(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 662 058**

(51) Int. CI.:

G06F 21/44 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.05.2008 PCT/US2008/065104**

(87) Fecha y número de publicación internacional: **03.12.2009 WO09145774**

(96) Fecha de presentación y número de la solicitud europea: **29.05.2008 E 08769798 (3)**

(97) Fecha y número de publicación de la concesión europea: **28.02.2018 EP 2294505**

(54) Título: **Autenticación de un componente de impresora reemplazable**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.04.2018

(73) Titular/es:

HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P. (100.0%)
11445 Compaq Center Drive West
Houston, TX 77070, US

(72) Inventor/es:

REFSTRUP, JACOB GRUNDTVIG

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Autenticación de un componente de impresora reemplazable

Antecedentes

Los sistemas de impresión actuales suelen incluir uno o más componentes de impresora reemplazables, como cartuchos de inyección de tinta, conjuntos de cabezales de impresión de inyección de tinta, cartuchos de tóner, suministros de tinta, etc. Algunos sistemas existentes proporcionan estos componentes de impresora reemplazables con memoria incorporada para comunicar información a una impresora sobre el componente reemplazable, como nivel de llenado de tinta, información de comercialización, etc.

La publicación de patente de EE.UU. No. 7,246,098 divulga un protocolo de autenticación consumible para validar la existencia de un chip de autenticación que no es de confianza, así como para garantizar que el chip de autenticación tenga una duración solo tan larga como el consumible. La publicación de patente de EE.UU. No. 6,799,273 divulga un proceso de identificación mutua entre un primer y un segundo aparato de procesamiento de datos, para proteger los datos protegidos por derechos de autor. La publicación de la solicitud de patente de EE.UU. No. 2007/0160204 divulga un microcontrolador que realiza la autenticación de accesorios reemplazables, tales como cartuchos de tinta, usando un número aleatorio encriptado.

Breve descripción de los dibujos

Los dibujos adjuntos se incluyen para proporcionar una comprensión adicional de las realizaciones y se incorporan y constituyen una parte de esta especificación. Los dibujos ilustran realizaciones y junto con la descripción sirven para explicar los principios de las realizaciones. Se apreciarán fácilmente otras realizaciones y muchas de las ventajas pretendidas de las realizaciones cuando se hagan más comprensibles por referencia a la siguiente descripción detallada. Los elementos de los dibujos no están necesariamente a escala entre sí. Los números de referencia similares designan partes similares correspondientes.

La Figura 1 es un diagrama de bloques que ilustra una realización de una disposición de impresión.

La Figura 2 es un diagrama de flujo que ilustra una realización de un método para autenticar un componente de impresora reemplazable.

La Figura 3 es un diagrama de flujo que ilustra una realización de un método para autenticar una solicitud de lectura emitida por un sistema de impresión para un valor de datos que indica la autenticidad de un componente de impresora reemplazable.

La Figura 4 es un diagrama de flujo que ilustra una realización de un método para autenticar una respuesta de un componente de impresora reemplazable.

Descripción detallada

En la siguiente descripción detallada, se hace referencia a los dibujos adjuntos que forman una parte de la misma, y en los que se muestra a modo de ilustración realizaciones específicas en las que se puede poner en práctica la invención. A este respecto, la terminología direccional, tal como "superior", "inferior", "delantera", "posterior", , etc., se usa con referencia a la orientación de la(s) figura(s) descrita(s). Debido a que los componentes de las realizaciones se pueden posicionar en varias orientaciones diferentes, la terminología direccional se usa con fines de ilustración y no es de ninguna manera limitante. Debe entenderse que se pueden utilizar otras realizaciones y se pueden realizar cambios estructurales o lógicos sin salirse del alcance de la presente invención. La siguiente descripción detallada, por lo tanto, no debe tomarse en un sentido limitativo, y el alcance de la presente invención está definido por las reivindicaciones adjuntas.

Debe entenderse que las características de las diversas realizaciones a modo de ejemplo descritas en este documento se pueden combinar entre sí, a menos que se indique específicamente lo contrario.

La figura 1 es un diagrama de bloques que ilustra una realización de una disposición de impresión 100. La disposición de impresión 100 incluye un servidor 102 y un sistema de impresión 104. El sistema de impresión 104 facilita la impresión de imágenes gráficas y/o texturales en un medio de impresión 118, como papel, cartulina, transparencias, Mylar, tela y similares. El sistema de impresión 104 incluye, por ejemplo, una impresora de inyección de tinta, una impresora láser u otra impresora adecuada. El servidor 102 se comunica con el sistema de impresión 104 y proporciona señales de datos y / o de control al sistema de impresión 104. El servidor 102 puede estar o puede ser incluso en una variedad de fuentes de información tales como una computadora, aparato u otro dispositivo adecuado tal como un dispositivo digital personal asistente (PDA), cámara digital, teléfono móvil, etc.

En una realización, el sistema de impresión 104 incluye un controlador de impresora 116, un dispositivo de memoria 122 y un componente de impresora reemplazable 108. El componente de impresora reemplazable 108 incluye un dispositivo de memoria 109. En una realización, el controlador de impresora 116 determina la autenticidad del componente de impresora reemplazable 108 en base a claves secretas almacenadas en el dispositivo de memoria

109 y en el dispositivo de memoria 122.

El controlador de impresora 116 controla el funcionamiento del sistema de impresión 104 y, como tal, recibe señales de datos y / o de control desde el servidor 102. El controlador de impresora 116 se comunica con el servidor 102 a través de un enlace de comunicación 106. El enlace de comunicación 106 incluye, por ejemplo, una trayectoria de transferencia de información óptica, de infrarrojos o de otro tipo adecuado entre el controlador de impresora 116 y el servidor 102. El controlador de impresora 116 se comunica con el dispositivo de memoria 122 a través de un enlace de comunicación 120. El enlace de comunicación 120 incluye, por ejemplo, una trayectoria de transferencia de información eléctrica, óptica, de infrarrojos o de otro tipo adecuado entre el controlador de impresora 116 y el dispositivo de memoria 122.

