(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 717 099**

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **27.10.2016 PCT/US2016/059118**

(87) Fecha y número de publicación internacional: **03.05.2018 WO18080497**

(96) Fecha de presentación y número de la solicitud europea: **27.10.2016 E 16797683 (6)**

(97) Fecha y número de publicación de la concesión europea: **20.02.2019 EP 3338143**

(54) Título: **Autentificación de artículo sustituible**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.06.2019

(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

DESCRIPCION

Autentificación de artículo sustituible

Antecedentes

Los dispositivos que utilizan artículos sustituibles incluyen dispositivos de impresión, que incluyen impresoras independientes, máquinas de copias, y dispositivos todo-en-uno (AIO) que pueden realizar múltiples funciones, tales como impresión, copia, escaneo y/o fax. Ejemplos de artículos sustituibles incluyen tinta, tóner, y/u otros tipos de colorante, incluyendo colorante bi-dimensional (2D). Otros artículos de sustitución ilustrativos, específicamente para dispositivos de impresión tri-dimensional (3D), incluyen agente de impresión 3D y material de formación de impresión 3D.

El documento US2011/0078449 describe un ejemplo, en el que un artículo sustituible puede limitar el número de veces que una clave de encriptación puede ser recuperada desde una memoria.

Breve descripción de los dibujos

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

La figura 2 es un diagrama de flujo de un método ejemplar que puede ejecutar un cartucho de sustancia de impresión u otro artículo sustituible para un dispositivo.

La figura 3 es un diagrama de flujo de un método ejemplar que puede ejecutar un cartucho de sustancia de impresión u otro artículo sustituible para un dispositivo para implementar una porción del método de la figura 2.

La figura 4 es un diagrama de flujo de otro método ejemplar que puede ejecutar un cartucho de sustancia de impresión u otro artículo sustituible para un dispositivo para implementar una porción del método de la figura 2.

La figura 5 es un diagrama de flujo de un método ejemplar que puede ejecutar un cartucho de sustancia de impresión u otro artículo sustituible para un dispositivo para implementar una porción del método de la figura 2.

Descripción detallada

Como se ha indicado en los antecedentes, los dispositivos que utilizan artículos sustituibles 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 se agota el suministro, el cartucho se puede sustituir con un cartucho que tiene un suministro nuevo de la sustancia de impresión en cuestión. Cartuchos que tienen diferentes tipos de sustancias de impresión también se pueden sustituir, cuando se desee. Como un ejemplo, un cartucho que tiene tinta de finalidad general se puede sustituir por un cartucho que tiene tinta de calidad fotográfica dentro de un dispositivo de impresión de chorro de tinta, cuando se desee.

Los fabricantes de dispositivos de impresión producen también típicamente o suministran de otra manera la sustancia de impresión utilizada en dispositivos de impresión. Desde la perspectiva del usuario final, la utilización de cartuchos de sustancias de impresión suministrados por el fabricante o aprobados por el fabricante puede facilitar la salida deseada por los dispositivos de impresión y/o inhibir daño a los dispositivos de impresión. Para el fabricante del 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 utiliza cartuchos de terceros. Una sustancia de impresión de terceros está fuera del control del OEM. Por ejemplo, podría proporcionar diferente salida de impresión o implicar un riesgo de acortamiento de la vida del dispositivo de impresión. En algunos casos, tales como impresores 3D, podría existir incluso un riesgo para la seguridad de un usuario cuando una sustancia de impresión es una sustancia de impresión no-aprobada. En ciertos casos, el uso de sustancia de impresión no-aprobada puede afectar a 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 cierto procedimiento, tal como, por ejemplo, informar al usuario final, tal como inmediatamente o poco después de la instalación.

Técnicas descritas aquí proporcionan un esquema de autentificación nuevo, innovador para un cartucho de sustancia de impresión para un dispositivo de impresión y, más generalmente, para un artículo sustituible para un dispositivo (servidor), en el que se puede instalar el artículo (es decir, más generalmente, el dispositivo al que se puede conectar el artículo). El cartucho de sustancia de impresión almacena un número de valores de autentificación, o palabras de paso. El cartucho incluye lógica (tal como circuitería similar a un procesador y memoria que almacena código que el procesador ejecuta, firmware, etc.) para responder satisfactoriamente a las solicitudes de estos valores de autentificación un número máximo predeterminado de veces.

Cuando se utiliza aquí, una respuesta a una solicitud de un valor de autentificación es una respuesta satisfactoria si la respuesta incluye el valor de autentificación solicitado. Es decir, que una respuesta a una solicitud de un valor de

autentificación es una respuesta satisfactoria si la respuesta satisface la solicitud incluyendo el valor de autentificación solicitado. Por lo tanto, una respuesta insatisfactoria a tal solicitud es una que no incluye el valor de autentificación solicitado.

El número máximo predeterminado de veces que el cartucho responderá satisfactoriamente a solicitudes del valor de autentificación puede considerarse como el primer número de solicitudes del valor de autentificación que recibe el cartucho. Esto es debido a que el cartucho cumplirá las respuestas del valor de autentificación a medida que las recibe hasta que se ha cumplido el número máximo de tales solicitudes. Una vez que se ha cumplido el número máximo de solicitudes del valor de autentificación, el cartucho no cumplirá ninguna otra solicitud del valor de autentificación.

El número máximo predeterminado de veces que el cartucho responderá satisfactoriamente a solicitudes del valor de autentificación puede ser específico de un valor de autentificación. Por ejemplo, su el cartucho almacena sesenta y cuatro valores de autentificación, cada valor de autentificación puede ser retornado el número máximo predeterminado de veces. El número máximo predeterminado de veces que el cartucho responderá satisfactoriamente a solicitudes del valor de autentificación puede ser específico del dispositivo de impresión que realiza la solicitud. Por ejemplo, el cartucho puede responder satisfactoriamente el número máximo predeterminado de veces a solicitudes desde un primer dispositivo de impresión en el que el cartucho ha sido insertado. Si el cartucho se retira de este dispositivo de impresión y se instala en un segundo dispositivo de impresión, el cartucho puede responder satisfactoriamente a solicitudes desde el segundo dispositivo de impresión también el número máximo predeterminado de veces.

El número máximo predeterminado de veces que el cartucho responderá satisfactoriamente a solicitudes del valor de autentificación puede ser específico de ambos de un valor de autentificación y del dispositivo de impresión que realiza la solicitud. Por ejemplo, si el cartucho almacena sesenta y cuatro valores de autentificación diferentes, cada valor de autentificación puede ser retornado el número máximo predeterminado de veces a un primer dispositivo de impresión, en el que ha sido insertado el cartucho. Si el cartucho es retirado de este dispositivo de impresión e instalado en un segundo dispositivo de impresión, el cartucho retornará cada valor de autentificación también el número máximo predeterminado de veces a este dispositivo de impresión.

El número máximo predeterminado de veces que el cartucho responderá satisfactoriamente a solicitudes del valor de autentificación puede no ser específico de un valor de autentificación o del dispositivo de impresión que hace la solicitud. En otras palabras, el cartucho puede responder satisfactoriamente justo a un número máximo predeterminado de veces independientemente del dispositivo de impresión que hace la solicitud, o el valor de autentificación que está siendo solicitado. Una vez que el cartucho ha retornado valores de autentificación en respuesta al número máximo predeterminado de veces, el cartucho no retornará ya una autentificación en respuesta a la siguiente solicitud, incluso si es para un valor de autentificación que no ha sido solicitado anteriormente e incluso si es desde un dispositivo de impresión que no ha solicitado anteriormente un valor de autentificación.

El cartucho de sustancia de impresión puede almacenar también valores Hash de los valores de autentificación, o palabras de paso. Los valores Hash proporciona una manera determinar si un valor de autentificación dado, que el cartucho ha proporcionado, es correcto o no. Un esquema de autentificación utilizando tal cartucho de sustancia de impresión puede incluir un dispositivo de impresión servidor que puede solicitar cuatro palabras de paso diferentes, o valores de autentificación, almacenados en el cartucho. Diferentes cartuchos de impresión pueden y probablemente solicitarán diferentes palabras de paso desde un cartucho dado. De manera similar, un dispositivo de impresión dado puede y probablemente solicitará diferentes palabras de paso desde cartuchos diferentes.

