memoria no volátil (106) que almacena varios valores hash (110) de las contraseñas, en donde la lógica (104) debe permitir la recuperación de cualquier valor hash (110) un número ilimitado de veces desde la memoria no volátil (106).

18. El cartucho de suministro de impresión (100) de la reivindicación 11, en donde la sustancia de impresión es uno o más de:

tinta, tóner, colorante bidimensional (2D), agente de impresión tridimensional (3D) y material de construcción de impresión 3D.

FIG. 1

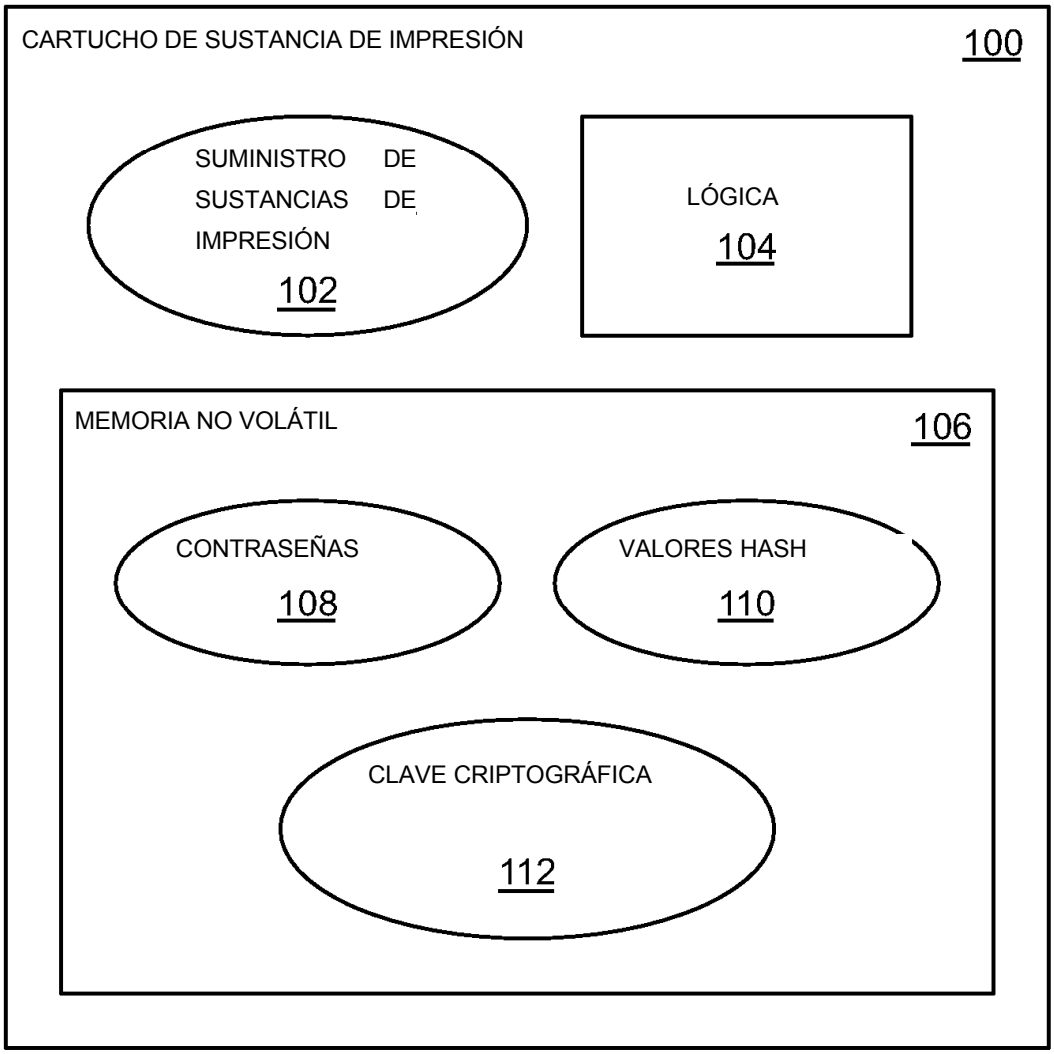
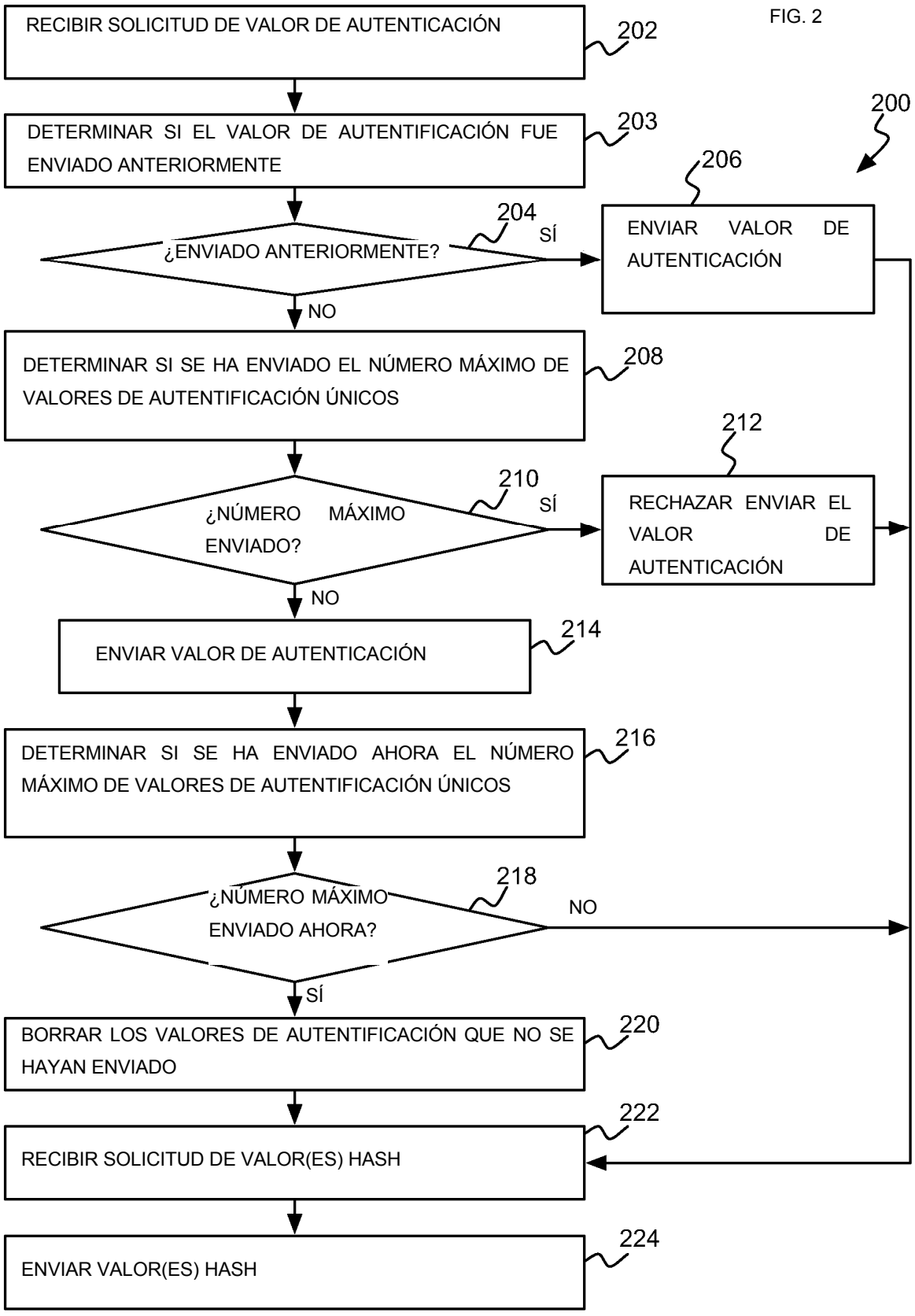

