(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 765 485**

(51) Int. CI.:

G06F 21/60 (2013.01)
G06F 21/44 (2013.01)
B41J 2/175 (2006.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **29.05.2008 E 17166673 (8)**

(97) Fecha y número de publicación de la concesión europea: **18.12.2019 EP 3208736**

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

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.06.2020

(73) Titular/es:

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

(72) Inventor/es:

REFSTRUP, JACOB

(74) Agente/Representante:

SÁNCHEZ SILVA, Jesús Eladio

DESCRIPCIÓN

Autenticación de un componente reemplazable de la impresora

Antecedentes

Los sistemas de impresión actuales generalmente incluyen uno o más componentes reemplazables de la impresora, tales 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 reemplazables de la impresora con memoria integrada para comunicar información a una impresora sobre el componente reemplazable, tal como nivel de llenado de tinta, información de marketing, etc.

El documento US7246098 divulga un protocolo de autenticación consumible para validar un chip de autenticación no confiable, así como también para garantizar que el chip de autenticación dure solo el tiempo del consumible. El documento US2007/0223942 divulga un cartucho de tóner que tiene un microcontrolador que almacena datos para crear un código de autenticación de mensaje.

Breve descripción de los dibujos

Los dibujos acompañantes se incluyen para proporcionar una mejor comprensión de las realizaciones y se incorporan y constituyen una parte de esta descripción. Los dibujos ilustran las realizaciones y, junto con la descripción, sirven para explicar los principios de las realizaciones. Otras realizaciones y muchas de las ventajas previstas de las realizaciones se apreciarán fácilmente a medida que se entiendan mejor con referencia a la siguiente descripción detallada. Los elementos de los dibujos no están necesariamente a escala uno con relación al otro. 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 reemplazable de la impresora.

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

Descripción detallada

En la siguiente descripción detallada, se hace referencia a los dibujos acompañantes, que forman parte de la misma, y en los que se muestran, a manera de ilustración las realizaciones específicas en las que puede ponerse en práctica la invención, en este sentido, la terminología direccional, tal como "parte superior", "parte inferior", "frontal", "posterior", "delantero", "trasero", etc., se usa con referencia a la orientación de la(s) figura(s) que se describen. Debido a que los componentes de las realizaciones pueden posicionarse en varias orientaciones diferentes, la terminología direccional se usa con fines de ilustración, y de ninguna manera es limitante. Se debe comprender que se pueden utilizar otras realizaciones y se pueden realizar cambios estructurales o lógicos sin apartarse del alcance de la presente invención. La siguiente descripción detallada, por lo tanto, no debe ser tomarse en un sentido limitante, y el alcance de la presente invención se define por las reivindicaciones adjuntas.

Debe entenderse que las características de las diversas realizaciones ilustrativas descritas en este documento pueden combinarse 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 ordenador central 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, tal 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 ordenador central 102 se comunica con el sistema de impresión 104 y proporciona datos y/o señales de control al sistema de impresión 104. El ordenador central 102 puede ser o puede incluirse en una variedad de fuentes de información, tal como una computadora, un aparato u otro dispositivo adecuado, tal como un asistente digital personal (PDA), una cámara digital, un teléfono celular, etc.

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

El controlador de la impresora 116 controla el funcionamiento del sistema de impresión 104 y, como tal, recibe datos y/o señales de control del ordenador central 102. El controlador de la impresora 116 se comunica con el ordenador central 102 a través de un enlace de comunicación 106. El enlace de comunicación 106 incluye, por ejemplo, una vía de transferencia de información eléctrica, óptica, infrarroja u otra adecuada entre el controlador de la impresora 116 y el ordenador central 102. El controlador de la 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 vía de transferencia de información eléctrica, óptica, infrarroja u otra adecuada entre el controlador de la impresora 116 y el dispositivo de memoria 122.

El dispositivo de memoria 122 incluye una memoria no volátil (NVM) 123 y lógica 124. En una realización, el dispositivo de memoria 122 es a prueba de manipulaciones o resistente a manipulaciones. En una realización, la lógica 124 es un circuito lógico o software incorporado 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 incorporada 123. En otra realización, el dispositivo de memoria 122 incluye una CPU o SoC con memoria no volátil externa 123. En otra realización, el dispositivo de memoria 122 incluye lógica dedicada con memoria no volátil interna o externa 123. En otra realización, el dispositivo de memoria 122 se incorpora dentro del controlador de la 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 reemplazable de la impresora 108. El componente reemplazable de la impresora 108 se autentica mediante la autenticación de una comunicación entre el controlador de la impresora 116 y el dispositivo de memoria 109 mediante el uso de claves de sesión. Para generar una clave de sesión, el controlador de la 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 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 la clave de sesión generada al controlador de la impresora 116.

El componente reemplazable de la impresora 108 incluye un componente del sistema de impresión 104 que se puede insertar y retirar del sistema de impresión 104. En una realización, el componente reemplazable de la impresora 108 incluye un componente consumible que se dispone y reemplaza al final de su vida útil. Un ejemplo de tal componente consumible incluye un contenedor 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 se deposita en el medio de impresión 118 mediante el sistema de impresión 104 y se agota durante una vida útil del contenedor de tinta o cartucho de tóner. Como tal, el contenedor de tinta o el cartucho de tóner se disponen y reemplazan al final de su vida útil o se reciclan y reutilizan.