La figura 1 muestra un cartucho de sustancia de impresión 100 ejemplar para un dispositivo de impresión. El cartucho 100 incluye un suministro de sustancia de impresión 102. El cartucho 100 puede incluir cualquier volumen de sustancia de impresión, tal como varios mililitros de décimas de litros. Diferentes ejemplos de sustancia de impresión incluyen tinta para un dispositivo de impresión de chorro de tinta, o tóner líquido o en polvo para un dispositivo de impresión por láser. Tales tinta o tóner son ellos mismos ejemplos de colorante bi-dimensional (2D), que es colorante utilizado por un dispositivo de impresión adecuado para formar imágenes sobre medios tales como papel que se extienden mínimamente en todo caso en una tercera dimensión perpendicular a las dos dimensiones que definen el plano de la superficie de los medios sobre los que se han formado las imágenes. Otros ejemplos de sustancia de impresión incluyen agente de impresión tri-dimensional (3D) y material de formación de impresión 3D, que se utilizan por un dispositivo de impresión 3D adecuado para formar un objeto 3D que se puede retirar típicamente de cualquier sustrato sobre el que está construido el objeto. Ciertas sustancias de impresión, tales como tinta, pueden utilizarse para ambas impresiones 2D y 3D.

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

Como otro ejemplo, la lógica 104 puede ser o incluir un circuito integrado específico de la aplicación (ASIC) o una matriz de puertas programables en el campo (FPGA). Más generalmente, a este respecto, la lógica 104 puede ser implementada utilizado puertas lógicas. Como un tercer ejemplo, la lógica 104 puede ser implementada como cualquier combinación de un procesador, software almacenado dentro del procesador o en un medio separado del procesador, o puertas lógicas.

El cartucho de sustancia de impresión 100 incluye memoria no-volátil 106. La memoria 106 puede ser memoria de semiconductores. y es no-volátil por que cuando se retira la potencia desde el cartucho 100, la memoria 106 retiene todavía su contenido. La memoria 106 almacena palabras de paso 108, que se refieren aquí también como valores de autentificación. La memoria 106 puede almacenar valores Hash 110 de palabras de paso y que pueden corresponder individualmente a palabras de paso 108. La memoria 106 puede almacenar una clave criptográfica 112 a partir de la cual se pueden generar las palabras de paso 108.

La memoria 106 almacena un número de palabras de paso 108, que se refiere a un número total de palabras de paso 108. Las palabras de paso 108, o valores de autentificación, son almacenados por el cartucho 100 para que el cartucho 100 pueda probar a un dispositivo de impresión servidor que es auténtico. Establecido de otra manera, las palabras de paso 108 se utilizan para autentificar el cartucho 100 dentro del dispositivo de impresión. Las palabras de paso 108 pueden ser aseguradas de una manera criptográfica encriptada, de manera que las palabras de paso 108 son esencialmente irrecuperables desde el cartucho 100 fuera de los métodos descritos aquí. Cada una de las palabras de paso 108 puede ser una serie de bits, tal como 256 bits.

La memoria 106 puede almacenar un valor Hash 110 para cada palabra de paso 108. Los valores Hash 110 son almacenados por el cartucho 100, de manera que el cartucho 100 puede probar al dispositivo de impresión servidor que las palabras de paso 108 son correctas. Establecido de otra manera, los valores Hash 110 se utilizan para verificar las palabras de paso 108 proporcionadas por el cartucho 100 dentro del dispositivo de impresión. Los valores Hash 110 pueden no estar asegurados criptográficamente para que se pueden recuperar libremente desde el cartucho 100, pero pueden estar asegurados criptográficamente para que los valores Hash 110 no se puedan modificar. Los valores hash 110 pueden ser valores Hash 110 unidireccionales de las palabras de paso 108, lo que significa que una palabra de paso 108 no puede ser determinada justamente conociendo su valor Hash 110 correspondiente, incluso si se conoce la función Hash unidireccional utilizada para generar el valor Hash 110 a partir de la palabra de paso 108.

Los valores Hash 110 pueden ser proporcionados por el cartucho 100 en una implementación, de tal manera que un dispositivo servidos es capaz de validar los valores Hash 110 a medida que están siendo generados por una entidad (es decir, el fabricante o proveedor del cartucho 100) que en la que confía el dispositivo servidor. Como un ejemplo, los valores Hash 110 pueden estar firmados criptográficamente con una clave criptográfica privada antes de almacenarlos en el cartucho 100. El dispositivo servidor puede utilizar una clave criptográfica pública correspondiente para validar los valores Hash 110. La clara privada puede no estar almacenada en el cartucho 100, y no está disponible públicamente.

La lógica 104 permite la recuperación de las palabras de paso un número máximo predeterminado de veces. La lógica 104 puede permitir la recuperación de un número máximo predeterminado de las palabras de paso 108, menor que el número total de las palabras de paso 108 almacenadas en la memoria no-volátil 106. En tal implementación, la lógica 104 prohíbe la recuperación de cualquier palabra de paso 108 distinta del número máximo predeterminado de palabras de paso, incluso una vez, desde la memoria 106. Tal implementación se describe en la solicitud de patente en tramitación con la presente presentada el 16 de Junio de 2016, y con el número de solicitud de patente asignado PCT/US2016/38211.

La lógica 104 puede permitir la recuperación de las palabras de paso 108 un número máximo predeterminado de veces, independientemente de las palabras de paso 108 que se pregunten. Es decir, que la lógica 104 responde satisfactoriamente al primer número máximo predeterminado de solicitudes de las palabras de paso 108, independientemente de las palabras de paso 108 dentro de esas solicitudes, y no retorna palabras de paso 108 es respuesta a solicitudes recibidas posteriormente de las palabras de paso 108. El número máximo predeterminado de solicitudes de las palabras de paso 108, que la lógica 104 responderá satisfactoriamente puede ser inferior, igual o mayor que el número de las palabras de paso 108. Si el número máximo predeterminado de solicitudes es inferior al número de las palabras de paso 108, la lógica 104 nunca retornará una o más de las palabras de paso 108. Si el número máximo predeterminado de solicitudes es igual o mayor que el número de las palabras de paso 108, la lógica 104 puede retornar potencialmente todas las palabras de paso 108, pero dependiendo de las palabras de paso 108 solicitadas en el primer número máximo predeterminado de solicitudes, puede no retornar nunca una o más de las palabas de paso 108.

La lógica 104 puede permitir la recuperación de las palabras de paso 108 un número máximo predeterminado de veces, sobre una base por palabra de paso. Es decir, que la lógica 104 responde satisfactoriamente al primer número máximo predeterminado de solicitudes para cada palabra de paso 108. Por ejemplo, si existe sesenta y cuatro palabras de paso 108, la lógica 104 retornará la primera palabra de paso 108 el número máximo predeterminado de veces, la segunda palabra de paso 108 el número máximo predeterminado de veces y así sucesivamente.

La lógica 104 puede permitir la recuperación de las palabras de paso 108 un número máximo predeterminado de veces, independientemente del dispositivo de impresión servidor que realiza las solicitudes. Es decir, que la lógica 104 responde satisfactoriamente al primer número máximo predeterminado de solicitudes de las palabras de paso 108, independientemente del dispositivo de impresión servidor desde el que ha sido recibida cada una de tales solicitudes, y no retorna palabras de paso 108 en respuesta a solicitudes recibidas posteriormente de las palabras de paso 108. Por ejemplo, el número máximo predeterminado de veces que la lógica 104 retorna las palabras de paso 108 puede ser cien. Si la lógica 104 está instalada en un primer dispositivo de impresión desde el que se reciben cien solicitudes, la lógica 104 no responderá satisfactoriamente a ninguna solicitud más recibida desde este dispositivo de impresión. Además, si el cartucho 100 es retirado entonces desde el primer dispositivo de impresión y es instalado en otro segundo dispositivo de impresión servidor, la lógica 104 no responderá satisfactoriamente a ninguna solicitud recibida desde el segundo dispositivo de impresión.

La lógica 104 puede permitir la recuperación de las palabras de paso un número máximo predeterminado de veces sobre una base por dispositivo de impresión servidor. Es decir, que la lógica 104 responde satisfactoriamente al primer número máximo predeterminado de solicitudes, que recibe desde cada dispositivo de impresión. Por ejemplo, el número máximo predeterminado de veces, que la lógica 104 retorna las palabras de paso 108 puede ser cien. La lógica 104 puede instalarse en un primer dispositivo de impresión servidor desde el que se reciben cincuenta solicitudes y al que la lógica 104 responde satisfactoriamente. Si el cartucho 100 es retirado entonces desde el primer dispositivo de impresión e instalado en otro segundo dispositivo de impresión servidor, la lógica 104 responderá todavía satisfactoriamente a las primeras cien solicitudes recibidas desde el segundo dispositivo de impresión.