CARTUCHO DE SUSTANCIA DE IMPRESIÓN
100
SUMINISTRO DE SUSTANCIAS DE IMPRESIÓN
102
LÓGICA
104
MEMORIA NO VOLÁTIL
106
CONTRASEÑAS
108
VALORES HASH
110
CLAVE CRIPTOGRÁFICA
112

FIG. 2


RECIBIR SOLICITUD DE VALOR DE AUTENTICACIÓN
202
DETERMINAR SI EL VALOR DE AUTENTIFICACIÓN FUE ENVIADO ANTERIORMENTE
203
200
206
204
¿ENVIADO ANTERIORMENTE?
SÍ
ENVIAR VALOR DE AUTENTICACIÓN
NO
DETERMINAR SI SE HA ENVIADO EL NÚMERO MÁXIMO DE VALORES DE AUTENTIFICACIÓN ÚNICOS
208
212
210
¿NÚMERO MÁXIMO ENVIADO?
SÍ
RECHAZAR ENVIAR EL VALOR DE AUTENTICACIÓN
NO
ENVIAR VALOR DE AUTENTICACIÓN
214
DETERMINAR SI SE HA ENVIADO AHORA EL NÚMERO MÁXIMO DE VALORES DE AUTENTIFICACIÓN ÚNICOS
216
218
¿NÚMERO MÁXIMO ENVIADO AHORA?
NO
SÍ
BORRAR LOS VALORES DE AUTENTIFICACIÓN QUE NO SE HAYAN ENVIADO
220
222
RECIBIR SOLICITUD DE VALOR(ES) HASH
ENVIAR VALOR(ES) HASH
224

