(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 693 448**

(51) Int. CI.:

B41J 2/175 (2006.01)
H04W 12/06 (2009.01)
G06F 21/44 (2013.01)
G06F 7/58 (2006.01)
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.08.2013 E 17170486 (9)**

(97) Fecha y número de publicación de la concesión europea: **03.10.2018 EP 3231617**

(54) Título: **Autenticación de suministro de a través de respuesta al desafío de temporización**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.12.2018

(73) Titular/es:

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

(72) Inventor/es:

WARD, JEFFERSON P. y
PANSHIN, STEPHEN D.

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Autenticación de suministro de a través de respuesta al desafío de temporización

Antecedentes

Muchos sistemas tienen componentes sustituibles que son integrales al funcionamiento del sistema. Los componentes sustituibles a menudo son dispositivos que contienen material consumible que se agota con cada uso del sistema. Tales sistemas pueden incluir, por ejemplo, teléfonos celulares que usan baterías sustituibles, sistemas médicos que dispensan medicinas desde dispositivos de administración sustituibles, sistemas de impresión que dispensan fluidos (por ejemplo, tinta) o tóner desde cartuchos de suministro sustituibles, etc. Verificar que un dispositivo de suministro sustituible es un dispositivo auténtico de un fabricante legítimo puede ayudar a un usuario de sistema a evitar problemas asociados con el uso no intencionado de un dispositivo defectuoso y/o falsificado.

Breve descripción de los dibujos

Las presentes realizaciones se describirán ahora, a modo de ejemplo, con referencia a los dibujos anexos, en los que:

la FIG. 1 muestra un diagrama de cajas que ilustra componentes de un sistema de autenticación ejemplo, genérico, adecuado para autenticar un dispositivo de suministro sustituible;

la FIG. 2 muestra un ejemplo de datos de caracterización almacenados en un dispositivo de suministro sustituible;

la FIG. 3 muestra un ejemplo de un sistema de autenticación encarnado como un sistema de impresión de chorro de tinta;

la FIG. 4 muestra una vista en perspectiva de un cartucho de suministro de impresión de chorro de tinta ejemplo;

la FIG. 5 muestra un diagrama de flujo de un proceso de autenticación de suministro ejemplo.

En todos los dibujos, números de referencia idénticos designan elementos similares, pero no necesariamente idénticos.

Descripción detallada

Visión general

Como se señaló anteriormente, verificar la autenticidad de dispositivos de suministro sustituibles para uso en ciertos sistemas puede ayudar a los usuarios de sistemas a evitar problemas asociados con el uso no intencionado de dispositivos defectuosos y/o falsificados. Por ejemplo, en sistemas de impresión que emplean cartuchos de tóner o de tinta consumibles, sustituir inadvertidamente los cartuchos con cartuchos falsificados puede provocar diversos problemas que varían desde impresiones de escasa calidad a cartuchos con fugas que pueden dañar el sistema de impresión.

Los métodos anteriores de autenticación de un dispositivo sustituible han incluido emplear autenticación fuerte que implica el uso de una clave secreta conocida por una tarjeta inteligente o un microcontrolador seguro en el dispositivo sustituible (por ejemplo, un cartucho de tinta/tóner consumible) y el dispositivo anfitrión (por ejemplo, una impresora). Si el dispositivo sustituible puede proporcionar una respuesta a un desafío emitido por el anfitrión que demuestra que contiene una clave adecuada, el anfitrión deducirá que el dispositivo es de fabricación original, y entonces autenticará el dispositivo (véase el documento US2012/0221863) . Una debilidad con este método de autenticación es que se basa en la capacidad del sistema de preservar la clave secreta. Si un atacante puede recuperar una clave o claves o bien a partir del anfitrión o bien a partir del dispositivo sustituible, puede almacenar la(s) clave(s) robada(s) en una tarjeta inteligente o un microcontrolador, permitiéndole crear entonces dispositivos sustituibles que responderán a desafíos como si esos dispositivos fueran dispositivos auténticos del fabricante original. Típicamente, una vez que se compromete(n) la(s) clave(s), la respuesta al desafío y otra funcionalidad de un dispositivo sustituible no auténtico (es decir, falsificado) se puede simular con un microprograma que se ejecuta en un microcontrolador barato, estándar.