La lógica 104 puede permitir la recuperación de las palabras de paso 108 un número máximo predeterminado de veces, independientemente de las palabras de paso 108 que son solicitadas e independientemente del dispositivo de impresión servidor que realiza las solicitudes. Es decir, que no importa qué palabra de paso 108 ha sido solicitada en una solicitud y qué dispositivo de impresión servidor ha hecho la solicitud en cuanto a si la lógica 104 responderá o no satisfactoriamente a la solicitud. Una vez que la lógica 104 ha respondido satisfactoriamente al número máximo predeterminado de tales solicitudes, independientemente del dispositivo de impresión servidor que hace la siguiente solicitud o la palabra de paso 108 solicitada en esta solicitud, la lógica 104 no retornará la palabra de paso solicitada 108 al dispositivo de impresión que hace la solicitud.

La lógica 104 puede permitir la recuperación de las palabras de paso 108 un número máximo predeterminado de veces, sobre una base por dispositivo de impresión servidor y sobre una base por palabra de paso. La lógica 104 puede retornar cada palabra de paso 108 a cada dispositivo de impresión el número máximo predeterminado de veces. Una vez que un dispositivo de impresión servidor ha recibido una palabra de paso 108 dada el número máximo predeterminado de veces, el dispositivo de impresión puede recibir todavía otras palabras de paso 108 desde la lógica 104, y otro dispositivo de impresión servidor puede recibir todavía la palabra de paso dada.

La memoria no-volátil 106 utilizada para el almacenamiento de las palabras de paso 108 puede ser una memoria escrita una vez, de lectura limitada. Las palabras de paso 108 son escritas en la memoria 106 justamente una veza, tal como durante un proceso de fabricación seguro. Las palabras de paso 108 pueden ser borradas al menos funcionalmente una vez que se ha alcanzado el número máximo predeterminado de veces. Se pueden borrar completamente y de manera indeleble de la memoria 108 mediante la lógica 104, de tal manera que se considera imposible el "desborrado" o la recuperación de las palabras de paso 108 borradas. Las palabras de paso 108 en cuestión pueden borrarse funcionalmente por que estas palabras de paspo 108 permanecen almacenadas en la memoria 108, pero no irrecuperables. Por ejemplo, enlaces fundidos a las partes físicas de la memoria 108 donde las palabras de paso 108 en cuestión están almacenadas se pueden cortar, haciendo las palabras de paso 108 irrecuperables y de esta manera son borradas funcionalmente, aunque en realidad las palabras de paso 108 permanecen en la memoria.

La memoria 106 puede almacenar la clave criptográfica 112 en lugar de las palabras de paso 108 cuando el cartucho 100 es fabricado. En esta implementación, antes del primer uso del cartucho 100, no se pueden almacenar palabras de paso 108 en el cartucho 100. En su lugar, cuando se solicita una palabra de paso 108, el cartucho 100 genera la palabra de paso 108 “al vuelo”. Una vez que la lógica 104 ha respondido satisfactoriamente al número máximo predeterminado de solicitudes, la clave criptográfica 112 puede ser borrada al menos funcionalmente, de la manera descrita en el párrafo anterior.

La figura 2 muestra un método ejemplar 200 que puede realizar un artículo sustituible para un dispositivo, tal como el cartucho de sustancia de impresión 100 para un dispositivo de impresión. El método 200 puede implementarse como código legible por ordenador en un medio de almacenamiento 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 artículo sustituible realiza el método 200 una vez que ha sido instalado en un dispositivo servidor.

El artículo sustituible recibe una solicitud desde el dispositivo servidor para un valor de autentificación particular de un número de valores de autentificación que el artículo puede almacenar (202). La solicitud puede estar firmada con una clave criptográfica digital, o puede ser autentificada de otra manera. El artículo sustituible determina si se ha cumplido ya o no un número máximo predeterminado de solicitudes de valores de autentificación (204). El número

máximo predeterminado de solicitudes, a las que el artículo sustituible responderá satisfactoriamente puede ser sobre una base por valor de autentificación y/o una base por dispositivo servidor, o sobre ni una base por valor de autentificación ni una base por dispositivo servidor.

Si el número máximo predeterminado de solicitudes ha sido cumplido (206), entonces el artículo sustituible no enviará el valor de autentificación solicitado al dispositivo servidor, en el que está instalado (208) el artículo. Sin embargo, si el artículo sustituible no ha respondido todavía satisfactoriamente al número máximo predeterminado de solicitudes, entonces el artículo envía el valor de autentificación solicitado al dispositivo servidor (210). Por ejemplo, el artículo sustituible puede recuperar el valor de autentificación solicitado desde una tabla de los valores de autentificación almacenada en memoria no-volátil del artículo sustituible. Como otro ejemplo, el artículo sustituible puede recuperar un valor semilla almacenado dentro de memoria no-volátil del artículo sustituible (diferente del que puede haber firmado la solicitud recibida) y generar el valor de autentificación solicitado a partir de la clave criptográfica.

El artículo sustituible puede determinar de nuevo si el artículo ha respondido ahora satisfactoriamente al número máximo de solicitudes (212), incluyendo la solicitud recibida en la parte 202 que ha sido cumplida. Si el número máximo predeterminado de solicitudes ha sido cumplido (214) ahora, entonces el artículo sustituible puede borrar al menos funcionalmente los valores de autentificación que almacena (216). Si el número máximo predeterminado de solicitudes es sobre una base por valor de autentificación y no sobre una base por dispositivo servidor, entonces se borra justamente el valor de autentificación que ha sido enviado en la parte 210, y no se borran otros valores de autentificación. Si el número máximo predeterminado de solicitudes es sobre una base por dispositivo servidor, independientemente de si este número es sobre una base por valor de autentificación o no, entonces no se puede borrar ningún valor de autentificación, debido a que otros dispositivos servidores pueden solicitar el mismo (u otro) valor de autentificación.

En una implementación, en la que el artículo sustituible genera valores de autentificación a partir de una clave criptográfica, el borrado de los valores de autentificación en la parte 212 significa o incluye el borrado de esta clave. Si el número máximo predeterminado de solicitudes es sobre una base por valor de autentificación y no sobre una base por dispositivo servidor, entonces la clave criptográfica no ocurre hasta que se ha recibido el número máximo predeterminado de solicitudes para todos los valores de autentificación. Si el número máximo predeterminado de solicitudes es sobre una base por dispositivo servidor, independientemente de si este número es o no sobre una base por valor de autentificación, entonces no se puede borrar la clave criptográfica, debido a que valores de autentificación pueden haber sido generados para otros dispositivos servidores.

En una implementación, el valor de autentificación no puede ser enviado hasta que se determine si se realizará o no el borrado – y, además, si se determina que se realizará el borrado del valor de autentificación, el valor de autentificación puede ser borrado desde la memoria no-volátil hasta antes de enviar el valor de autentificación. Es decir, que después de que el artículo sustituible determina que no se ha cumplido todavía el número máximo predeterminado de solicitudes en la parte 206, el artículo sustituible determina entonces si el número máximo predeterminado se cumplirá con el cumplimiento de la solicitud recibida en la parte 202. Si el número máximo predeterminado de solicitudes no se cumplirá todavía con el cumplimiento de la solicitud recibida, entonces el artículo sustituible envía el valor de autentificación y prosigue. Si el número máximo predeterminado de solicitudes se cumplirá con el cumplimiento de la solicitud recibida, entonces el artículo sustituible copia el valor de autentificación solicitado desde memoria no-volátil antes de borrar al menos este valor de autentificación desde memoria no-volátil y entonces envía el valor de autentificación copiado al dispositivo servidor.

Desde las partes 208 y 216, y desde la parte 214 cuando no se ha cumplido todavía el número máximo de solicitudes, o como un punto de entrada al método 200, el artículo sustituible puede recibir desde el dispositivo servidor una solicitud de uno o más valores Hash que corresponden a uno o más valores de autentificación (218). Por ejemplo, el artículo sustituible puede recibir una solicitud de todos los valores Hash que corresponden a todos los valores de autentificación, justamente de uno de los valores Hash que corresponden justamente a uno de los valores de autentificación, y así sucesivamente. El artículo sustituible puede recibir una solicitud de uno p más valores Hash, incluso después de que los valores de autentificación han sido borrados en la parte 216. Es decir, que el artículo sustituible no puede borrar los valores Hash para los valores de autentificación que borra, por ejemplo, la parte 218 puede considerarse como un punto de entrada del método 200 por que la solicitud de los valores Hash puede recibirse antes de la recepción de una solicitud de un valor de autentificación.