En otra realización, el componente reemplazable de la impresora 108 incluye un componente de impresión que se reemplaza fácilmente en el sistema de impresión 104. Los ejemplos de tal componente de impresión incluyen un cabezal de impresión que deposita de manera selectiva la tinta en el medio de impresión 118 en respuesta a las señales de control del controlador de la impresora 116 o un cartucho de impresora que incluye un cabezal de impresión y un suministro de tinta. Por lo tanto, el componente reemplazable de la impresora 108 puede incluir un contenedor de tinta, un cabezal de impresión o un cartucho de impresora si, por ejemplo, el sistema de impresión 104 incluye una impresora de inyección de tinta. Además, el componente reemplazable de la impresora 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 reemplazable de la impresora 108 puede incluir un dispositivo periférico del sistema de impresión 104, tal como una tarjeta Ethernet, un accesorio de impresión a doble cara, un finalizador de papel (por ejemplo, grapadora, perforadora, etc.) u otro dispositivo adecuado.

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

El componente reemplazable de la impresora 108 incluye un dispositivo de memoria 109 que almacena información para el componente reemplazable de la impresora 108 y/o el sistema de impresión 104. El dispositivo de memoria 109 incluye una memoria no volátil (NVM) 110 y lógica 111. En una realización, el dispositivo de memoria 109 es a prueba de manipulaciones o resistente a manipulaciones. En una realización, la lógica 111 es un circuito lógico o software incorporado que se ejecuta en un procesador. Por ejemplo, en una realización, el dispositivo de memoria 109 incluye una CPU o SoC con memoria no volátil incorporada 110. En otra realización, el dispositivo de memoria 109 incluye una CPU o SoC con memoria no volátil externa 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 no volátil 110 es una memoria no volátil de 256 bytes u otra memoria no volátil de tamaño adecuado, 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 reemplazable de

la impresora 108 y/o información que es aplicable al sistema de impresión 104. Además, la memoria no volátil 110 puede tener información que va a usarse 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 almacenarse en la memoria no volátil 110 incluye parámetros operativos y/o no operativos para el componente reemplazable de la impresora 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 reemplazable de la impresora 108 es genuino. Además, la memoria no volátil 110 almacena una o más claves secretas utilizadas para autenticar el componente reemplazable de la impresora 108. En una realización, la una o más claves secretas almacenadas en la memoria no volátil 110 del dispositivo de memoria 109 se derivan de 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 de memoria 122 se derivan de una o más claves secretas comunes. Como tal, la una o más claves secretas almacenadas en la memoria no volátil 110 se relacionan con la una o más claves secretas almacenadas en la memoria no volátil 123.

En una realización, el componente reemplazable de la impresora 108 incluye un enlace de comunicación 112 que acopla eléctricamente o acopla comunicativamente el dispositivo de memoria 109 con el enlace de comunicación 114 y, por lo tanto, con el controlador de la impresora 116 cuando el componente reemplazable de la impresora 108 se instala en el sistema de impresión 104. Como tal, cuando el componente reemplazable de la impresora 108 se instala en el sistema de impresión 104, el dispositivo de memoria 109 se comunica con el controlador de la impresora 116 a través de los 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 o terminales que se acoplan con los nodos o receptáculos eléctricos correspondientes, respectivamente.

El componente reemplazable de la impresora 108 se autentica mediante la autenticación de una comunicación entre el controlador de la impresora 116 y el dispositivo de memoria 109 mediante el uso de claves de sesión. Para generar una clave de sesión, el controlador de la 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 de un identificador de clave de sesión. Por lo tanto, cada identificador de clave de sesión y cada clave de sesión asociada se usa solo una vez. El circuito lógico 111 proporciona el identificador de clave de sesión generado al controlador de la 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 reemplazable de la impresora 108. En 152, se instala un componente reemplazable de la impresora 108 en un sistema de impresión 104 que incluye un controlador de la impresora 116. El componente reemplazable de la impresora 108 incluye un dispositivo de memoria 109 que se ha configurado con una o más claves secretas para autenticar el componente reemplazable de la impresora 108. El sistema de impresión 104 también incluye un dispositivo de memoria 122 que se ha configurado con una o más claves secretas para autenticar el componente reemplazable de la impresora 108.

En 154, el controlador de la impresora 116 solicita un identificador de clave de sesión del dispositivo de memoria 109 del componente reemplazable de la impresora 108 a través de los enlaces de comunicación 114 y 112. En una realización, el controlador de la impresora 116 usa una comprobación aleatoria al solicitar el identificador de clave de sesión para evitar ataques de reproducción contra el controlador de la 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 en base a 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 la impresora 116.

En 160, el controlador de la impresora 116 proporciona el identificador de clave de sesión recibido del 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 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 se relaciona 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 circuito lógico 124. En 164, el circuito lógico 124 del dispositivo de memoria 122 proporciona la clave de sesión solicitada al controlador de la impresora 116. En 166, el controlador de la impresora 116 usa la clave de sesión recibida para determinar la autenticidad del componente reemplazable de la impresora 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 reemplazable de la impresora 108. En 170, con una clave de sesión establecida en el dispositivo de memoria 109 del componente reemplazable de la impresora 108 y con una clave de sesión establecida en el sistema de impresión 104, el controlador de la impresora 116 calcula un primer código de autenticación de mensaje (MAC) para una solicitud de lectura mediante el uso de su clave de sesión y un algoritmo criptográfico adecuado. La solicitud de lectura es para un campo de datos de memoria no volátil 110 que almacena un valor que indica si el componente reemplazable de la impresora 108 es genuino. El primer MAC se calcula sobre el comando y los parámetros del comando de la solicitud de lectura.