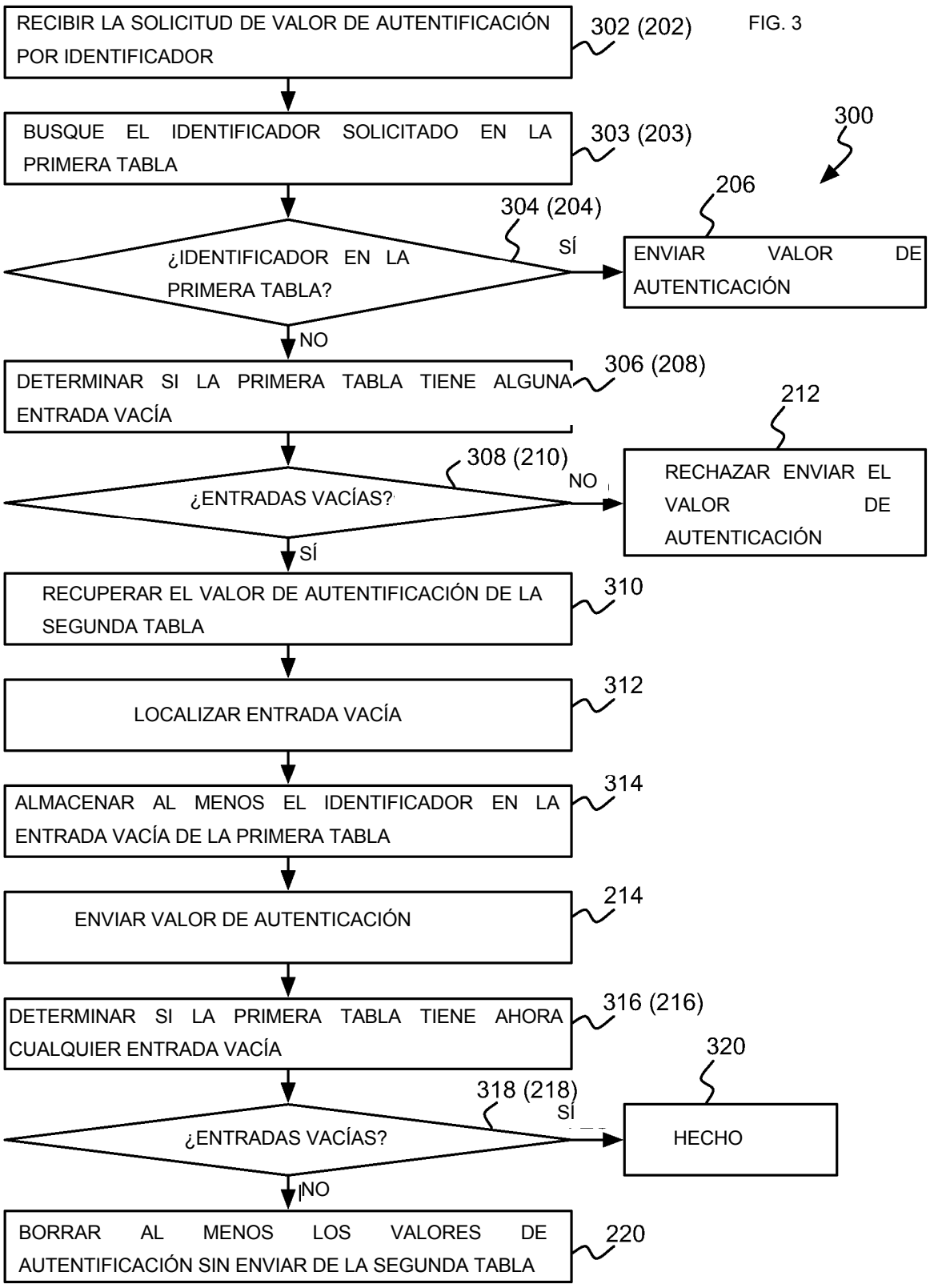

RECIBIR LA SOLICITUD DE VALOR DE AUTENTIFICACIÓN POR IDENTIFICADOR
302 (202)
BUSQUE EL IDENTIFICADOR SOLICITADO EN LA PRIMERA TABLA
303 (203)
300
206
304 (204)
¿IDENTIFICADOR EN LA PRIMERA TABLA?
SÍ
ENVIAR VALOR DE AUTENTICACIÓN
NO
DETERMINAR SI LA PRIMERA TABLA TIENE ALGUNA ENTRADA VACÍA
306 (208)
212
308 (210)
¿ENTRADAS VACÍAS?
NO
RECHAZAR ENVIAR EL VALOR DE AUTENTICACIÓN
SÍ
RECUPERAR EL VALOR DE AUTENTIFICACIÓN DE LA SEGUNDA TABLA
310
LOCALIZAR ENTRADA VACÍA
312
ALMACENAR AL MENOS EL IDENTIFICADOR EN LA ENTRADA VACÍA DE LA PRIMERA TABLA
314
ENVIAR VALOR DE AUTENTICACIÓN
214
DETERMINAR SI LA PRIMERA TABLA TIENE AHORA CUALQUIER ENTRADA VACÍA
316 (216)
320
318 (218)
¿ENTRADAS VACÍAS?
SÍ
HECHO
NO
BORRAR AL MENOS LOS VALORES DE AUTENTIFICACIÓN SIN ENVIAR DE LA SEGUNDA TABLA
220