La figura 3 muestra un método ejemplar 300 que es un ejemplo de una implementación particular de las partes 202 a 216 del método 200. Las partes numeradas idénticamente en las figuras 2 y 3 se realizan en el método 300 al menos sustancialmente como se ha descrito anteriormente con relación al método 200. Los números entre paréntesis indican que una parte dada del método 300 está implementando una parte correspondiente del método 200. Es decir, que Y(X) en la figura 3 significa que la parte Y del método 300 está implementando la parte X del método 200.

El artículo sustituible recibe una solicitud de un valor de autentificación desde el dispositivo servidor en el que está instalado (202). El artículo sustituible mantiene un contador del número de solicitudes del valor de autentificación que se han cumplido. Es decir, que el artículo sustituible mantiene un contador del número de solicitudes del valor

de autentificación al que ha respondido satisfactoriamente. El contador puede ser un contador sólo de incremento, que se puede incrementar y no disminuir. El contador está almacenado en memoria no-volátil, tal como la memoria no-volátil 106, y se puede asegurar.

El artículo sustituible determina si el contador es igual al número máximo predeterminado de solicitudes, al que el artículo ha respondido satisfactoriamente para cumplir las solicitudes (302). Puede existir un contador sobre una base por valor de autentificación y/o sobre una base por dispositivo servidor, o ni una base por valor de autentificación ni una base por dispositivo servidor. Si el contador es igual a este número máximo predeterminado (304), entonces el artículo sustituible rechaza enviar el valor de autentificación (208) solicitado.

Sin embargo, si el contador no es igual al número máximo predeterminado de solicitudes a los que el artículo sustituible ha respondido satisfactoriamente (304), entonces el artículo sustituible envía el valor de autentificación al dispositivo servidor en respuesta y para cumplir la solicitud (210). El artículo sustituible incrementa el contador (306), y determina si el contador es ahora igual al número máximo predeterminado de solicitudes que el artículo cumplirá (308). Si el contador no es todavía igual a este número máximo (310), entonces se termina (312) el método 300. Sin embargo, si el contador es ahora igual a este número (310), entonces el artículo sustituible puede borrar los valores de autentificación (216).

En una implementación diferente, el contador se incrementa antes de enviar el valor de autentificación. Es decir que, en esta implementación, se determina si el número máximo de autentificaciones habrá sido enviado ahora con la emisión de un valor de autentificación, y si es así, entonces se incrementa el contador y después de que se ha incrementado el contador, se envía el valor de autentificación. El borrado de los valores de autentificación, en su caso, puede ocurrir en esta implementación antes de enviar el valor de autentificación en cuestión. Más generalmente, cualquier acción que se realice debido al envío del último valor de autentificación único que será proporcionado por el artículo sustituible, puede realizarse antes de enviar este último valor de autentificación único. Hay que indicar a este respecto que, más generalmente todavía, cualquier acción de este tipo que se realice en combinación con la emisión de un valor de autentificación (y no el último valor de autentificación) puede realizarse antes de que se envíe realmente el valor de autentificación.

La figura 4 muestra un método ejemplar 400 que es otro ejemplo de una implementación particular de las partes 202 a 216 del método 200. Las partes numeradas idénticamente en las figuras 2 y 4 se realizan en el método 400 al menos sustancialmente como se ha descrito anteriormente con relación al método 200. Los números entre paréntesis indican que una parte dada del método 400 está implementando una parte correspondiente del método 200. Es decir, que Y(X) en la figura 4 significa que la parte Y del método 400 está implementando la parte X del método 200.

El artículo sustituible recibe una solicitud de un valor de autentificación desde el dispositivo servidor, en el que está instalado (202). El artículo sustituible mantiene una etiqueta que corresponde a si el número máximo predeterminado de solicitudes de valores de autentificación ha sido cumplido por el artículo sustituible respondiendo satisfactoriamente a ellas. La etiqueta puede ser una etiqueta sólo-ajustable, que se puede colocar, pero que no se puede borrar. La etiqueta está almacenada en memoria no-volátil, tal como la memoria no-volátil 106, y se puede asegurar.

El artículo sustituible determina si la etiqueta ha sido colocada (402). Puede existir una etiqueta sobre una base por valor de autentificación y/o sobre una base por dispositivo servidor, o ni sobre una base por valor de autentificación ni sobre una base por dispositivo servidor. Si la etiqueta ha sido colocada (404), entonces el artículo sustituible rechaza enviar el valor de autentificación solicitado (208).

Sin embargo, s la etiqueta no ha sido colocada (404), entonces el artículo sustituible envía el valor de autentificación al dispositivo servidor en respuesta y para cumplir la solicitud (210). El artículo sustituible determina si ahora se ha cumplido (212) el número máximo de solicitudes al que responderá satisfactoriamente. Si el artículo sustituible no ha respondido todavía satisfactoriamente al número máximo de solicitudes del valor de autentificación (214), entonces el método 400 se termina (404). En cambio, si el artículo sustituible ha cumplido el número máximo de tales solicitudes (214), entonces el artículo sustituible coloca la etiqueta (408) y puede borrar los valores de autentificación (216).

En una implementación diferente, la etiqueta se coloca antes de la emisión del valor de autentificación. Es decir, que en esta implementación, se determina si el número máximo de autentificaciones habrá sido enviado ahora con la emisión de un valor de autentificación y si es así, entonces se coloca la etiqueta, y después de que la etiqueta ha sido colocada, se envía el valor de autentificación. El borrado de los valores de autentificación, en sui caso, puede ocurrir en esta implementación antes de enviar el valor de autentificación en cuestión. Más generalmente, cualquier acción que se realice debido a la emisión del último valor de autentificación único, que sea proporcionada por el artículo sustituible, puede realizarse antes de la emisión de este último valor de autentificación único. Hay que indicar a este respecto que, más generalmente todavía, cualquier acción de este tipo que se realice en combinación con la emisión de un valor de autentificación (y no el último valor de autentificación) se puede realizar antes de que el valor de autentificación sea enviado realmente.

La figura 5 muestra un método ejemplar 500 que es un ejemplo de una implementación de la parte 210 del método 200. Es decir, que en lugar enviar el valor de autentificación automáticamente en la parte 210 del método 200, el artículo sustituible realiza el método 500. El artículo sustituible determina si ha enviado previamente el valor de autentificación, que ha sido solicitado por un dispositivo servidor en la solicitud que el artículo recibió desde el dispositivo, a cualquier dispositivo servidor (502), incluyendo el dispositivo servidor, en el que el artículo está actualmente instalado, así como cualquier otro dispositivo servidor. Si el artículo sustituible ha enviado previamente el valor de autentificación (504) solicitado, el artículo retorna el valor solicitado al dispositivo servidor (506).

Sin embargo, si el artículo sustituible no ha enviado previamente el valor de autentificación solicitado (504), entonces el artículo determina si ya ha enviado el número máximo de valores de autentificación únicos (508). Por ejemplo, de sesenta y cuatro valores de autentificación que el artículo sustituible puede almacenar, el artículo no puede enviar más de sesenta de estos valores. Si el artículo de sustitución ya ha enviado el número máximo de valores de autentificación únicos (510), entonces no envía el valor de autentificación que ha solicitado (512) el dispositivo servidor, en el que el artículo está instalado. El método 500 se termina con el artículo sustituible no enviando el valor de autentificación solicitado, incluso si no se ha alcanzado todavía el número máximo de solicitudes que el artículo sustituible responderá satisfactoriamente.

En cambio, si el artículo sustituible no ha enviado todavía el número máximo de valores de autentificación únicos, entonces el artículo envía el valor de autentificación solicitado al dispositivo servidor (514). El artículo sustituible puede determinar entonces de nuevo si se ha enviado o no (516) el número máximo de valores de autentificación, incluyendo el valor de autentificación que el artículo acaba de enviar a la parte 514. Por ejemplo si se permite al artículo que envíe justamente dieciséis de los sesenta y cuatro valores de autentificación, si han sido enviados quince valores antes de la realización de la parte 514, entonces reenvía un décimo sexto valor de autentificación diferente en la parte 514, de tal manera que ahora se ha enviado el número máximo de dieciséis valores de autentificación diferentes.