Se describen en la presente memoria sistemas de autenticación y procesos de autenticación de suministro que proporcionan autenticación robusta de dispositivos de sistema sustituibles, en general, a través de una respuesta al desafío de temporización. Un anfitrión, tal como una impresora, emite un desafío de temporización criptográfico a un microcontrolador seguro fijado a un dispositivo sustituible, tal como un cartucho de tinta o tóner consumible. El desafío requiere que el dispositivo consumible (es decir, el microcontrolador en el dispositivo consumible) realice una serie de operaciones matemáticas en base a datos suministrados por el anfitrión/impresora. La impresora monitoriza la cantidad de tiempo que tarda el dispositivo consumible en completar la tarea, y verifica independientemente la respuesta proporcionada por el dispositivo. Si la respuesta y el tiempo transcurrido mientras que se calcula la respuesta cumplen ambos las expectativas de la impresora, la impresora concluirá que el dispositivo es un dispositivo auténtico. Si o bien la respuesta, o bien el tiempo transcurrido mientras que se calcula la respuesta (o ambos), no cumplen las expectativas de la impresora, la impresora concluirá que el dispositivo no es un dispositivo auténtico.

Las operaciones matemáticas a partir del desafío se realizan dentro del microcontrolador del dispositivo consumible mediante lógica de hardware dedicada diseñada específicamente para tales operaciones. La lógica dedicada es capaz de lograr la respuesta al desafío realizando los cálculos matemáticos significativamente más rápido que se podría lograr de otro modo por un microcontrolador estándar que ejecuta un microprograma. De esta manera, un dispositivo sustituible no auténtico/falsificado en el que un microcontrolador contiene una(s) clave(s) robada(s), puede ser capaz de lograr una respuesta al desafío correcta. No obstante, tal dispositivo falsificado no es capaz de lograr la respuesta al desafío dentro de una trama de tiempo esperada por el dispositivo anfitrión.

En una implementación ejemplo, un cartucho de suministro de impresión incluye un microcontrolador para recibir un desafío de temporización y habilitar una autenticación del cartucho proporcionando una respuesta al desafío en un tiempo de respuesta al desafío que cae dentro de una ventana de tiempo esperado. En otra implementación, el cartucho además incluye lógica de hardware dedicada en el microcontrolador para realizar un cálculo matemático en respuesta al desafío de temporización. La realización del cálculo matemático produce la respuesta al desafío dentro de la ventana de tiempo esperado.

En otra implementación ejemplo, un dispositivo de suministro sustituible incluye un microcontrolador. El microcontrolador es para derivar una clave de sesión con un dispositivo anfitrión y para recibir un desafío dependiente del tiempo desde el dispositivo anfitrión que especifica una semilla aleatoria, la clave de sesión, y un ciclo de cálculo. El dispositivo sustituible incluye además una lógica dedicada dentro del microcontrolador para realizar un cálculo de desafío un número de veces igual al ciclo de cálculo, en donde un primer cálculo usa la semilla aleatoria y la clave de sesión para producir una salida, y cada cálculo posterior usa una salida de un cálculo precedente.

En otra implementación ejemplo, un sistema de autenticación incluye un dispositivo anfitrión, un controlador integrado en el dispositivo anfitrión y un algoritmo de autenticación ejecutable en el controlador para emitir un desafío de temporización criptográfico y para autenticar el dispositivo de suministro cuando el dispositivo de suministro proporciona una respuesta al desafío en un tiempo de respuesta al desafío que cae dentro de una ventana de tiempo esperado.

En otra implementación ejemplo, un sistema de autenticación incluye una impresora que tiene un controlador y una memoria. El sistema de autenticación también incluye un algoritmo de autenticación almacenado en la memoria y ejecutable en el controlador para emitir un desafío de temporización criptográfico y para autenticar un cartucho de suministro de impresión cuando el cartucho proporciona una respuesta al desafío que corresponde a una respuesta esperada dentro de una ventana de tiempo esperado.

En otra implementación ejemplo, un medio no transitorio legible por procesador almacena instrucciones de representación de código que cuando se ejecutan por un procesador hacen que el procesador reconozca un dispositivo de suministro, y emita un desafío de temporización criptográfico al dispositivo de suministro. El desafío de temporización solicita que sea realizado un cálculo matemático sobre datos que incluyen una clave de sesión, una semilla aleatoria, y un recuento de cálculo. Las instrucciones además hacen que el procesador reciba una respuesta al desafío en un tiempo de respuesta al desafío desde el dispositivo de suministro, y autentique el dispositivo de suministro cuando la respuesta al desafío coincida con una respuesta esperada y el tiempo de respuesta al desafío caiga dentro de una ventana de tiempo esperado.