FIG. 3

FIG. 4

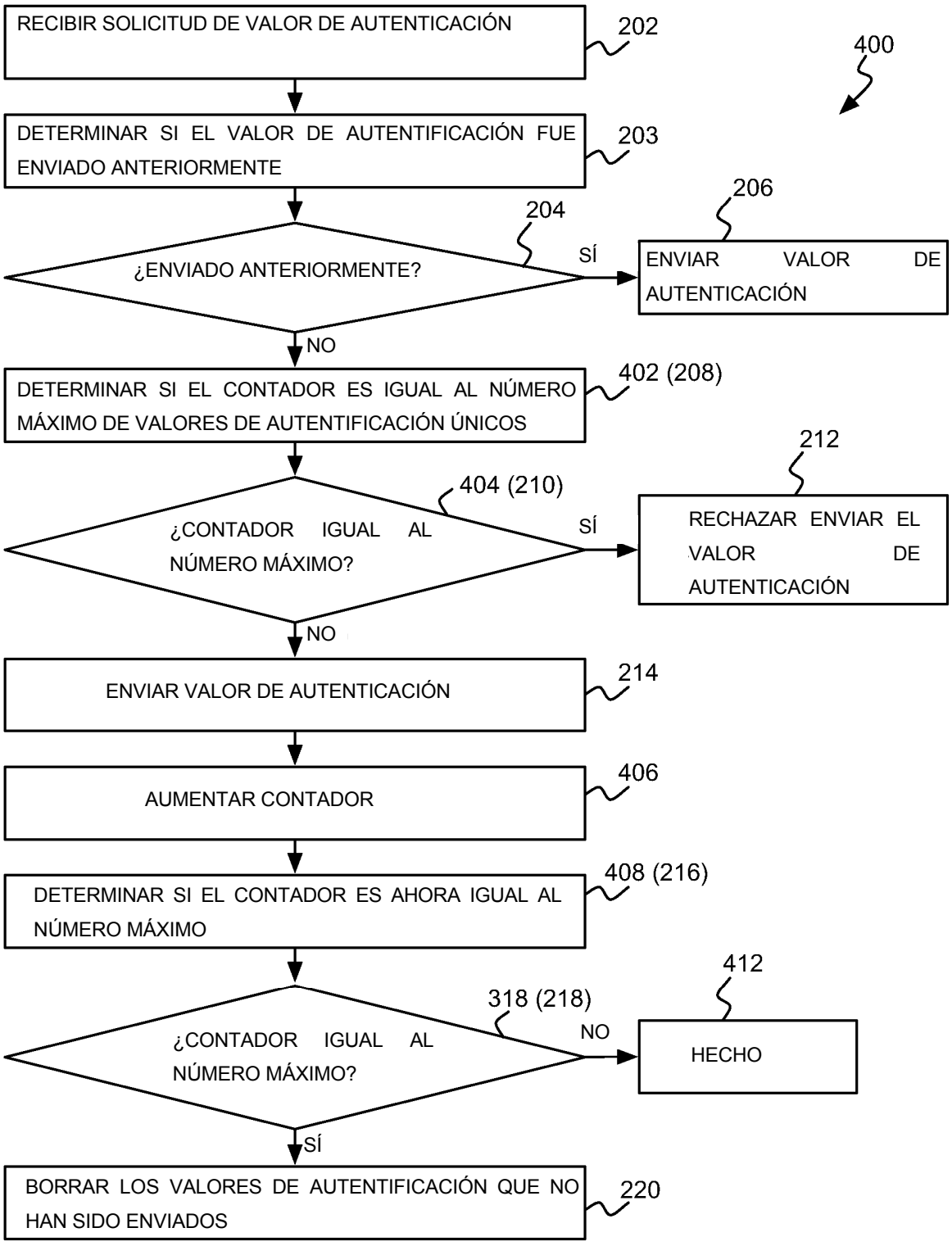

400
RECIBIR SOLICITUD DE VALOR DE AUTENTICACIÓN
202
DETERMINAR SI EL VALOR DE AUTENTIFICACIÓN FUE ENVIADO ANTERIORMENTE
203
¿ENVIADO ANTERIORMENTE?
204
SÍ
206
ENVIAR VALOR DE AUTENTICACIÓN
NO
DETERMINAR SI EL CONTADOR ES IGUAL AL NÚMERO MÁXIMO DE VALORES DE AUTENTIFICACIÓN ÚNICOS
402 (208)
¿CONTADOR IGUAL AL NÚMERO MÁXIMO?
404 (210)
SÍ
212
RECHAZAR ENVIAR EL VALOR DE AUTENTICACIÓN
NO
ENVIAR VALOR DE AUTENTICACIÓN
214
AUMENTAR CONTADOR
406
DETERMINAR SI EL CONTADOR ES AHORA IGUAL AL NÚMERO MÁXIMO
408 (216)
¿CONTADOR IGUAL AL NÚMERO MÁXIMO?
318 (218)
NO
412
HECHO
SÍ
BORRAR LOS VALORES DE AUTENTIFICACIÓN QUE NO HAN SIDO ENVIADOS
220