El dispositivo de memoria 122 incluye una memoria no volátil (NVM) 123 y una lógica 124. En una realización, el dispositivo de memoria 122 es inviolable o resistente a la manipulación. En una realización, la lógica 124 es un circuito lógico o software integrado que se ejecuta en un procesador. Por ejemplo, en una realización, el dispositivo de memoria 122 incluye una unidad de procesamiento central (CPU) o sistema en un chip (SoC) con memoria no volátil integrada 123. En otra realización, el dispositivo de memoria 122 incluye una CPU o SoC con memoria externa no memoria volátil 123. En otra realización, el dispositivo de memoria 122 incluye lógica dedicada con memoria no volátil interna o externa 1.23. En otra realización, el dispositivo de memoria 122 está embebido dentro del controlador de impresora 116 con memoria no volátil interna o externa 123.

En una realización, la memoria no volátil 123 es una EEPROM, una FLASH u otra memoria adecuada. La memoria no volátil 123 almacena una o más claves secretas utilizadas para autenticar el componente de impresora reemplazable 108. El componente de impresora reemplazable 108 se autentica autenticando una comunicación entre el controlador de impresora 116 y el dispositivo de memoria 109 usando claves de sesión. Para generar una clave de sesión, el controlador de impresora 116 pasa un identificador de clave de sesión y una solicitud de una clave de sesión al dispositivo de memoria 122. En respuesta al identificador de clave de sesión y a la solicitud de una clave de sesión, el circuito lógico 124 genera una clave de sesión basada en el identificador de clave de sesión y una clave secreta almacenada en la memoria no volátil 123. El circuito lógico 124 proporciona entonces la clave de sesión generada al controlador de impresora 116.

El componente de impresora reemplazable 108 incluye un componente del sistema de impresión 104 que es insertable y extraíble del sistema de impresión 104. En una realización, el componente de impresora reemplazable 108 incluye un componente consumible que se desecha y reemplaza al final de su vida útil. Un ejemplo de dicho componente consumible incluye un recipiente de tinta o un cartucho de tóner que contiene un suministro de material de marcado para el sistema de impresión 104. El material de marcado es depositado en el medio de impresión 118 por el sistema de impresión 104 y se reduce durante una vida útil del recipiente de tinta o cartucho de tóner. Como tal, el recipiente de tinta o cartucho de tóner se desecha y reemplaza al final de su vida útil o se refabrica y reutiliza.

En otra realización, el componente de impresora reemplazable 108 incluye un componente de impresión que se reemplaza fácilmente en el sistema de impresión 104. Ejemplos de dicho componente de impresión incluyen un cabezal de impresión que deposita selectivamente tinta en el medio de impresión 118 en respuesta a señales de control procedentes del controlador de impresora 116 o un cartucho de impresora que incluye un cabezal de impresión y un suministro de tinta. Por lo tanto, el componente de impresora reemplazable 108 puede incluir un recipiente de tinta, un cabezal de impresión o un cartucho de impresora si, por ejemplo, el sistema de impresión 104 incluye una impresora de chorro de tinta. Además, el componente de impresora reemplazable 108 puede incluir un cartucho de tóner o un tambor de revelado si, por ejemplo, el sistema de impresión 104 incluye una impresora láser. Además, el componente de impresora reemplazable 108 puede incluir un dispositivo periférico del sistema de impresión 104, tal como una tarjeta de Ethernet, un duplexor, un finalizador de papel (por ejemplo, grapadora, perforadora, etc.), u otro dispositivo adecuado.

El controlador de impresora 116 y el componente de impresora reemplazable 108 se comunican entre sí a través de un enlace de comunicación 114. El enlace de comunicación 114 facilita la transferencia de información entre el controlador de impresora 116 y el componente de impresora reemplazable 108 cuando el componente de impresora reemplazable 108 está instalado en el sistema de impresión 104. El enlace de comunicación 114 incluye, por ejemplo, una trayectoria de transferencia de información eléctrica, óptica, infrarroja u otra adecuada, entre el componente 108 de impresora reemplazable y el controlador de impresora 116.

El componente de impresora reemplazable 108 incluye un dispositivo de memoria 109 que almacena información para el componente de impresora reemplazable 108 y / o el sistema de impresión 104. El dispositivo de memoria 109 incluye una memoria no volátil (NVM) 110 y una lógica 111. En una realización, el dispositivo de memoria 109 es inviolable o a prueba de manipulación. En una realización, la lógica 111 es un circuito lógico o software integrado que se ejecuta en un procesador. Por ejemplo, en una realización, el dispositivo de memoria 109 incluye una CPU o un SoC con memoria integrada no volátil 110. En otra realización, el dispositivo de memoria 109 incluye una CPU o un SoC con memoria externa no volátil 110. En otra realización, el dispositivo de memoria 109 incluye lógica dedicada con memoria no volátil interna o externa 110.

En una realización, la memoria 110 no volátil es una memoria no volátil de 256 bytes u otra memoria no volátil

dimensionada adecuadamente , tal como una EEPROM, una FLASH u otra memoria adecuada. En una realización, la memoria no volátil 110 del dispositivo de memoria 109 almacena, por ejemplo, información que es específica del componente 108 de impresora reemplazable y / o información que es aplicable al sistema 104 de impresión. Además, la memoria no volátil 110 puede tener información para ser utilizada por el sistema de impresión 104 almacenada en la misma o puede registrar información para el sistema de impresión 104. En una realización, la información que puede ser almacenada en la memoria no volátil 110 incluye parámetros operativos y / o no operativos para el componente de impresora reemplazable 108 y / o el sistema de impresión 104.

La memoria no volátil 110 también almacena un valor en un campo de datos que indica que el componente de impresora reemplazable 108 es genuino. Además, la memoria no volátil 110 almacena una o más claves secretas utilizadas para autenticar el componente de impresora reemplazable 108. En una realización, la una o más claves secretas almacenadas en la memoria 110 no volátil del dispositivo 109 de memoria son obtenidas a partir de la una o más claves secretas almacenadas en la memoria no volátil 123 del dispositivo de memoria 122. En otras realizaciones, la una o más claves secretas almacenadas en la memoria no volátil 110 del dispositivo de memoria 109 y la una o más claves secretas almacenadas en la memoria no volátil 123 del dispositivo 122 de memoria son obtenidas a partir de una o más claves secretas comunes. Como tal, la una o más claves secretas almacenadas en la memoria no volátil 110 están relacionadas con la una o más claves secretas almacenadas en la memoria no volátil 123.