Implementaciones ejemplo

La FIG. 1 muestra un diagrama de cajas que ilustra componentes de un sistema 100 de autenticación genérico, ejemplo, adecuado para autenticar un dispositivo de suministro sustituible. El sistema 100 de autenticación incluye un dispositivo 102 anfitrión y un dispositivo 104 de suministro sustituible. El dispositivo 102 anfitrión incluye un controlador 106 que típicamente incluye componentes de un sistema de cálculo estándar tal como un procesador (CPU) 108, una memoria 110, microprograma, y otra electrónica para controlar las funciones generales del sistema 100 de autenticación y para comunicarse con y controlar el dispositivo 104 de suministro. La memoria 110 puede incluir componentes de memoria volátiles (es decir, RAM) y no volátiles (por ejemplo, ROM, disco duro, disco flexible, CD-ROM, etc.) que comprenden medios no transitorios legibles por ordenador/por procesador que proporcionan el almacenamiento de instrucciones y/o datos codificados legibles por ordenador/procesador, en forma de algoritmos, módulos de programa, estructuras de datos, JDF, etc. El dispositivo 104 de suministro comprende un microcontrolador 112 (es decir, una tarjeta inteligente) que incluye también un procesador (CPU) 114 y una memoria 116.

En general, al encender el dispositivo 102 anfitrión, el dispositivo 102 anfitrión y el dispositivo 104 de suministro establecen comunicaciones seguras a través de técnicas criptográficas estándar usando algoritmos 118 criptográficos estándar. Por ejemplo, ejecutando un algoritmo 118 criptográfico (es decir, en el procesador 108), el dispositivo 102 anfitrión puede solicitar el ID 120 único del dispositivo 104 de suministro y determinar la “clave de base” 122 del dispositivo a través de una relación criptográfica. Usando la clave de base 122, el dispositivo anfitrión y el dispositivo de suministro pueden derivar una “clave de sesión” 124 secreta que permite una comunicación segura para un intercambio de comunicación actual. El dispositivo 102 anfitrión determina la clave de base 122 de esta manera cada vez que se enciende, y cada vez que se instala un nuevo dispositivo 104 de suministro. La clave

de base 122 permanece igual y no cambia. No obstante, se deriva una clave de sesión 124 nueva y diferente cada vez que se hace un intercambio de comunicación entre el dispositivo 102 anfitrión y el dispositivo 104 de suministro.

En una implementación, la memoria 110 incluye un algoritmo 126 de autenticación ejecutable sobre el procesador 108 del controlador 106 para determinar la autenticidad del dispositivo 104 de suministro sustituible. El dispositivo 104 de suministro se determina que es auténtico cuando responde correctamente a un desafío 128 de temporización criptográfico emitido por el algoritmo 126 de autenticación, y cuando su respuesta 130 al desafío se completa dentro de una ventana de tiempo esperado. De esta manera, un dispositivo 104 de suministro cuyo valor de respuesta 130 al desafío es correcto, pero cuyo tiempo 131 de respuesta al desafío no cae dentro de una ventana de tiempo esperado, se determina que no es auténtico. Del mismo modo, un dispositivo 104 de suministro cuyo tiempo 131 de respuesta al desafío cae dentro de una ventana de tiempo esperado pero cuyo valor de respuesta 130 al desafío es incorrecto, se determina que no es auténtico. La autenticidad del dispositivo 104 de suministro, por lo tanto, depende de que proporcione una respuesta 130 correcta a un desafío 128 de temporización criptográfico en un tiempo 131 de respuesta al desafío (es decir, el tiempo que tarda en proporcionar la respuesta 130) que cae dentro de una ventana de tiempo esperado.

El desafío 128 de temporización criptográfico emitido por el algoritmo 126 de autenticación en el dispositivo 102 anfitrión comprende una solicitud para realizar un cálculo matemático específico que incorpora ciertos parámetros de desafío. El cálculo matemático ha de ser realizado un número particular de veces. El desafío 128 de temporización criptográfico incluye o está acompañado por estos parámetros de desafío, que incluyen la clave de sesión derivada, un número de semilla aleatoria generado en el dispositivo 102 anfitrión por el controlador 106, y un recuento o ciclo de cálculo que indica el número de veces que ha de ser realizado el cálculo. El cálculo matemático usa la clave de sesión y comienza con una operación en el número de semilla aleatorio. El resultado o salida de cada cálculo se vuelve a alimentar repetidamente al siguiente cálculo hasta que se haya alcanzado el recuento de cálculo. El último resultado o salida del cálculo matemático proporciona la respuesta 130 al desafío, que se habrá logrado o calculado en un tiempo 131 de respuesta al desafío particular. El tiempo 131 de respuesta al desafío se mide mediante el algoritmo 126 de autenticación, por ejemplo, iniciando una secuencia de temporización cuando se emite el desafío, y deteniendo la secuencia de temporización una vez que el dispositivo 104 de suministro se completa y devuelva la respuesta 130 al desafío al dispositivo 102 anfitrión. El tiempo 131 de respuesta al desafío es un valor temporal que en algunas implementaciones puede residir brevemente en el dispositivo 102 anfitrión en un componente volátil de la memoria 110 y/o dentro del procesador 108 anterior a o durante una comparación con una ventana de tiempo determinada por el anfitrión. El algoritmo 126 de autenticación en el anfitrión 102 determina si la respuesta 130 al desafío y el tiempo 131 de respuesta al desafío son correctos (es decir, esperados) o no, y entonces autentica el dispositivo 104 de suministro, en consecuencia.