Si ahora se ha enviado (518) el número máximo de valores de autentificación únicos, entonces el artículo sustituible puede borrar al menos funcionalmente los valores de autentificación que almacena y que no han sido enviados (520). Como tal, en el presente ejemplo, una vez que han sido enviados dieciséis valores de autentificación diferentes, se borran los otros cincuenta y ocho valores de autentificación. Hay que indicar que cada vez que se ejecuta el método 500 de la figura 5, entonces el artículo sustituible puede enviar cualquier valor de autentificación que ha enviado previamente hasta el número máximo permitido de veces que el artículo responderá satisfactoriamente a solicitudes de valores de autentificación. Además, cada vez que se ejecute el método 500, el artículo sustituible puede enviar cualquier valor de autentificación que no ha enviado anteriormente, mientas no se alcance todavía el número máximo de valores de autentificación diferentes que enviará el artículo, hasta el número máximo permitido de veces que el artículo responderá satisfactoriamente a solicitudes de valores de autentificación. Desde las partes 506 y 520, y desde la parte 518 cuando no se ha alcanzado todavía el número máximo de valores de autentificación únicos enviados, el método 500 pasa a la parte 212 del método 200 de la figura 2 (524).

Las diferentes implementaciones de las partes del método 200 que han sido descritas en relación a los métodos 300, 400 y 500 se pueden combinar o modificar de diferentes maneras. Por ejemplo, el contador del método 300 se puede utilizar en combinación con la etiqueta del método 400. El método 500 se puede utilizar en combinación con el método 300 y/o también con el método 400.

Las técnicas descritas aquí pueden mejorar o proporcionar otro esquema para seguridad criptográfica de un artículo sustituible para un dispositivo, tal como un cartucho de suministro de tinta para un dispositivo de impresión. Un artículo sustituible responde satisfactoriamente a un número máximo predeterminado de solicitudes de valores de autentificación. Una vez que se ha recibido el número máximo predeterminado de solicitudes de autentificación, las solicitudes recibidas adicionalmente no serán satisfechas, incluso si permanecen almacenadas en el artículo sustituible. El número máximo predeterminado de solicitudes, a las que el artículo sustituible responderá satisfactoriamente puede ser sobre una base por valor de autentificación y/o sobre una base por dispositivo servidor, ni sobre una base por valor de autentificación ni sobre una base por dispositivo servidor.

REIVINDICACIONES

1. Un medio de almacenamiento de datos no-volátil legible por ordenador, que almacena código ejecutable por ordenador ejecutable por un artículo sustituible (100) para realizar un método, caracterizado por que el método comprende:

en respuesta a la recepción de una solicitud de un valor de autentificación particular de una pluralidad de valores de autentificación del artículo sustituible (100) desde un dispositivo servidor, al que ha sido conectado el artículo sustituible, determinar si el artículo sustituible ha respondido ya satisfactoriamente a solicitudes del valor de autentificación un número máximo permitido de veces;

en respuesta a la determinación de que el artículo sustituible (100) ya ha respondido satisfactoriamente a solicitudes del valor de autentificación el número máximo permitido de veces, rechazar enviar el valor de autentificación al dispositivo servidor; y

en respuesta a la determinación de que el artículo sustituible (100) no ha respondido ya todavía satisfactoriamente a solicitudes del valor de autentificación el número máximo permitido de veces, enviar el valor de autentificación solicitado al dispositivo servidor, en donde el dispositivo servidor es un dispositivo de impresión, y el artículo sustituible (100) es un cartucho de sustancia de impresión para el dispositivo de impresión.

2. El medio de almacenamiento de datos no-volátil legible por ordenador de la reivindicación 1, en donde la determinación de si el artículo sustituible (100) ha respondido o no ya satisfactoriamente a solicitudes del valor de autentificación el número máximo permitido de veces comprende: determinar si el artículo sustituible (100) ha respondido o no ya satisfactoriamente a solicitudes del valor de autentificación el número máximo permitido de veces independientemente de qué valores de autentificación han sido solicitados en las solicitudes del valor de autentificación.

3. El medio de almacenamiento de datos no-volátil legible por ordenador de la reivindicación 1, en donde la determinación de si el artículo sustituible (100) ha respondido o no ya satisfactoriamente a solicitudes del valor de autentificación el número máximo permitido de veces comprende: determinar si el artículo sustituible (100) ha respondido o no ya satisfactoriamente a solicitudes del valor de autentificación para el valor de autentificación solicitado el número máximo permitido de veces.

4. El medio de almacenamiento de datos no-volátil legible por ordenador de la reivindicación 1, en donde la determinación de si el artículo sustituible (100) ha respondido o no ya satisfactoriamente a solicitudes del valor de autentificación el número máximo permitido de veces comprende: determinar si el artículo sustituible (100) ha respondido o no ya satisfactoriamente a solicitudes del valor de autentificación el número máximo permitido de veces independientemente de qué dispositivos servidores enviaron las solicitudes del valor de autentificación.

5. El medio de almacenamiento de datos no-volátil legible por ordenador de la reivindicación 1, en donde la determinación de si el artículo sustituible (100) ha respondido o no ya satisfactoriamente a solicitudes del valor de autentificación el número máximo permitido de veces comprende: determinar si el artículo sustituible ha respondido o no ya satisfactoriamente a solicitudes del valor de autentificación desde el dispositivo servidor el número máximo permitido de veces.

6.- El medio de almacenamiento de datos no-volátil legible por ordenador de la reivindicación 1, en donde la determinación de si el artículo sustituible (100) ha respondido o no ya satisfactoriamente a solicitudes del valor de autentificación el número máximo permitido de veces comprende: determinar si el artículo sustituible (100) ha respondido o no ya satisfactoriamente a solicitudes del valor de autentificación el número máximo permitido de veces independientemente de qué valores de autentificación fueron solicitados en las solicitudes de valores de autentificación e independientemente de qué dispositivos servidores enviaron las solicitudes del valor de autentificación.

7. El medio de almacenamiento de datos no-volátil legible por ordenador de la reivindicación 1, en donde la determinación de si el artículo sustituible (100) ha respondido o no ya satisfactoriamente a solicitudes del valor de autentificación el número máximo permitido de veces comprende: determinar si el artículo sustituible (100) ha respondido o no ya satisfactoriamente a solicitudes del valor de autentificación para el valor de autentificación solicitado desde el dispositivo servidor el número máximo permitido de veces.

8. El medio de almacenamiento de datos no-volátil legible por ordenador de la reivindicación 1, en donde la determinación de si el artículo sustituible (100) ha respondido o no ya satisfactoriamente a solicitudes del valor de autentificación el número máximo permitido de veces comprende:

determinar si un contador de un número de veces que el artículo sustituible (100) ha respondido ya satisfactoriamente a solicitudes del valor de autentificación es igual al número máximo permitido de veces, y

en donde el método comprende. además, en respuesta a la determinación de que el artículo sustituible no ha respondido todavía a solicitudes del valor de autentificación el número máximo permitido de veces,

incrementar el contador.

9. El medio de almacenamiento de datos no-volátil legible por ordenador de la reivindicación 1, en donde la determinación de si el artículo sustituible (100) ha respondido o no ya satisfactoriamente a solicitudes del valor de autentificación el número máximo permitido de veces comprende:

determinar si ha sido enviada una etiqueta que corresponde al artículo sustituible (100) que ya ha respondido a solicitudes del valor de autentificación el número máximo permitido de veces, y en donde el método comprende, además, en respuesta a la determinación de que el artículo sustituible (100) no ha respondido ya todavía a solicitudes del valor de autentificación el número máximo permitido de veces:

determinar si el artículo sustituible (100) ha respondido ahora o habrá respondido ahora a solicitudes del valor de autentificación el número máximo permitido de veces;

en respuesta a la determinación de que el artículo sustituible (100) ha respondido ahora o habrá respondido ahora a solicitudes del valor de autentificación el número máximo permitido de veces;

colocar la etiqueta.

10. El medio de almacenamiento de datos no-volátil legible por ordenador de la reivindicación 1, en donde la emisión del valor de autentificación comprende recuperar el valor de autentificación solicitado desde una tabla de los valores de autentificación dentro del artículo sustituible (100), y en donde el método comprende, además, en respuesta a la determinación de que el artículo sustituible no ha respondido ya todavía satisfactoriamente a solicitudes del valor de autentificación el número máximo permitido de veces,

determinar si el artículo sustituible (100) ha respondido ahora o habrá respondido ahora a solicitudes del valor de autentificación el número máximo permitido de veces;

en respuesta a la determinación de que el artículo sustituible (100) ha respondido ahora o habrá respondido ahora a solicitudes del valor de autentificación el número máximo permitido de veces, borrar funcionalmente los valores de autentificación desde el artículo sustituible.