En una realización, el componente de impresora reemplazable 108 incluye un enlace de comunicación 112 que conecta eléctricamente o conecta comunicativamente el dispositivo de memoria 109 con el enlace de comunicación 114 y, por lo tanto, con el controlador de impresora 116 cuando el componente de impresora reemplazable 108 está instalado en el sistema de impresión 104. Como tal, cuando el componente de impresora reemplazable 108 está instalado en el sistema de impresión 104, el dispositivo de memoria 109 se comunica con el controlador de impresora 116 a través de enlaces de comunicación 112 y 114. Por lo tanto, los enlaces de comunicación 112 y 114 incluyen, por ejemplo, acoplamientos o conexiones eléctricas tales como contactos eléctricos con los correspondientes nodos eléctricos o receptáculos, respectivamente.

El componente de impresora reemplazable 108 se autentica autenticando una comunicación entre el controlador de impresora 116 y el dispositivo de memoria 109 usando claves de sesión. Para generar una clave de sesión, el controlador de impresora 116 pasa una solicitud de un identificador de clave de sesión al dispositivo de memoria 109. En respuesta a la solicitud de un identificador de clave de sesión, el circuito lógico 111 del dispositivo de memoria 109 genera un identificador de clave de sesión y una clave de sesión asociada basada en una clave secreta almacenada en la memoria no volátil 110. En una realización, el circuito lógico 111 del dispositivo de memoria 109 genera un identificador de clave de sesión diferente y una clave de sesión asociada en respuesta a cada solicitud para un identificador de clave se sesión . Por lo tanto, cada identificador de clave de sesión y cada clave de sesión asociada se utilizan solo una vez. El circuito lógico 111 proporciona el identificador de clave de sesión generado al controlador de impresora 116, que a su vez pasa el identificador de clave de sesión al dispositivo de memoria 122 como se describió anteriormente.

La Figura 2 es un diagrama de flujo que ilustra una realización de un método 150 para autenticar un componente de impresora reemplazable 108. En 152, un componente de impresora reemplazable 108 está instalado en un sistema de impresión 104 que incluye un controlador de impresora 116. El componente de impresora reemplazable 108 incluye un dispositivo de memoria 109 que se ha configurado con una o más claves secretas para autenticar el componente de impresora reemplazable 108. El sistema 104 de impresión también incluye un dispositivo 122 de memoria que se ha configurado con una o más claves secretas para autenticar el componente 108 de impresora reemplazable.

En 154, el controlador de impresora 116 solicita un identificador de clave de sesión desde el dispositivo de memoria 109 del componente de impresora reemplazable 108 a través de los enlaces de comunicación 114 y 112. En una realización, el controlador de impresora 116 usa un cuestionamiento aleatorio al solicitar el identificador de clave de sesión para prevenir ataques de reproducción contra el controlador de impresora 116. En 156, en respuesta a la recepción de la solicitud de un identificador de clave de sesión, el circuito lógico 111 del dispositivo de memoria 109 genera el identificador de clave de sesión solicitado y su clave de sesión asociada basada en una primera clave secreta almacenada en la memoria no volátil 110. En 158, el circuito lógico 111 del dispositivo de memoria 109 proporciona el identificador de clave de sesión solicitado al controlador de impresora 116.

En 160, el controlador de impresora 116 proporciona el identificador de clave de sesión, recibido desde el dispositivo de memoria 109, al dispositivo de memoria 122 a través del enlace de comunicación 120 y solicita una clave de sesión. En 162, en respuesta a la recepción del identificador de clave de sesión y a la solicitud de una clave de sesión, el circuito lógico 124 del dispositivo de memoria 122 genera la clave de sesión solicitada en base al identificador de clave de sesión recibido y una segunda clave secreta almacenada en la memoria no volátil 123. Si la primera clave secreta almacenada en la memoria no volátil 110 del dispositivo de memoria 109 está relacionada con la segunda clave secreta almacenada en la memoria no volátil 123 del dispositivo de memoria 122, entonces la clave de sesión generada por el circuito lógico 111 coincide con la clave de sesión generada por el circuito lógico 124. En 164, el circuito lógico 124 del dispositivo de memoria 122 proporciona la clave de sesión solicitada al controlador de impresora 116. En 166, el controlador de impresora 116 usa la clave de sesión recibida para

determinar la autenticidad del componente de impresora reemplazable 108.

La Figura 3 es un diagrama de flujo que ilustra una realización de un método 166 para autenticar una solicitud de lectura emitida por un sistema de impresión 104 para un valor de datos que indica la autenticidad de un componente de impresora reemplazable 108. En 170, con una clave de sesión establecida en un dispositivo de memoria 109 del componente de impresora reemplazable 108 y con una clave de sesión establecida en el sistema de impresión 104, el controlador de impresora 116 calcula un primer código de autenticación de mensaje (MAC) para una solicitud de lectura usando su clave de sesión y un algoritmo criptográfico adecuado. La solicitud de lectura es para un campo de datos de la memoria no volátil 110 que almacena un valor que indica si el componente de impresora reemplazable 108 es genuino. El primer MAC se calcula sobre los parámetros de comando y comando de la solicitud de lectura.

En una realización, el primer MAC se calcula en base a un código de autenticación de mensajes hash (HMAC) con un hash seguro tal como el algoritmo de hash seguro uno (SHA-1), SHA-2 u otro algoritmo de hash seguro adecuado. En otra realización, el primer MAC se calcula en base a un MAC basado en cifrado (CMAC) con un algoritmo de cifrado de bloque como estándar de cifrado de datos (DES), 3DES, estándar de cifrado avanzado (AES), cifrado Rivest dos (RC2) o otro algoritmo de bloques de cifrado adecuado. En otras realizaciones, el primer MAC se calcula usando otra técnica adecuada.

En 172, el controlador de impresora 116 emite la solicitud de lectura que incluye el primer MAC al dispositivo de memoria 109 del componente de impresora reemplazable 108. En 174, en respuesta a la solicitud de lectura, el circuito lógico 111 del dispositivo de memoria 109 calcula un segundo MAC para la solicitud de lectura recibida usando su clave de sesión y el algoritmo criptográfico. En 176, el circuito lógico 111 del dispositivo de memoria 109 compara el primer MAC recibido con el segundo MAC calculado.