En una realización, el primer MAC se calcula en base a un código de autenticación de mensaje basado en 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 bloque de cifrado como la norma de cifrado de datos (DES), 3DES, la norma de cifrado avanzado (AES), el cifrado Rivest dos (RC2) u otro algoritmo de cifrado de bloques adecuado. En otras realizaciones, el primer MAC se calcula mediante el uso de otra técnica adecuada.

En 172, el controlador de la impresora 116 emite la solicitud de lectura que incluye el primer MAC al dispositivo de memoria 109 del componente reemplazable de la impresora 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 mediante el uso de 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 la impresora 116 no se autentica. En 182, el circuito lógico 111 del dispositivo de memoria 109 aborta o niega la operación de lectura solicitada. Al negar la operación de lectura solicitada, el componente reemplazable de la impresora 108 ha determinado que el controlador de la impresora 116 no se autentica. Por lo tanto, el componente reemplazable de la impresora 108 no se comunica con el controlador de la impresora 116. En 184, el circuito lógico 111 del dispositivo de memoria 109 marca su clave de sesión como inválida, de manera que no puede usarse 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 la impresora 116 se autentica. 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 reemplazable de la impresora 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 reemplazable de la impresora 108. En 186, el dispositivo de memoria 109 calcula un tercer MAC para la respuesta mediante el uso de 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 la impresora 116. En 190, en respuesta a la respuesta del dispositivo de memoria 109, el controlador de la impresora 116 calcula un cuarto MAC para la respuesta recibida mediante el uso de su clave de sesión y el algoritmo criptográfico. En 192, el controlador de la 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 la impresora 116 y el dispositivo de memoria 109 no se autentica. Por lo tanto, en 198 el controlador de la impresora 116 determina que el componente reemplazable de la impresora 108 no se autentica.

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 la impresora 116 y el dispositivo de memoria 109 se autentica. Dado que la comunicación entre el dispositivo de memoria 109 y el controlador de la impresora 116 se ha autenticado, el controlador de la impresora 116 puede confiar en el valor devuelto en respuesta a la solicitud de lectura. Por lo tanto, en 196 el controlador de la impresora 116 determina que el componente reemplazable de la impresora 108 se autentica.

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

Aunque en este documento se han ilustrado y descrito las realizaciones específicas, los expertos en la técnica apreciarán que una variedad de implementaciones alternativas y/o equivalentes pueden sustituirse por las realizaciones específicas mostradas y descritas, sin apartarse del alcance de la presente invención. Esta solicitud está destinada a cubrir cualquiera de las adaptaciones o variaciones de las realizaciones específicas descritas en este documento. Por lo tanto, se pretende que esta invención esté limitada solo por las reivindicaciones y sus equivalentes.

REIVINDICACIONES

1. Un sistema de impresión (104) que comprende:
un controlador de la impresora (116) y un dispositivo de memoria (122) que comprende un circuito lógico, el dispositivo de memoria que almacena una clave secreta y se enlaza comunicativamente al controlador de la impresora (116); en el que:
el controlador de la impresora (116) se configura para determinar la autenticidad de un componente reemplazable de la impresora (108) basado en la clave secreta almacenada;
el circuito lógico (124) del dispositivo de memoria (122) se configura para generar una clave de sesión basada en un identificador de clave de sesión recibido del componente reemplazable de la impresora (108) y la clave secreta almacenada, en el que el componente reemplazable de la impresora (108) se configura para generar un identificador de clave de sesión y una clave de sesión diferentes en respuesta a cada solicitud del sistema de impresión;
en donde el controlador de la impresora (116) se configura además para:
emitir una solicitud de lectura al componente reemplazable de la impresora (108), la solicitud de lectura incluye un código de autenticación de mensaje, MAC, generado mediante el uso de la clave de sesión generada y un algoritmo criptográfico y se comunica a un dispositivo de memoria (109) del componente reemplazable de la impresora (108);
y autenticar una respuesta del componente reemplazable de la impresora (108), en el que una respuesta recibida del componente reemplazable (108) comprende un MAC, y
en el que autenticar la respuesta comprende:
calcular un MAC para la respuesta recibida mediante el uso de la clave de sesión generada y el algoritmo criptográfico;
comparar el MAC calculado con el MAC recibido; y autenticar la comunicación entre el controlador de la impresora (116) y el dispositivo de memoria (109) del componente reemplazable de la impresora (108) si el MAC calculado coincide con el MAC recibido; y en el que la clave de sesión generada por el componente reemplazable de la impresora (108) coincide con la clave de sesión generada en base al identificador de clave de sesión.

2. Un sistema de impresión de acuerdo con la reivindicación 1, en el que el controlador de la impresora (116) se configura para solicitar el identificador de clave de sesión desde el dispositivo de memoria (109) del componente reemplazable de la impresora (108).