11. El medio de almacenamiento de datos no-volátil legible por ordenador de la reivindicación 1, en donde la emisión del valor de autentificación comprende generar el valor de autentificación solicitado a partir de una clave criptográfica almacenada dentro del elemento sustituible (100);

y en donde el método comprende, además, en respuesta a la determinación de que el artículo sustituible (100) no ha respondido ya todavía a solicitudes del valor de autentificación el número máximo permitido de veces:

determinar si el si el artículo sustituible (100) ha respondido ahora o habrá respondido ahora a solicitudes del valor de autentificación el número máximo permitido de veces;

en respuesta a la determinación de que el artículo sustituible (100) ha respondido ahora o habrá respondido ahora a solicitudes del valor de autentificación el número máximo permitido de veces, borrar funcionalmente la criptográfica desde el artículo sustituible.

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

recibir una segunda solicitud desde el dispositivo servidor, para un valor Hash unidireccional (110) del valor de autentificación; y

enviar el valor Hash unidireccional (110) al dispositivo servidor,

en donde la primera solicitud es recibida antes o de que de recibir la segunda solicitud.

13. El medio de almacenamiento de datos no-volátil legible por ordenador de la reivindicación 1, en donde la emisión del valor de autentificación solicitado al dispositivo servidor comprende:

determinar si el artículo sustituible (100) ha enviado previamente el valor de autentificación solicitado;

en respuesta a la determinación de que el valor de autentificación solicitado ha sido enviado previamente, proceder a enviar el valor de autentificación solicitado al dispositivo servidor;

en respuesta a la determinación de que el valor de autentificación solicitado no ha sido enviado previamente, determinar si el artículo sustituible (100) ha enviado o no previamente un número máximo de valores de autentificación únicos de los valores de autentificación, siendo el número máximo de valores de autentificación únicos menor que un número total de los valores de autentificación:

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

en respuesta a la determinación de que ha sido enviado el número máximo de valores de autentificación únicos, rechazar el envío del valor de autentificación solicitado al dispositivo servidor.

14. 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 que almacena (106) una pluralidad de palabreas de paso (108); y

lógica (104) para responder satisfactoriamente a un número máximo permitido de solicitudes de las palabras de paso para autentificar el cartucho de sustancia de impresión dentro del dispositivo de impresión, en donde las solicitudes comprenden solicitudes de una palabra de paso particular de la pluralidad de palabras de paso (108).

15. El cartucho de sustancia de impresión de la reivindicación 14, en donde la memoria no-volátil (106) almacena las palabras de paso (108), en donde la lógica (104) sirve, además, para borrar funcionalmente las palabras de paso (108) después de que ha sido recibido el número máximo permitido de solicitudes.

16. El cartucho de sustancia de impresión de la reivindicación 14, en donde la lógica (104) sirve, además, para; responder al número máximo permitido de solicitudes de un número máximo predeterminado de las palabras de paso (108) menor que un número total de las palabras de paso.

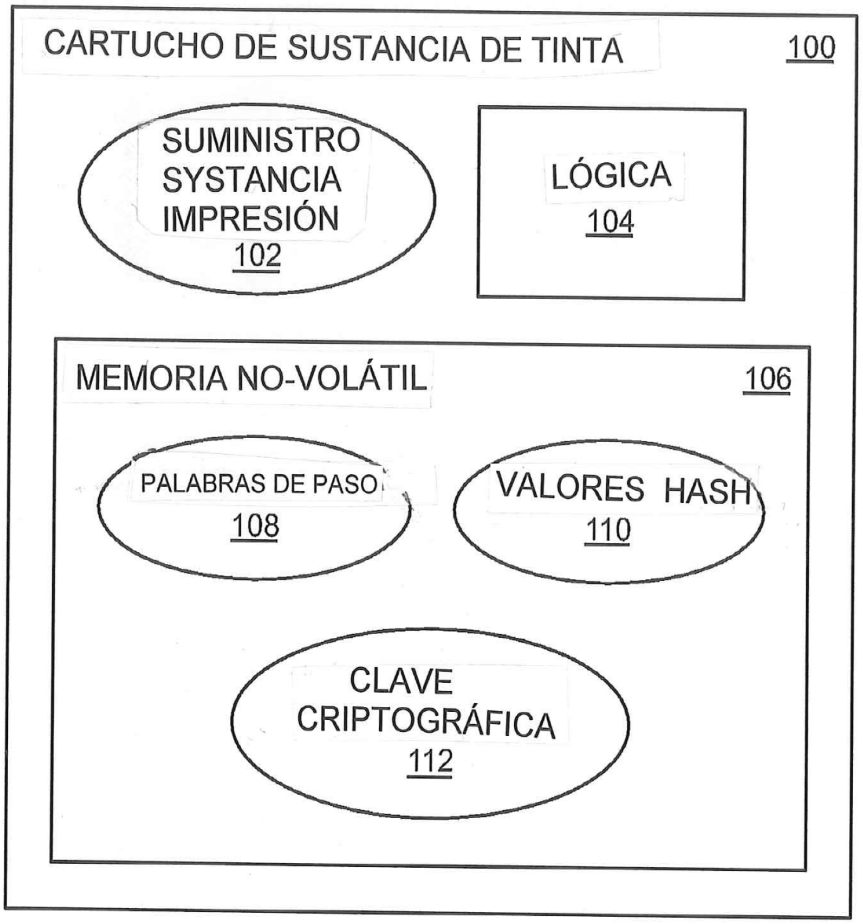
17. El cartucho de sustancia de impresión de la reivindicación 14, que comprende, además:

una memoria no-volátil que almacena una pluralidad de valores Hash (110) de las palabras de paso.

en donde la lógica (104) sirve para responder a solicitudes de los valores Hash (110) de las palabras de paso.

18.- El cartucho de sustancia de impresión de la reivindicación 14, en donde la sustancia de impresión es una o más de tinta, tóner, colorante bi-dimensional (2D), agente de impresión tri-dimensional (3D), y material de formación de impresión 3D.

FIG 1


CARTUCHO DE SUSTANCIA DE TINTA
100
SUMINISTRO SYSTANCIA IMPRESIÓN
102
LÓGICA
104
MEMORIA NO-VOLÁTIL
106
PALABRAS DE PASO
108
VALORES HASH
110
CLAVE CRIPTOGRÁFICA
112