En 178, si el primer MAC no coincide con el segundo MAC, entonces la clave de sesión del dispositivo de memoria 109 no coincide con la clave de sesión del sistema de impresión 104. Por lo tanto, la comunicación entre el dispositivo de memoria 109 y el controlador de impresora 116 no es autenticada. En 182, el circuito lógico 111 del dispositivo de memoria 109 aborta o deniega la operación de lectura solicitada. Al denegar la operación de lectura solicitada, el componente de impresora reemplazable 108 ha determinado que el controlador de impresora 116 no es auténtico. Por lo tanto, el componente de impresora reemplazable 108 no se comunica con el controlador de impresora 116. En 184, el circuito lógico 111 del dispositivo de memoria 109 marca su clave de sesión como inválida de modo que no puede ser utilizada usar de nuevo.

En 178, si el primer MAC coincide con el segundo MAC, entonces la clave de sesión del dispositivo de memoria 109 coincide con la clave de sesión del sistema de impresión 104. Por lo tanto, la comunicación entre el dispositivo de memoria 109 y el controlador de impresora 116 es autenticada. En 180, el circuito lógico 111 del dispositivo de memoria 109 realiza la operación de lectura solicitada. En respuesta a la operación de lectura, el dispositivo de memoria 109 devuelve una respuesta que incluye el valor del campo de datos que indica que el componente de impresora reemplazable 108 es genuino.

La Figura 4 es un diagrama de flujo que ilustra una realización de un método 180 para autenticar una respuesta del componente de impresora reemplazable 108. En 186, el dispositivo de memoria 109 calcula un tercer MAC para la respuesta usando su clave de sesión y el algoritmo criptográfico. El tercer MAC se calcula sobre el comando MAC y los datos de respuesta. En 188, el dispositivo de memoria 109 proporciona la respuesta que incluye el tercer MAC al controlador de impresora 116. En 190, en respuesta a la respuesta del dispositivo de memoria 109, el controlador de impresora 116 calcula un cuarto MAC para la respuesta recibida usando su clave de sesión y el algoritmo criptográfico . En 192, el controlador de impresora 116 compara el tercer MAC recibido con el cuarto MAC calculado.

En 194, si el tercer MAC no coincide con el cuarto MAC, entonces la clave de sesión del sistema de impresión 104 no coincide con la clave de sesión del dispositivo de memoria 109. Por lo tanto, la comunicación entre el controlador de impresora 116 y el dispositivo de memoria 109 no está autenticada. Por lo tanto, en 198 el controlador de impresora 116 determina que el componente 108 de impresora reemplazable no es auténtico.

En 194, si el tercer MAC coincide con el cuarto MAC, entonces la clave de sesión del sistema de impresión 104 coincide con la clave de sesión del dispositivo de memoria 109. Por lo tanto, la comunicación entre el controlador de impresora 116 y el dispositivo de memoria 109 es autenticada. Como la comunicación entre el dispositivo de memoria 109 y el controlador de impresora 116 se ha autenticado, el controlador de impresora 116 puede confiar en el valor devuelto en respuesta a la solicitud de lectura. Por lo tanto, en 196 el controlador de impresora 116 determina que el componente de impresora reemplazable 108 es auténtico.

Las realizaciones proporcionan un sistema de impresión en el que se puede instalar un componente de impresora reemplazable. Las realizaciones del sistema de impresión incluyen un dispositivo de memoria que almacena una o más claves secretas. Las realizaciones del componente de impresora reemplazable incluyen un dispositivo de memoria que almacena una o más claves secretas relacionadas con la una o más claves secretas almacenadas en el dispositivo de memoria de las realizaciones del sistema de impresión. La una o más claves secretas almacenadas en las realizaciones del sistema de impresión y en las realizaciones del componente de impresora reemplazable se usan para autenticar las realizaciones del componente de impresora reemplazable. Por lo tanto, se evita el uso de

componentes de impresora reemplazables falsificados en las realizaciones del sistema de impresión.

Aunque se han ilustrado y descrito aquí realizaciones específicas, los expertos en la técnica apreciarán que una variedad de implementaciones alternativas y equivalentes puede sustituir a las realizaciones específicas mostradas y descritas sin que se salgan del alcance de la presente invención. Esta solicitud está destinada a cubrir cualquier adaptación o variación de las realizaciones específicas discutidas aquí. Por lo tanto, se pretende que esta invención esté limitada únicamente por las reivindicaciones y sus equivalentes.

REIVINDICACIONES

1. Un componente de impresora reemplazable (108) que comprende:

un primer dispositivo de memoria (109) configurado para almacenar un primer secreto; y

un enlace de comunicación (112) configurado para vincular comunicativamente el primer dispositivo de memoria con un controlador de impresora (116) cuando el componente de impresora reemplazable está instalado en un sistema de impresión (104); donde el primer dispositivo de memoria está configurado para:

generar un identificador de clave de sesión y una primera clave de sesión basada en el primer secreto y proporcionar el identificador de clave de sesión a un segundo dispositivo de memoria del sistema de impresión en respuesta a una solicitud,

recibir una solicitud de lectura para un campo de datos que almacena un valor que indica la autenticidad del componente reemplazable de la impresora, incluyendo la solicitud de lectura un primer código de autenticación de mensaje calculado utilizando una segunda clave de sesión;

calcular un segundo código de autenticación de mensaje basado en la solicitud de lectura y la primera clave de sesión, y

realizar la solicitud de lectura en respuesta al segundo código de autenticación de mensaje coincidiendo con el primer código de autenticación de mensaje,

donde el primer dispositivo de memoria está configurado para denegar la solicitud de lectura y marcar la primera clave de sesión como inválida en respuesta al segundo código de autenticación de mensaje que no coincide con el primer código de autenticación de mensaje y el primer dispositivo de memoria configurado para realizar la solicitud de lectura proporcionando una respuesta que incluye el valor que indica la autenticidad del componente de impresora reemplazable y un tercer código de autenticación de mensaje calculado sobre el valor que indica la autenticidad del componente de impresora reemplazable utilizando la primera clave de sesión.

2. El componente de impresora reemplazable de una de la reivindicación 1, en el que el primer dispositivo de memoria está configurado para generar un identificador de clave de sesión y una clave de sesión diferentes en respuesta a cada solicitud.

3. El componente de impresora reemplazable de la reivindicación 1, en el que el componente de impresora reemplazable comprende uno de un cartucho de inyección de tinta, un conjunto de cabezal de impresión de inyección de tinta, un cartucho de tóner y un suministro de tinta.

4. Un sistema de impresión que comprende,

un controlador de impresora,

el componente de impresora reemplazable de una de las reivindicaciones 1 - 3, y

el segundo dispositivo de memoria (122) que almacena un segundo secreto, el segundo dispositivo de memoria vinculado comunicativamente con el controlador de impresora, y en el que el controlador de impresora está configurado para determinar una autenticidad del componente de impresora reemplazable basada en el primer secreto y en el segundo secreto.