3. Un sistema de impresión de acuerdo con la reivindicación 2, en el que el controlador de la impresora (116) se configura para solicitar el identificador de clave de sesión desde el dispositivo de memoria (109) del componente reemplazable de la impresora (108) mediante el uso de una comprobación aleatoria.

4. Un sistema de impresión de acuerdo con cualquiera de las reivindicaciones anteriores, en el que el sistema de impresión (104) comprende un enlace de comunicación (112, 114) y el controlador de la impresora (116) debe comunicarse con el componente reemplazable de la impresora (108) a través del enlace de comunicación.

5. Un sistema de impresión de acuerdo con cualquier reivindicación anterior en el que la solicitud de lectura es una solicitud de lectura para un valor de datos que indica la autenticidad de un componente reemplazable de la impresora (108).

6. Un método para autenticar un componente reemplazable de la impresora que comprende:
solicitar, mediante un controlador de la impresora (116) de un sistema de impresión (108) en el que se instala un componente reemplazable de la impresora (108), un identificador de clave de sesión desde un circuito lógico (111) de un dispositivo de memoria (109) del componente reemplazable de la impresora (108), que genera, mediante el circuito lógico (111), una clave de sesión y un identificador de clave de sesión, en el que la clave de sesión se genera en base a una primera clave secreta almacenada dentro de un dispositivo de memoria no volátil (110) del componente reemplazable de la impresora (108), en el que se genera un identificador de clave de sesión y una clave de sesión diferentes en respuesta a cada solicitud del sistema de impresión (108); proporcionar el identificador de clave de sesión al controlador de la impresora (116) del sistema de impresión (104), mediante el uso del identificador de clave de sesión y una clave secreta almacenada, que genera, mediante un circuito lógico (124) de un dispositivo de memoria (122) del sistema de impresión (104), una clave de sesión;
emitir, por el controlador de la impresora (116) del sistema de impresión (104), una solicitud de lectura al dispositivo de memoria (109) del componente reemplazable de la impresora (108), la solicitud de lectura incluye un código de autenticación de mensaje, MAC, generado mediante el uso de la clave de sesión generada y un algoritmo criptográfico;
determinar, mediante el circuito lógico (111) del dispositivo de memoria (109) del componente reemplazable de la impresora (108), una respuesta a la solicitud de lectura que comprende un MAC, el MAC se ha calculado por el circuito lógico (111) del dispositivo de memoria (109) del componente reemplazable de la impresora (108) mediante el uso de su clave de sesión y el algoritmo criptográfico;
calcular, mediante el controlador de la impresora (116) del sistema de impresión (104), un MAC para una respuesta recibida a la solicitud de lectura mediante el uso de la clave de sesión generada y el algoritmo criptográfico;
comparar, mediante el controlador de la impresora (116) del sistema de impresión (104), el MAC calculado para la respuesta recibida y el MAC recibido con la respuesta; y autenticar la comunicación entre el sistema de impresión

(104) y el dispositivo de memoria (109) del componente reemplazable de la impresora (108) si el MAC calculado para la respuesta recibida coincide con el MAC recibido con la respuesta; y
en donde la clave de sesión generada por el circuito lógico (111) del dispositivo de memoria (109) del componente reemplazable de la impresora (108) coincide con la clave de sesión generada en base al identificador de clave de sesión.

7. Un método de acuerdo con la reivindicación 6 en el que el MAC emitido con la solicitud de lectura se calcula sobre el comando y los parámetros del comando de la solicitud de lectura.

8. Un método de acuerdo con la reivindicación 7 en el que el MAC determinado por el circuito lógico (111) del componente reemplazable de la impresora (108) se calcula sobre el MAC emitido con la solicitud de lectura y los datos de respuesta.

9. Un método de acuerdo con cualquiera de las reivindicaciones 6 a 8, que comprende generar, mediante el circuito lógico (111), una clave de sesión diferente y un identificador de clave de sesión en respuesta a cada una de una pluralidad de solicitudes.

10. Un dispositivo de memoria (109) para un componente reemplazable de la impresora (108) que comprende:
un circuito lógico (111); y
una memoria no volátil (110) que almacena una o más claves secretas para su uso en la autenticación del componente reemplazable de la impresora (108) por un sistema de impresión (104) en el que se instala, en el que el circuito lógico (111) se configura para, en la autenticación del componente reemplazable de la impresora (108) por el sistema de impresión (104):
generar, en respuesta a una solicitud de un controlador de la impresora (116) del sistema de impresión (104), un identificador de clave de sesión y una clave de sesión asociada basada en una de dichas claves secretas y proporcionar el identificador de clave de sesión al sistema de impresión (104), en el que el circuito lógico (111) se configura para generar un identificador de clave de sesión diferente y una clave de sesión asociada en respuesta a cada solicitud del sistema de impresión;
recibir, desde el controlador de la impresora (116), una solicitud de lectura, la solicitud de lectura que incluye un código de autenticación de mensaje, MAC, generado mediante el uso de una clave de sesión basada en el identificador de clave de sesión; y
proporcionar una respuesta a la solicitud de lectura que incluye un MAC calculado mediante el uso de la clave de sesión generada por el circuito lógico y un algoritmo criptográfico; en donde la clave de sesión generada por el circuito lógico (111) coincide con la clave de sesión generada en base al identificador de clave de sesión.