FIG. 5

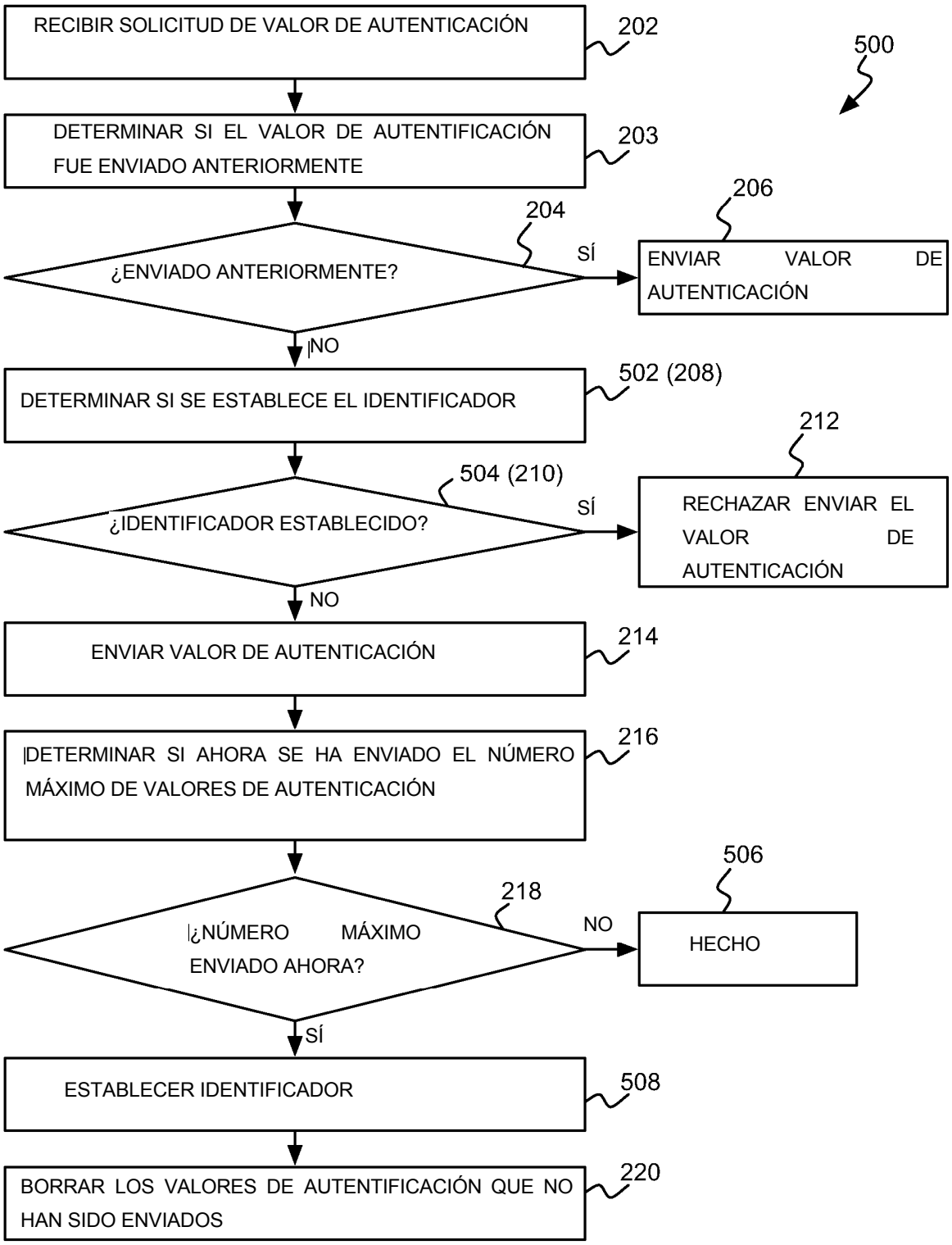
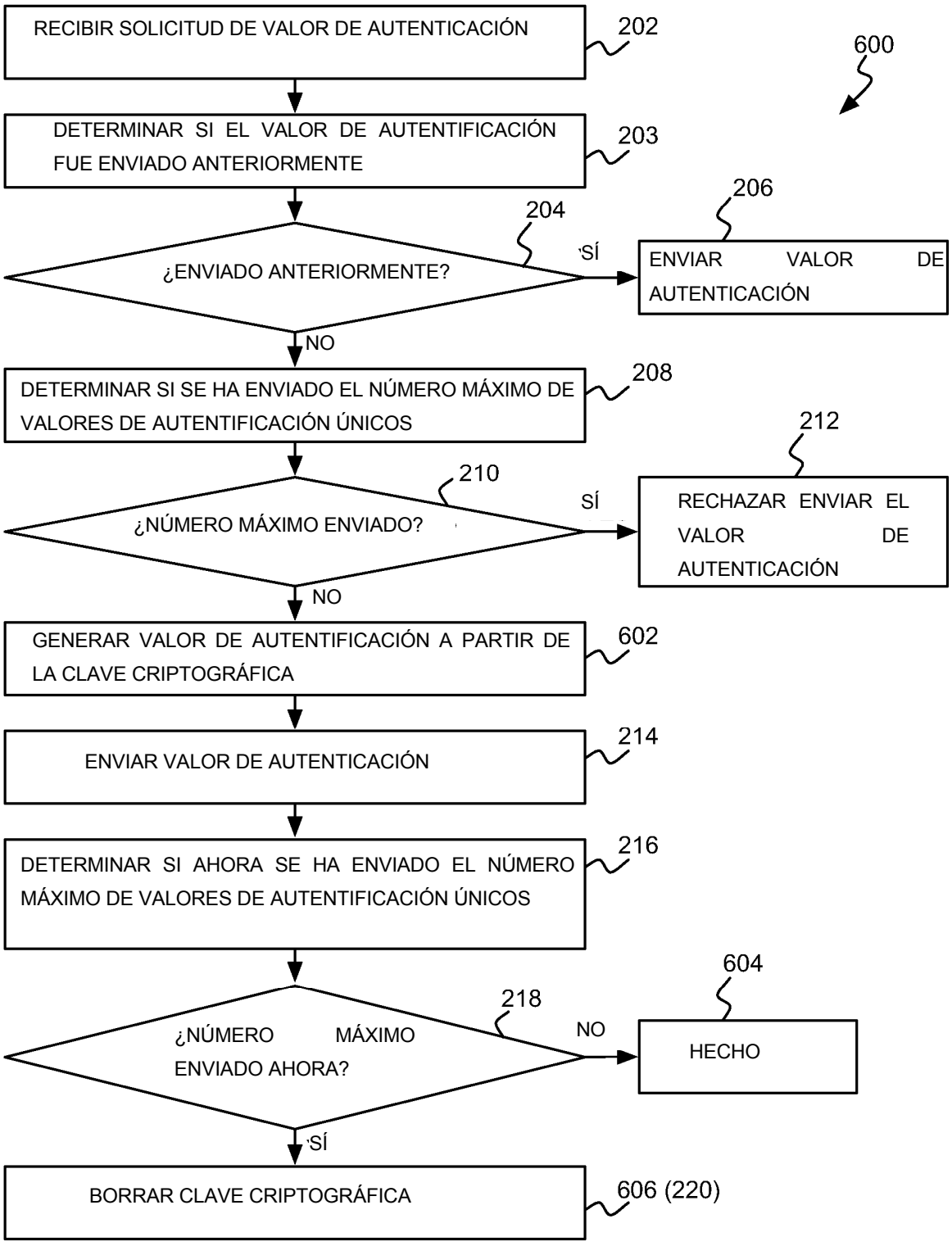