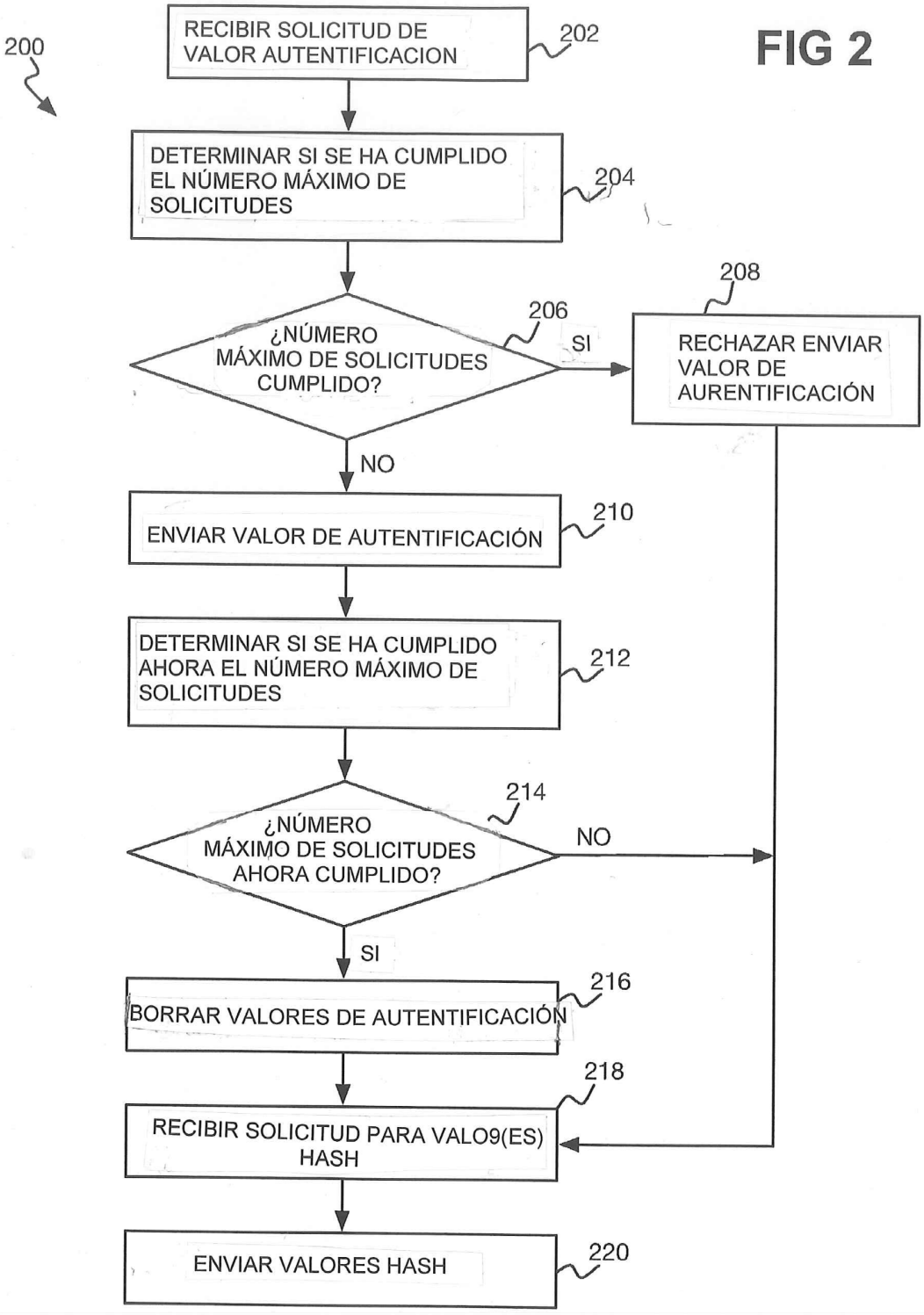

200
RECIBIR SOLICITUD DE VALOR AUTENTIFICACION
202
DETERMINAR SI SE HA CUMPLIDO EL NÚMERO MÁXIMO DE SOLICITUDES
204
¿NÚMERO MÁXIMO DE SOLICITUDES CUMPLIDO?
206
SI
208
RECHAZAR ENVIAR VALOR DE AURENTIFICACIÓN
NO
ENVIAR VALOR DE AUTENTIFICACIÓN
210
DETERMINAR SI SE HA CUMPLIDO AHORA EL NÚMERO MÁXIMO DE SOLICITUDES
212
¿NÚMERO MÁXIMO DE SOLICITUDES AHORA CUMPLIDO?
214
NO
SI
BORRAR VALORES DE AUTENTIFICACIÓN
216
RECIBIR SOLICITUD PARA VALO9(ES) HASH
218
ENVIAR VALORES HASH
220

FIG 2

FIG 3

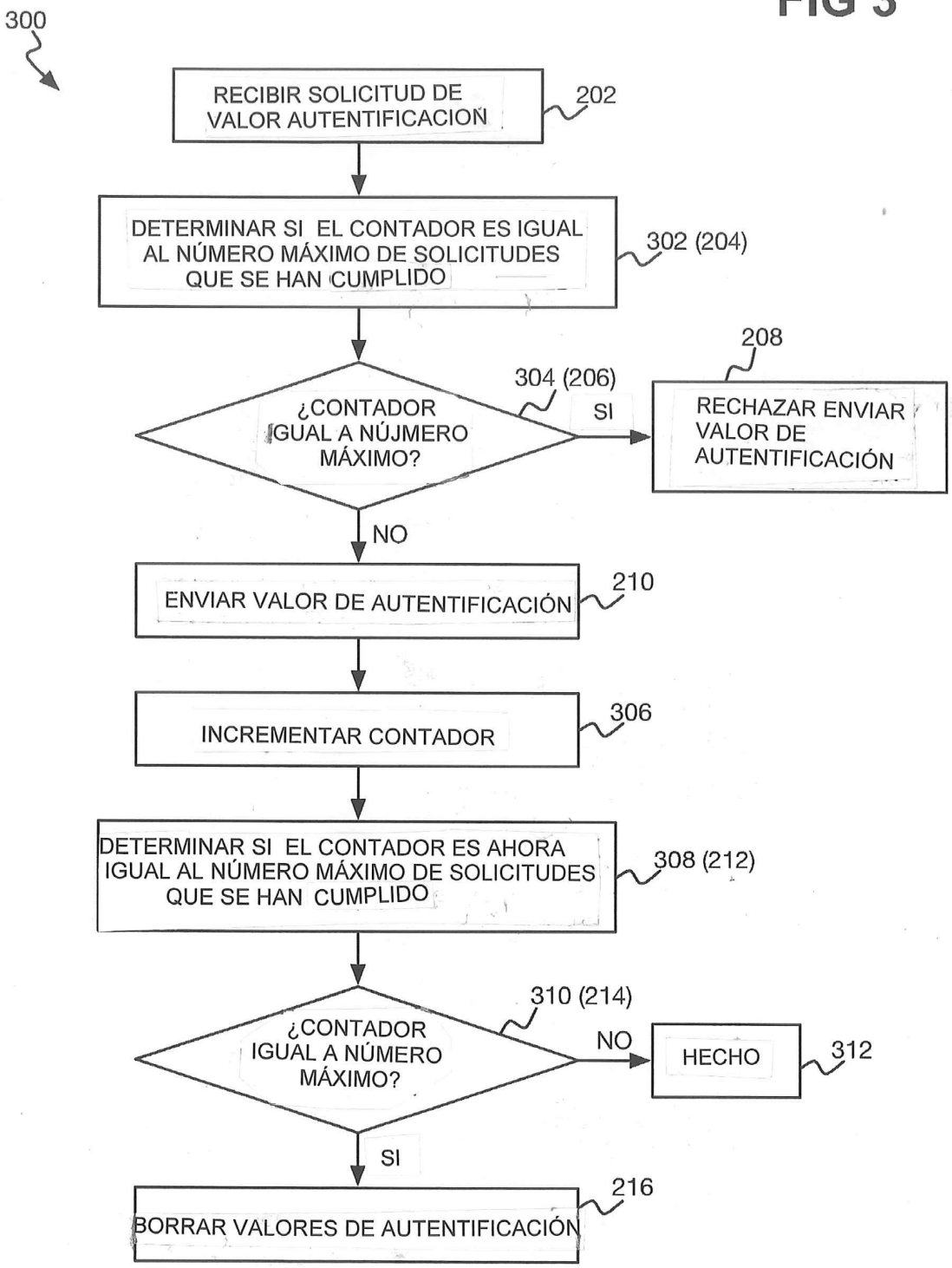

300
RECIBIR SOLICITUD DE VALOR AUTENTIFICACION
202
DETERMINAR SI EL CONTADOR ES IGUAL AL NÚMERO MÁXIMO DE SOLICITUDES QUE SE HAN CUMPLIDO
302 (204)
¿CONTADOR IGUAL A NÚJMERO MÁXIMO?
304 (206)
SI
208
RECHAZAR ENVIAR VALOR DE AUTENTIFICACIÓN
NO
ENVIAR VALOR DE AUTENTIFICACIÓN
210
INCREMENTAR CONTADOR
306
DETERMINAR SI EL CONTADOR ES AHORA IGUAL AL NÚMERO MÁXIMO DE SOLICITUDES QUE SE HAN CUMPLIDO
308 (212)
¿CONTADOR IGUAL A NÚMERO MÁXIMO?
310 (214)
NO
HECHO
312
SI
BORRAR VALORES DE AUTENTIFICACIÓN
216