11. Un dispositivo de memoria de acuerdo con la reivindicación 10 en el que el circuito lógico (111) se configura para calcular el MAC incluido con la respuesta sobre el MAC emitido con la solicitud de lectura y los datos de respuesta.

12. Un dispositivo de memoria de acuerdo con la reivindicación 10 u 11, en el que la solicitud de lectura es una solicitud de lectura para un valor de datos que indica la autenticidad de un componente reemplazable de la impresora (108).

13. Un dispositivo de memoria (109) de acuerdo con cualquiera de las reivindicaciones 10 a 12 en el que el circuito lógico (111) es para:
calcular un MAC en respuesta a la solicitud de lectura mediante el uso de la clave de sesión y un algoritmo criptográfico;
comparar el MAC recibido con el MAC calculado; y
abortar o denegar una operación de lectura y marcar la clave de sesión como inválida si el MAC recibido no coincide con el MAC calculado.

14. El dispositivo de memoria (109) de acuerdo con cualquiera de las reivindicaciones 10 a 13, en el que el dispositivo de memoria (109) es resistente a la manipulación.

15. El dispositivo de memoria (109) de acuerdo con cualquiera de las reivindicaciones 10 a 14, en el que al menos una de las una o más claves secretas se deriva de una clave secreta del sistema de impresión (104).

16. Un componente reemplazable de la impresora (108) **caracterizado por**:
un dispositivo de memoria (109) como se describe en cualquiera de las reivindicaciones 10 a 15; y
un enlace de comunicación (112) que comprende conexiones eléctricas y configurado para enlazar comunicativamente el dispositivo de memoria (109) a un controlador de la impresora (116) de un sistema de impresión (104) en el que se instala el componente reemplazable de la impresora (108).

17. El componente reemplazable de la impresora (108) de la reivindicación 16, en el que el componente reemplazable de la impresora (108) 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.

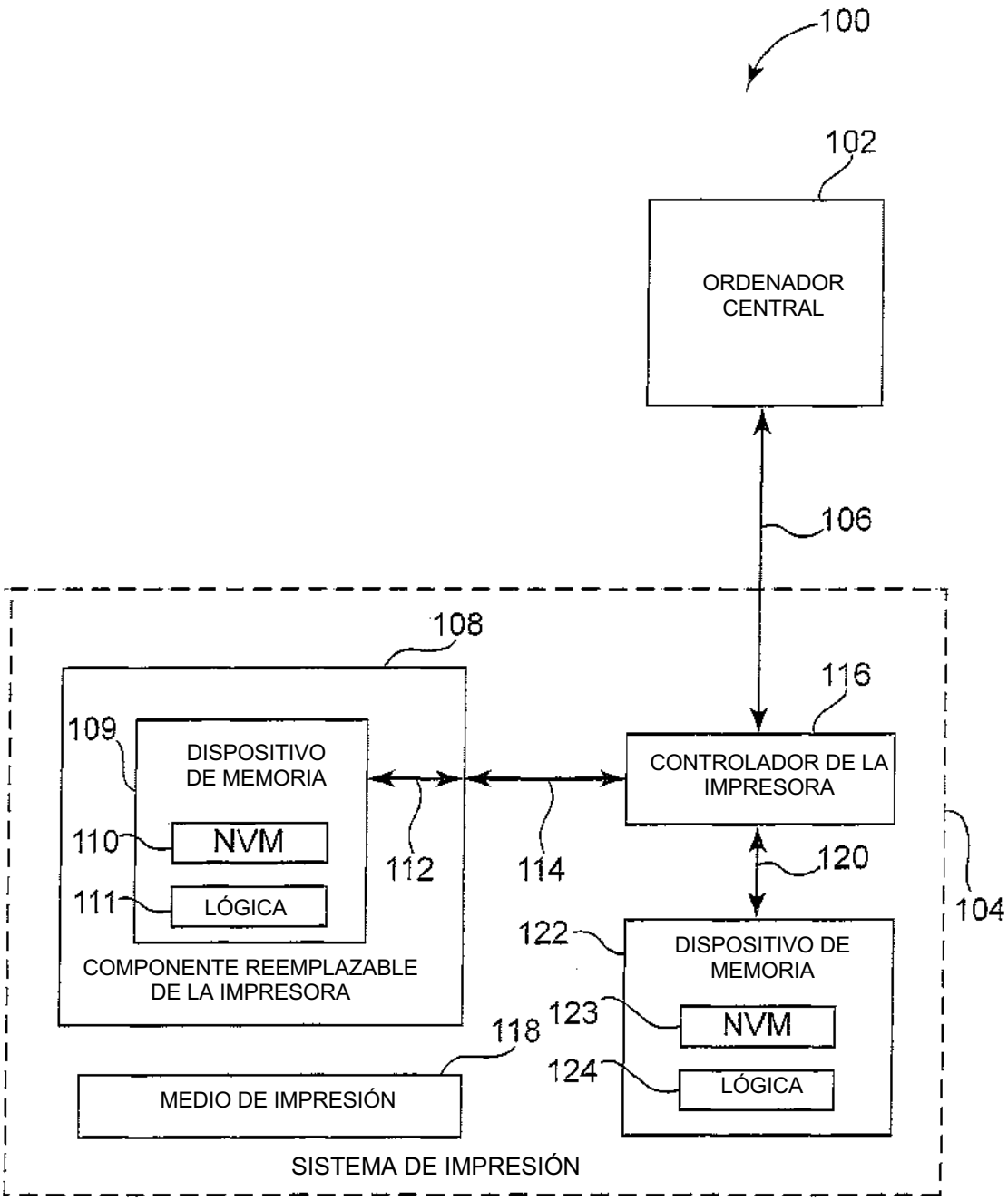
100
102
ORDENADOR CENTRAL
106
108
116
109
DISPOSITIVO DE MEMORIA
110
NVM
111
LÓGICA
112
114
CONTROLADOR DE LA IMPRESORA
120
104
122
DISPOSITIVO DE MEMORIA
123
NVM
124
LÓGICA
COMPONENTE REEMPLAZABLE DE LA IMPRESORA
118
MEDIO DE IMPRESIÓN
SISTEMA DE IMPRESIÓN