RECIBIR SOLICITUD DE VALOR DE AUTENTICACIÓN
202
500
DETERMINAR SI EL VALOR DE AUTENTIFICACIÓN FUE ENVIADO ANTERIORMENTE
203
206
204
¿ENVIADO ANTERIORMENTE?
SÍ
ENVIAR VALOR DE AUTENTICACIÓN
NO
DETERMINAR SI SE ESTABLECE EL IDENTIFICADOR
502 (208)
212
504 (210)
¿IDENTIFICADOR ESTABLECIDO?
SÍ
RECHAZAR ENVIAR EL VALOR DE AUTENTICACIÓN
NO
ENVIAR VALOR DE AUTENTICACIÓN
214
DETERMINAR SI AHORA SE HA ENVIADO EL NÚMERO MÁXIMO DE VALORES DE AUTENTICACIÓN
216
506
218
¿NÚMERO MÁXIMO ENVIADO AHORA?
NO
HECHO
SÍ
ESTABLECER IDENTIFICADOR
508
BORRAR LOS VALORES DE AUTENTIFICACIÓN QUE NO HAN SIDO ENVIADOS
220

FIG. 6


RECIBIR SOLICITUD DE VALOR DE AUTENTICACIÓN
202
600
DETERMINAR SI EL VALOR DE AUTENTIFICACIÓN FUE ENVIADO ANTERIORMENTE
203
206
204
¿ENVIADO ANTERIORMENTE?
SÍ
ENVIAR VALOR DE AUTENTICACIÓN
NO
DETERMINAR SI SE HA ENVIADO EL NÚMERO MÁXIMO DE VALORES DE AUTENTIFICACIÓN ÚNICOS
208
212
210
¿NÚMERO MÁXIMO ENVIADO?
SÍ
RECHAZAR ENVIAR EL VALOR DE AUTENTICACIÓN
NO
GENERAR VALOR DE AUTENTIFICACIÓN A PARTIR DE LA CLAVE CRIPTOGRÁFICA
602
ENVIAR VALOR DE AUTENTICACIÓN
214
DETERMINAR SI AHORA SE HA ENVIADO EL NÚMERO MÁXIMO DE VALORES DE AUTENTIFICACIÓN ÚNICOS
216
604
218
¿NÚMERO MÁXIMO ENVIADO AHORA?
NO
HECHO
SÍ
BORRAR CLAVE CRIPTOGRÁFICA
606 (220)