5. El sistema de impresión de la reivindicación 4, en el que el primer secreto se obtiene a partir del segundo secreto.

6. El sistema de impresión de la reivindicación 4, en el que el segundo dispositivo de memoria está configurado para generar una segunda clave de sesión en base al identificador de clave de sesión y el segundo secreto.

7. Sistema de impresión según la reivindicación 6, en el que el controlador de impresora está configurado para calcular un cuarto código de autenticación de mensaje basado en la respuesta y la segunda clave de sesión y autenticar el componente de impresora reemplazable en respuesta al tercer código de autenticación de mensaje que coincide con el cuarto código de autenticación de mensaje.

8. Un método para determinar la autenticidad de un componente de impresora reemplazable (108) que comprende:

almacenar una primera clave secreta en el componente reemplazable de la impresora;

instalar el componente de impresora reemplazable en un sistema de impresión (104), almacenando el sistema de impresión una segunda clave secreta;

solicitar, por un controlador de impresora del sistema de impresión, un identificador de clave de sesión del componente de impresora reemplazable;

generar el identificador de clave de sesión y una primera clave de sesión dentro del componente de impresora reemplazable en base a la primera clave secreta en respuesta a la solicitud;

proporcionar el identificador de clave de sesión al sistema de impresión;

generar una segunda clave de sesión dentro del sistema de impresión en base al identificador de clave de sesión y la segunda clave secreta; y

calcular un primer código de autenticación de mensaje utilizando la segunda clave de sesión dentro del sistema de impresión para una solicitud de lectura al componente de impresora reemplazable, siendo la solicitud de lectura para un campo de datos que almacena un valor que indica la autenticidad del componente de impresora reemplazable;

emitir la solicitud de lectura que incluye el primer código de autenticación de mensaje para el componente de impresora reemplazable;

calcular un segundo código de autenticación de mensaje para la solicitud de lectura usando la primera clave de sesión dentro del componente de impresora reemplazable;

realizar la solicitud de lectura en respuesta al segundo código de autenticación de mensaje que coincide con el primer código de autenticación de mensaje;

denegar la solicitud de lectura y marcar la primera clave de sesión como no válida como respuesta de que el segundo código de autenticación de mensaje que no coincide con el primer código de autenticación de mensaje;

proporcionar, mediante el componente de impresora reemplazable, al sistema de impresión, una respuesta a la solicitud de lectura que incluye el valor que indica la autenticidad del componente de impresora reemplazable y un tercer código de autenticación de mensaje calculado sobre el valor que indica la autenticidad del componente reemplazable clave de sesión; y

calcular un cuarto código de autenticación de mensaje sobre el valor que indica la autenticidad del componente de impresora reemplazable en la respuesta utilizando la segunda clave de sesión dentro del sistema de impresión; y

autenticar el componente de impresora reemplazable como respuesta de que el tercer código de autenticación de mensaje que coincide con el cuarto código de autenticación de mensaje.

9. El método de la reivindicación 8, en el que la primera clave secreta se obtiene a partir de la segunda clave secreta.

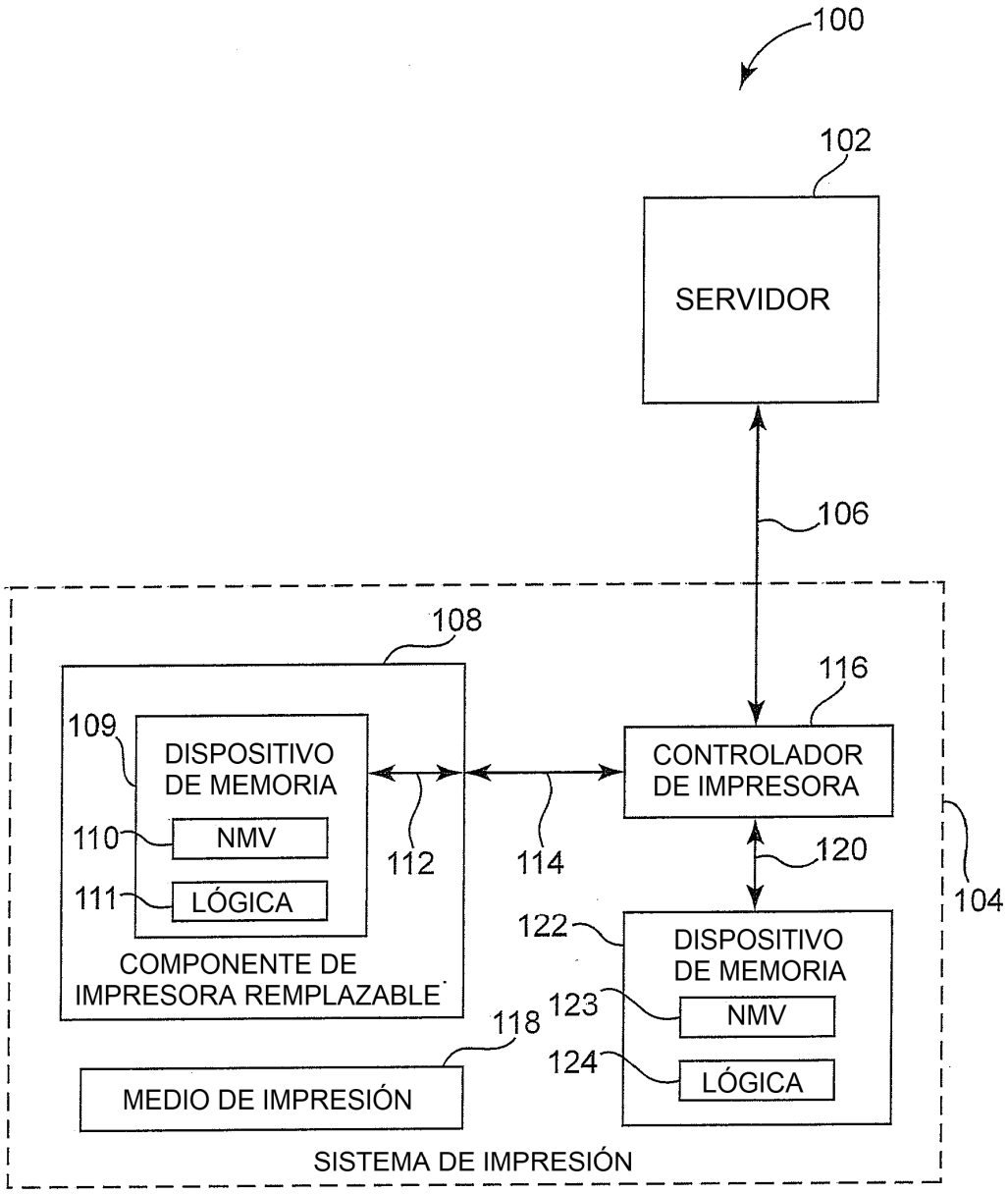
100
102
SERVIDOR
106
108
116
109
DISPOSITIVO DE MEMORIA
110
NMV
111
LÓGICA
112
114
CONTROLADOR DE IMPRESORA
120
104
122
DISPOSITIVO DE MEMORIA
123
NMV
124
LÓGICA
COMPONENTE DE IMPRESORA REMPLAZABLE
118
MEDIO DE IMPRESIÓN
SISTEMA DE IMPRESIÓN