Figura 1

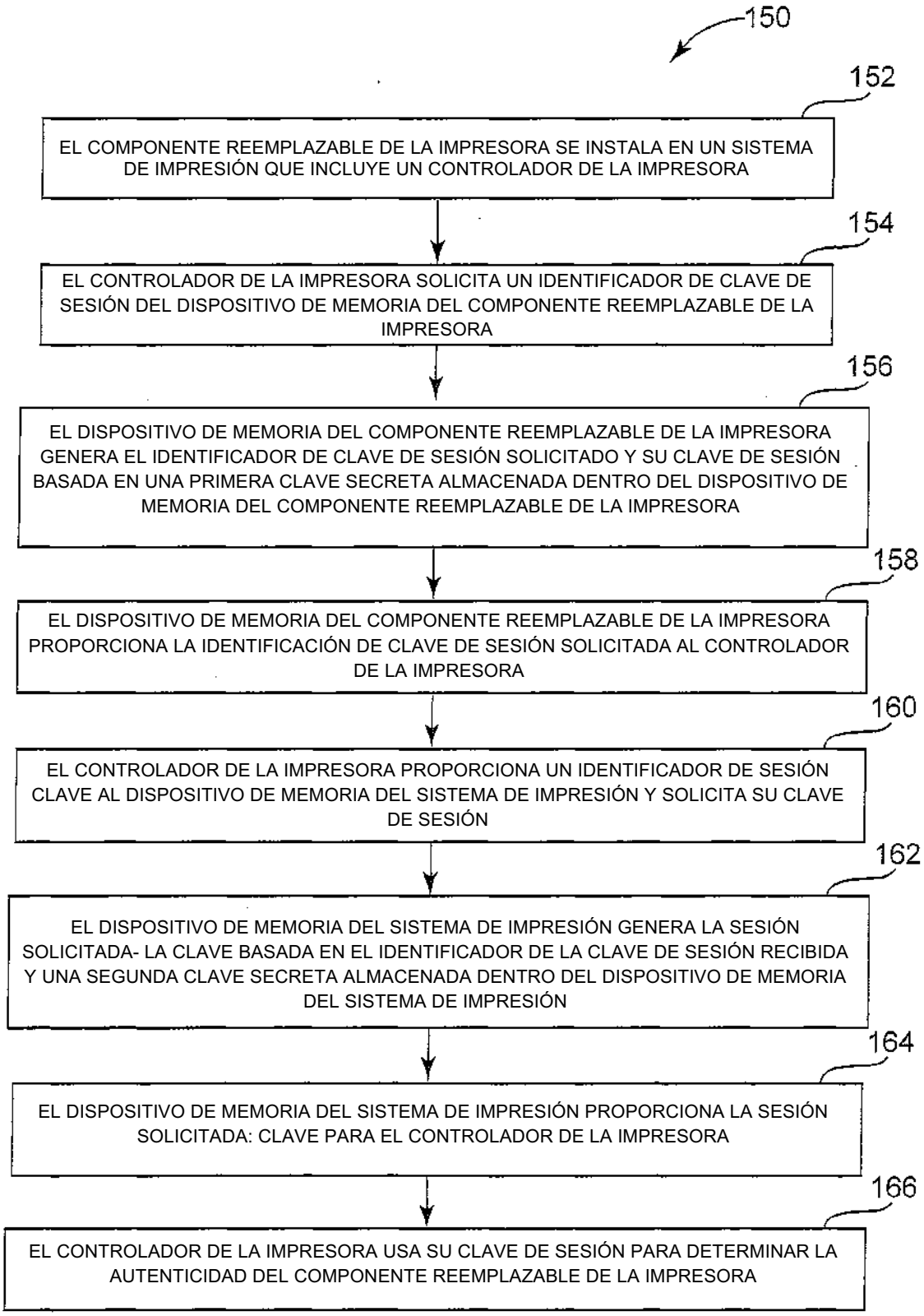
150
152
EL COMPONENTE REEMPLAZABLE DE LA IMPRESORA SE INSTALA EN UN SISTEMA DE IMPRESIÓN QUE INCLUYE UN CONTROLADOR DE LA IMPRESORA
154
EL CONTROLADOR DE LA IMPRESORA SOLICITA UN IDENTIFICADOR DE CLAVE DE SESIÓN DEL DISPOSITIVO DE MEMORIA DEL COMPONENTE REEMPLAZABLE DE LA IMPRESORA
156
EL DISPOSITIVO DE MEMORIA DEL COMPONENTE REEMPLAZABLE DE LA IMPRESORA GENERA EL IDENTIFICADOR DE CLAVE DE SESIÓN SOLICITADO Y SU CLAVE DE SESIÓN BASADA EN UNA PRIMERA CLAVE SECRETA ALMACENADA DENTRO DEL DISPOSITIVO DE MEMORIA DEL COMPONENTE REEMPLAZABLE DE LA IMPRESORA
158
EL DISPOSITIVO DE MEMORIA DEL COMPONENTE REEMPLAZABLE DE LA IMPRESORA PROPORCIONA LA IDENTIFICACIÓN DE CLAVE DE SESIÓN SOLICITADA AL CONTROLADOR DE LA IMPRESORA
160
EL CONTROLADOR DE LA IMPRESORA PROPORCIONA UN IDENTIFICADOR DE SESIÓN CLAVE 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 SESIÓN SOLICITADA- LA CLAVE BASADA EN EL IDENTIFICADOR DE LA CLAVE DE SESIÓN RECIBIDA Y UNA SEGUNDA CLAVE SECRETA ALMACENADA DENTRO DEL DISPOSITIVO DE MEMORIA DEL SISTEMA DE IMPRESIÓN
164
EL DISPOSITIVO DE MEMORIA DEL SISTEMA DE IMPRESIÓN PROPORCIONA LA SESIÓN SOLICITADA: CLAVE PARA EL CONTROLADOR DE LA IMPRESORA
166
EL CONTROLADOR DE LA IMPRESORA USA SU CLAVE DE SESIÓN PARA DETERMINAR LA AUTENTICIDAD DEL COMPONENTE REEMPLAZABLE DE LA IMPRESORA