FIG 4

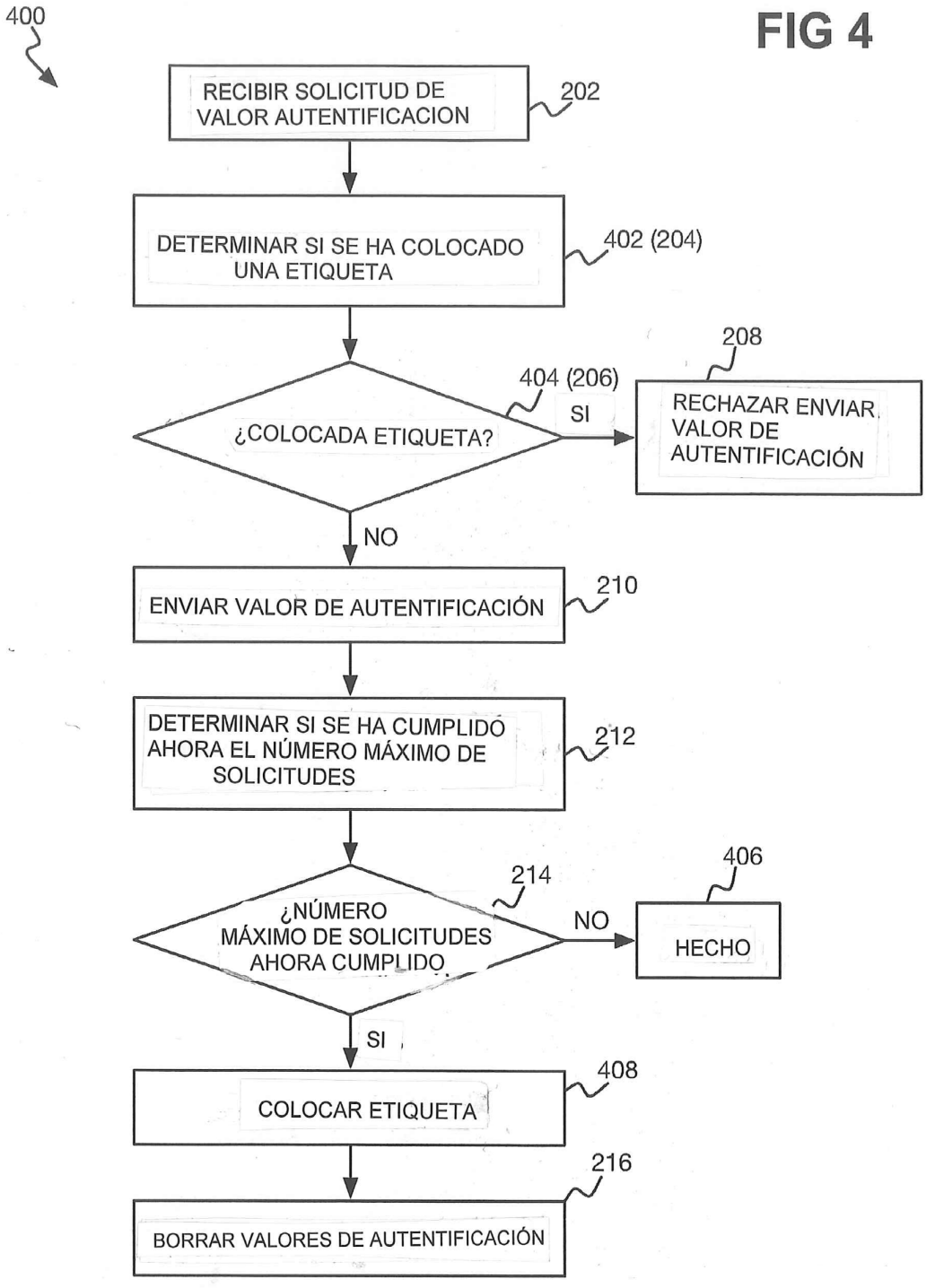
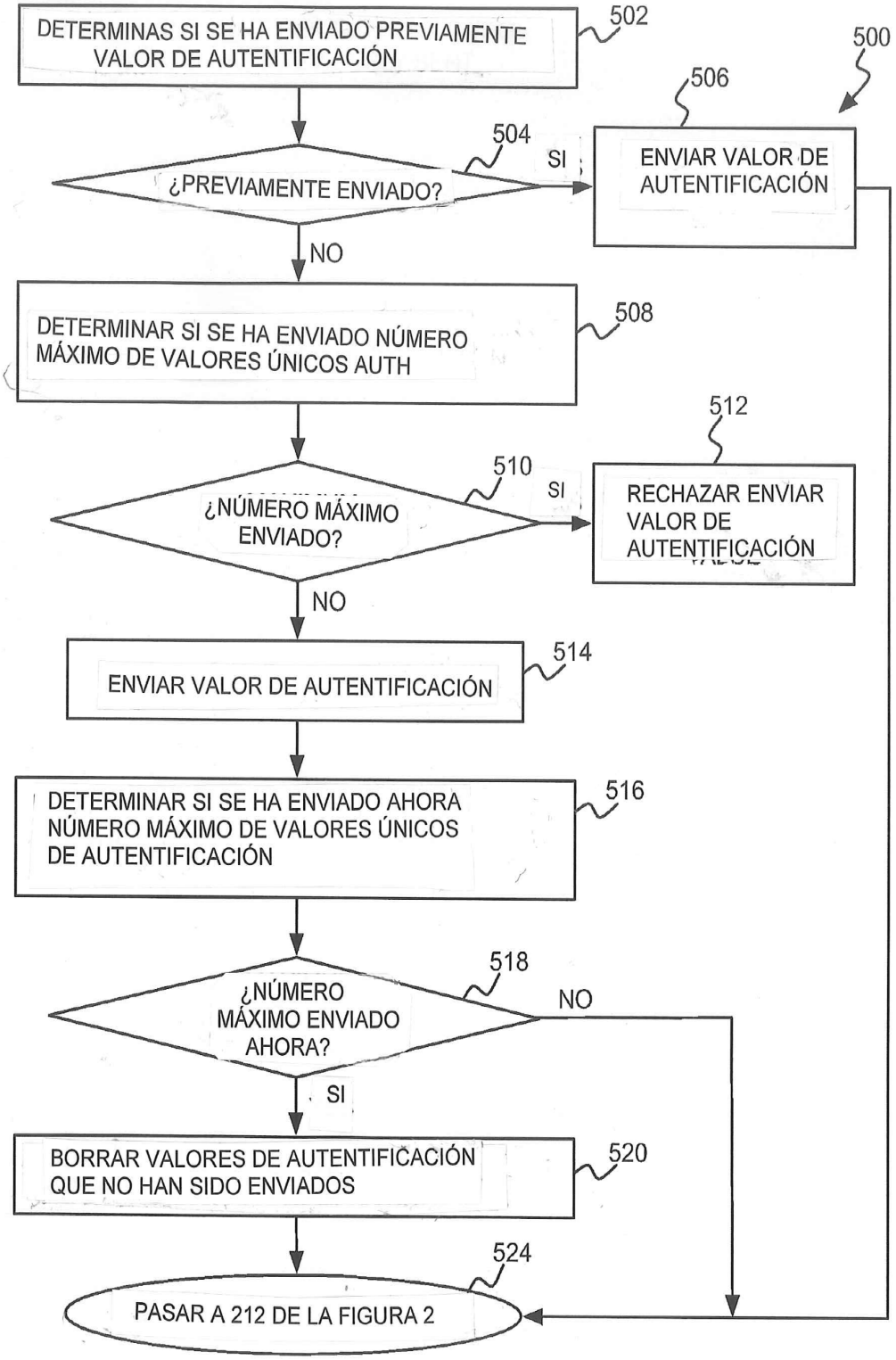

400
RECIBIR SOLICITUD DE VALOR AUTENTIFICACION
202
DETERMINAR SI SE HA COLOCADO UNA ETIQUETA
402 (204)
¿COLOCADA ETIQUETA?
404 (206)
SI
208
RECHAZAR ENVIAR VALOR DE AUTENTIFICACIÓN
NO
ENVIAR VALOR DE AUTENTIFICACIÓN
210
DETERMINAR SI SE HA CUMPLIDO AHORA EL NÚMERO MÁXIMO DE SOLICITUDES
212
¿NÚMERO MÁXIMO DE SOLICITUDES AHORA CUMPLIDO
214
NO
406
HECHO
SI
COLOCAR ETIQUETA
408
BORRAR VALORES DE AUTENTIFICACIÓN
216

FIG 5


DETERMINAS SI SE HA ENVIADO PREVIAMENTE VALOR DE AUTENTIFICACIÓN
502
500
506
504
SI
¿PREVIAMENTE ENVIADO?
ENVIAR VALOR DE AUTENTIFICACIÓN
NO
DETERMINAR SI SE HA ENVIADO NÚMERO MÁXIMO DE VALORES ÚNICOS AUTH
508
512
510
SI
¿NÚMERO MÁXIMO ENVIADO?
RECHAZAR ENVIAR VALOR DE AUTENTIFICACIÓN
NO
514
ENVIAR VALOR DE AUTENTIFICACIÓN
DETERMINAR SI SE HA ENVIADO AHORA NÚMERO MÁXIMO DE VALORES ÚNICOS DE AUTENTIFICACIÓN
516
518
¿NÚMERO MÁXIMO ENVIADO AHORA?
NO
SI
BORRAR VALORES DE AUTENTIFICACIÓN QUE NO HAN SIDO ENVIADOS
520
524
PASAR A 212 DE LA FIGURA 2