Fig. 1

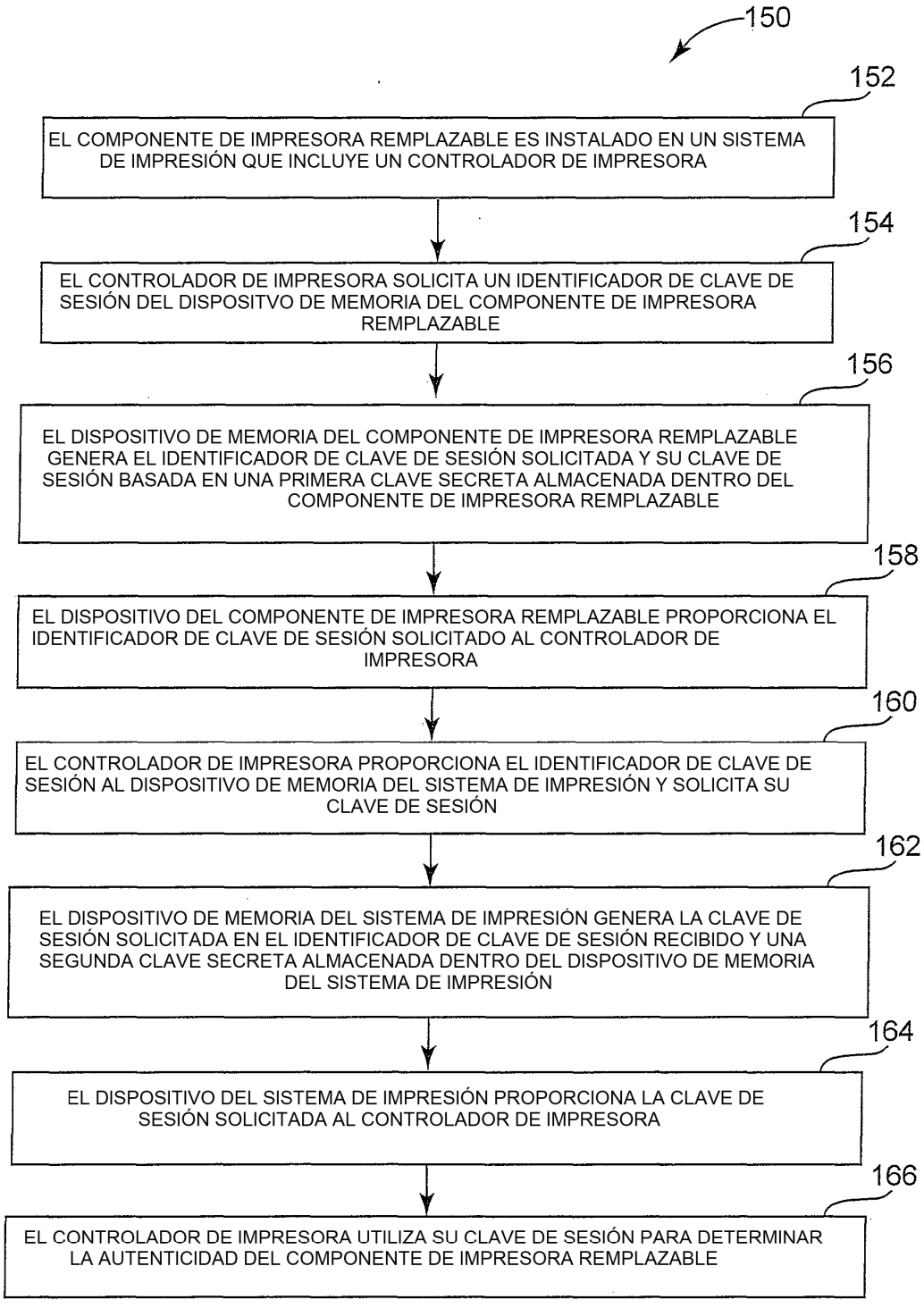
150
152
EL COMPONENTE DE IMPRESORA REMPLAZABLE ES INSTALADO EN UN SISTEMA DE IMPRESIÓN QUE INCLUYE UN CONTROLADOR DE IMPRESORA
154
EL CONTROLADOR DE IMPRESORA SOLICITA UN IDENTIFICADOR DE CLAVE DE SESIÓN DEL DISPOSITVO DE MEMORIA DEL COMPONENTE DE IMPRESORA REMPLAZABLE
156
EL DISPOSITIVO DE MEMORIA DEL COMPONENTE DE IMPRESORA REMPLAZABLE GENERA EL IDENTIFICADOR DE CLAVE DE SESIÓN SOLICITADA Y SU CLAVE DE SESIÓN BASADA EN UNA PRIMERA CLAVE SECRETA ALMACENADA DENTRO DEL COMPONENTE DE IMPRESORA REMPLAZABLE
158
EL DISPOSITIVO DEL COMPONENTE DE IMPRESORA REMPLAZABLE PROPORCIONA EL IDENTIFICADOR DE CLAVE DE SESIÓN SOLICITADO AL CONTROLADOR DE IMPRESORA
160
EL CONTROLADOR DE IMPRESORA PROPORCIONA EL IDENTIFICADOR DE CLAVE DE SESIÓN AL DISPOSITIVO DE MEMORIA DEL SISTEMA DE IMPRESIÓN Y SOLICITA SU CLAVE DE SESIÓN
162
EL DISPOSITIVO DE MEMORIA DEL SISTEMA DE IMPRESIÓN GENERA LA CLAVE DE SESIÓN SOLICITADA EN EL IDENTIFICADOR DE CLAVE DE SESIÓN RECIBIDO Y UNA SEGUNDA CLAVE SECRETA ALMACENADA DENTRO DEL DISPOSITIVO DE MEMORIA DEL SISTEMA DE IMPRESIÓN
164
EL DISPOSITIVO DEL SISTEMA DE IMPRESIÓN PROPORCIONA LA CLAVE DE SESIÓN SOLICITADA AL CONTROLADOR DE IMPRESORA
166
EL CONTROLADOR DE IMPRESORA UTILIZA SU CLAVE DE SESIÓN PARA DETERMINAR LA AUTENTICIDAD DEL COMPONENTE DE IMPRESORA REMPLAZABLE