Figura 2

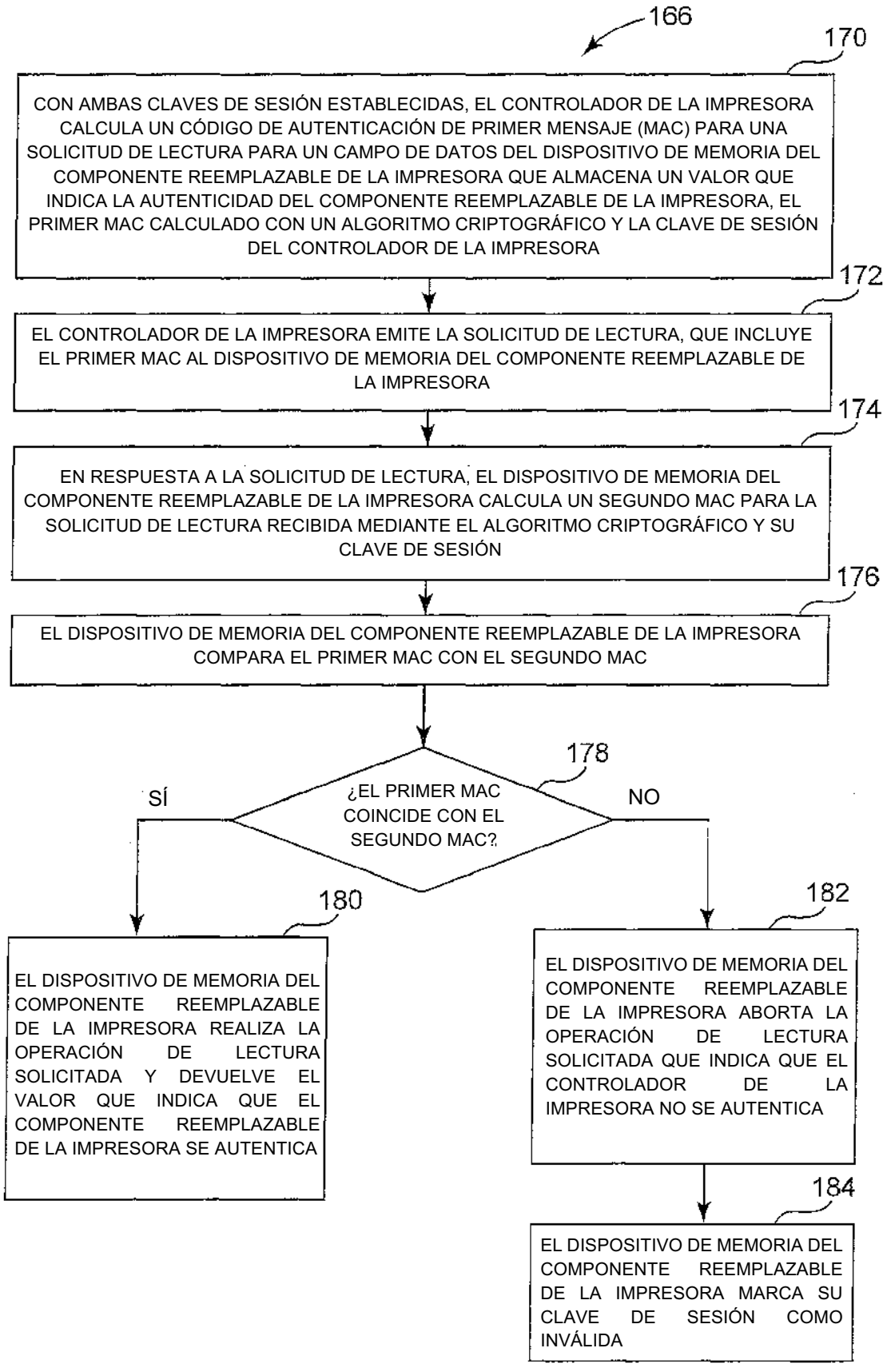
166
170
CON AMBAS CLAVES DE SESIÓN ESTABLECIDAS, EL CONTROLADOR DE LA IMPRESORA CALCULA UN CÓDIGO DE AUTENTICACIÓN DE PRIMER MENSAJE (MAC) PARA UNA SOLICITUD DE LECTURA PARA UN CAMPO DE DATOS DEL DISPOSITIVO DE MEMORIA DEL COMPONENTE REEMPLAZABLE DE LA IMPRESORA QUE ALMACENA UN VALOR QUE INDICA LA AUTENTICIDAD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