Fig. 2

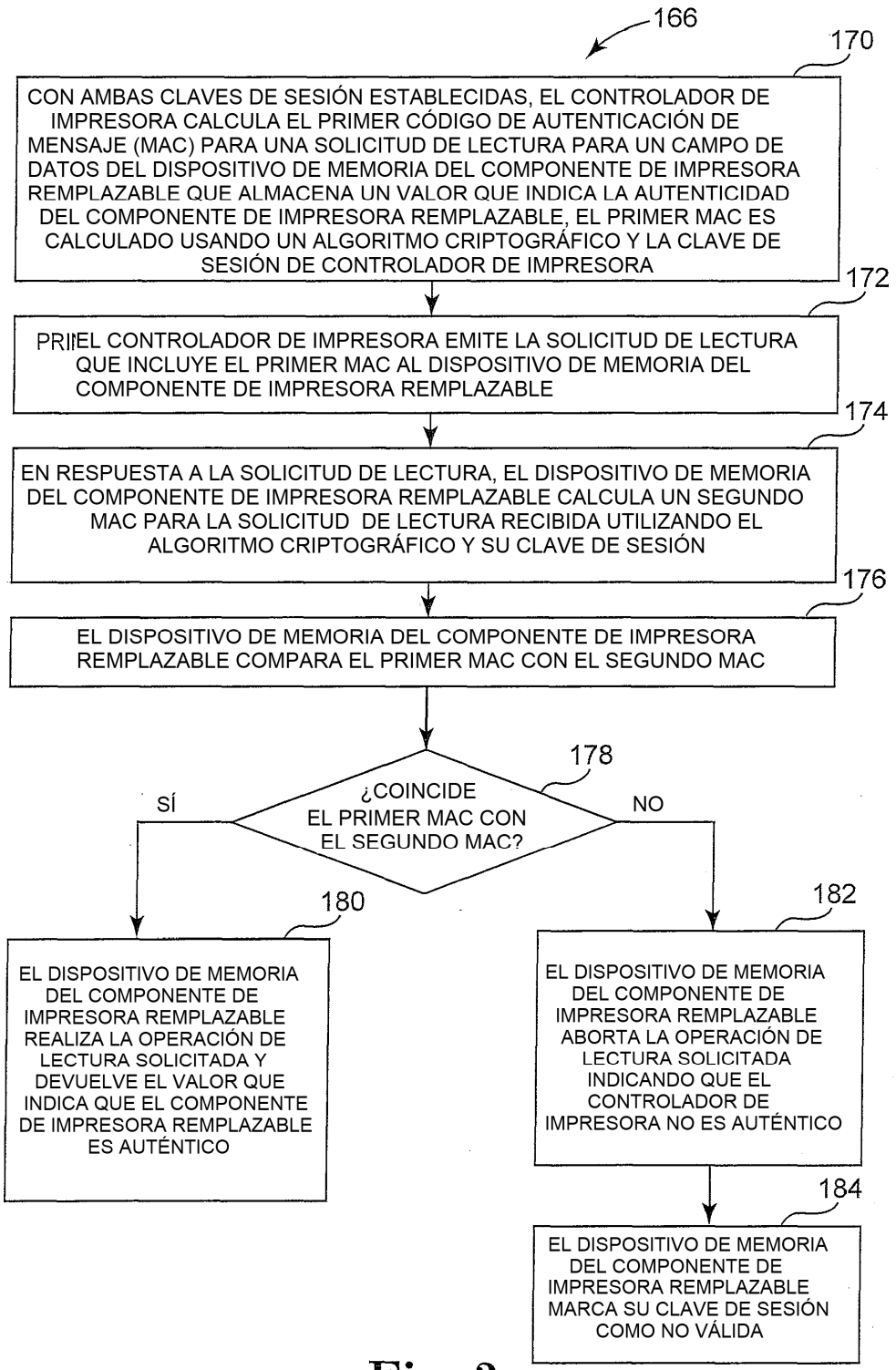
166
170
CON AMBAS CLAVES DE SESIÓN ESTABLECIDAS, EL CONTROLADOR DE IMPRESORA CALCULA EL PRIMER CÓDIGO DE AUTENTICACIÓN DE MENSAJE (MAC) PARA UNA SOLICITUD DE LECTURA PARA UN CAMPO DE DATOS DEL DISPOSITIVO DE MEMORIA DEL COMPONENTE DE IMPRESORA REMPLAZABLE QUE ALMACENA UN VALOR QUE INDICA LA AUTENTICIDAD DEL COMPONENTE DE IMPRESORA REMPLAZABLE, EL PRIMER MAC ES CALCULADO USANDO UN ALGORITMO CRIPTOGRÁFICO Y LA CLAVE DE SESIÓN DE CONTROLADOR DE IMPRESORA
172
EL CONTROLADOR DE IMPRESORA EMITE LA SOLICITUD DE LECTURA QUE INCLUYE EL PRIMER MAC AL DISPOSITIVO DE MEMORIA DEL COMPONENTE DE IMPRESORA REMPLAZABLE
174
EN RESPUESTA A LA SOLICITUD DE LECTURA, EL DISPOSITIVO DE MEMORIA DEL COMPONENTE DE IMPRESORA REMPLAZABLE CALCULA UN SEGUNDO MAC PARA LA SOLICITUD DE LECTURA RECIBIDA UTILIZANDO EL ALGORITMO CRIPTOGRÁFICO Y SU CLAVE DE SESIÓN
176
EL DISPOSITIVO DE MEMORIA DEL COMPONENTE DE IMPRESORA REMPLAZABLE COMPARA EL PRIMER MAC CON EL SEGUNDO MAC
178
¿COINCIDE EL PRIMER MAC CON EL SEGUNDO MAC?
SÍ
NO
180
EL DISPOSITIVO DE MEMORIA DEL COMPONENTE DE IMPRESORA REMPLAZABLE REALIZA LA OPERACIÓN DE LECTURA SOLICITADA Y DEVUELVE EL VALOR QUE INDICA QUE EL COMPONENTE DE IMPRESORA REMPLAZABLE ES AUTÉNTICO
182
EL DISPOSITIVO DE MEMORIA DEL COMPONENTE DE IMPRESORA REMPLAZABLE ABORTA LA OPERACIÓN DE LECTURA SOLICITADA INDICANDO QUE EL CONTROLADOR DE IMPRESORA NO ES AUTÉNTICO
184
EL DISPOSITIVO DE MEMORIA DEL COMPONENTE DE IMPRESORA REMPLAZABLE MARCA SU CLAVE DE SESIÓN COMO NO VÁLIDA