Figura 3

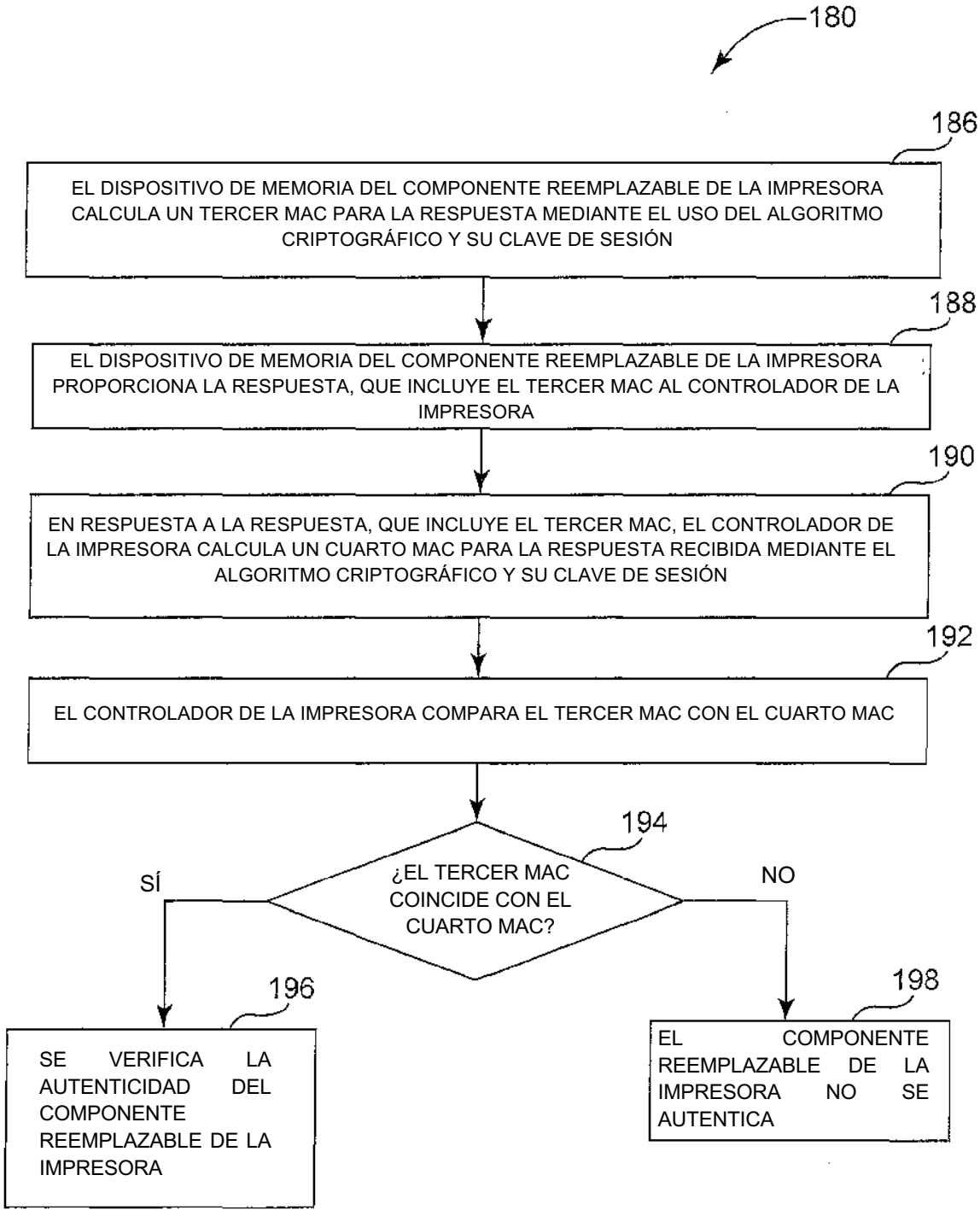
180
186
EL DISPOSITIVO DE MEMORIA DEL COMPONENTE REEMPLAZABLE DE LA IMPRESORA CALCULA UN TERCER MAC PARA LA RESPUESTA MEDIANTE EL USO DEL ALGORITMO CRIPTOGRÁFICO Y SU CLAVE DE SESIÓN
188
EL DISPOSITIVO DE MEMORIA DEL COMPONENTE REEMPLAZABLE DE LA IMPRESORA PROPORCIONA LA RESPUESTA, QUE INCLUYE EL TERCER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

Figura 4