Fig. 3

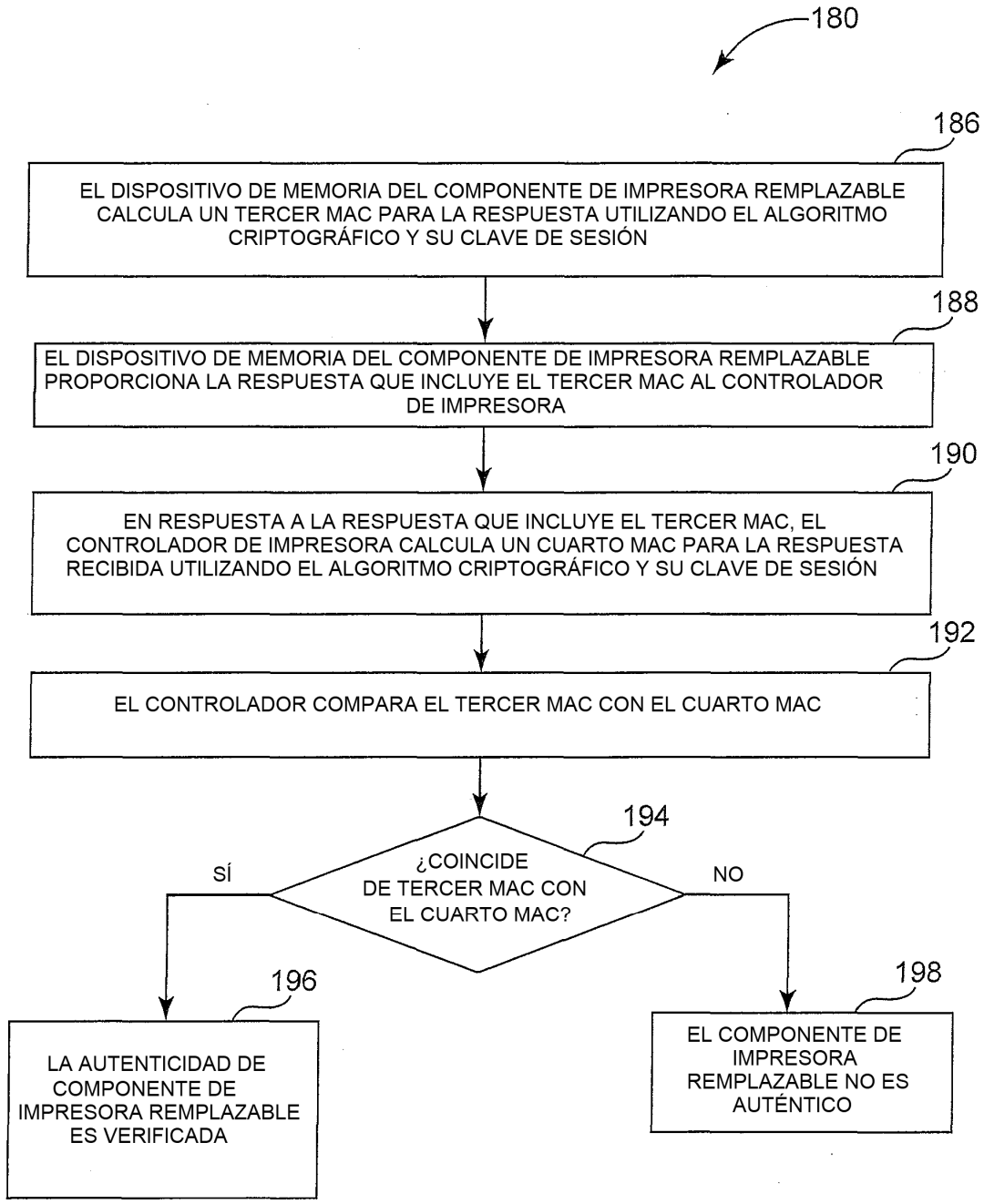
180
186
EL DISPOSITIVO DE MEMORIA DEL COMPONENTE DE IMPRESORA REMPLAZABLE CALCULA UN TERCER MAC PARA LA RESPUESTA UTILIZANDO EL ALGORITMO CRIPTOGRÁFICO Y SU CLAVE DE SESIÓN
188
EL DISPOSITIVO DE MEMORIA DEL COMPONENTE DE IMPRESORA REMPLAZABLE PROPORCIONA LA RESPUESTA QUE INCLUYE EL TERCER MAC AL CONTROLADOR DE IMPRESORA
190
EN RESPUESTA A LA RESPUESTA QUE INCLUYE EL TERCER MAC, EL CONTROLADOR DE IMPRESORA CALCULA UN CUARTO MAC PARA LA RESPUESTA RECIBIDA UTILIZANDO EL ALGORITMO CRIPTOGRÁFICO Y SU CLAVE DE SESIÓN
192
EL CONTROLADOR COMPARA EL TERCER MAC CON EL CUARTO MAC
194
¿COINCIDE DE TERCER MAC CON EL CUARTO MAC?
SÍ
NO
196
LA AUTENTICIDAD DE COMPONENTE DE IMPRESORA REMPLAZABLE ES VERIFICADA
198
EL COMPONENTE DE IMPRESORA REMPLAZABLE NO ES AUTÉNTICO

Fig. 4