Con referencia todavía a la FIG. 1, el microcontrolador 112 en el dispositivo 104 de suministro comprende una lógica 132 de desafío de hardware dedicada para realizar el cálculo matemático a partir de un desafío 128 de temporización criptográfico. La lógica 132 de desafío dedicada se diseña y fabrica específicamente en el microcontrolador 112 para realizar óptimamente el cálculo matemático particular. En una implementación ejemplo, el cálculo matemático comprende una función básica que define una secuencia de operaciones optimizada para ejecutarse muy rápido en la lógica 132 dedicada. El cálculo matemático, o función, se itera muchas veces con la salida de cada iteración que es parte de la entrada a la siguiente iteración. De esta manera, aunque uno o más operandos cambian con cada iteración del cálculo matemático, el cálculo matemático en sí mismo no cambia. Además, los valores de parámetros de desafío que acompañan al desafío 128 de temporización pueden cambiar con cada desafío 128 de temporización. Cada desafío 128 de temporización emitido por el algoritmo 126 de autenticación al dispositivo 104 de suministro puede tener diferentes valores para la clave de sesión, el número de semilla aleatoria generado en el dispositivo 102 anfitrión por el controlador 106, y el recuento o ciclo de cálculo. Por consiguiente, para cada desafío 128 de temporización, la respuesta 130 al desafío y el tiempo 131 de respuesta al desafío se determinan mediante los valores de parámetros de desafío. Más específicamente, la clave de sesión, la semilla aleatoria, y el recuento de cálculo afectan todos al valor de respuesta 130 al desafío, mientras que el recuento de cálculo también afecta al tiempo 131 de respuesta al desafío variando el número de iteraciones del cálculo matemático a través de la lógica 132 de desafío dedicada.

Como se señaló anteriormente, el algoritmo 126 de autenticación determina si la respuesta 130 al desafío y el tiempo 131 de respuesta al desafío, son correctos o esperados. Esto se hace comparando la respuesta 130 al desafío y el tiempo 131 de respuesta al desafío con valores correctos o esperados. En diferentes implementaciones, el algoritmo 126 determina los valores correctos o esperados de diferentes formas. En una implementación, por ejemplo, el algoritmo 126 recupera y accede a los datos 134 de caracterización almacenados en el dispositivo 104 de suministro. Los datos 134 de caracterización se pueden asegurar con una firma digital y verificar usando operaciones criptográficas estándar. Los datos 134 de caracterización proporcionan ventanas de tiempo esperadas en las que debería caer un tiempo 131 de respuesta al desafío dependiendo del recuento de cálculo proporcionado con el desafío 128 de temporización. De esta manera, en un ejemplo como se muestra en la FIG. 2, los datos 134 de caracterización pueden incluir una tabla de datos que asocia diferentes valores de recuento de cálculo con diferentes ventanas de tiempo. A modo de ejemplo solamente, tal asociación podría indicar que para un recuento de cálculo de 10.000 (es decir, donde el cálculo matemático ha de ser realizado 10.000 veces), se espera que el tiempo 131 de respuesta al desafío caiga dentro de una ventana de tiempo de 50 - 55 milisegundos. En otro ejemplo, los datos 134 de caracterización se podrían proporcionar a través de una relación matemática tal como la fórmula de intersección

de pendiente, y = mx + b. De esta manera, para un valor de recuento de cálculo dado, x, se puede determinar un tiempo esperado y. Una ventana de tiempo entonces se puede determinar por el algoritmo 126 de autenticación en el anfitrión 102, por ejemplo, usando el tiempo esperado y, +/- 5%.

En otra implementación ejemplo, el algoritmo 126 de autenticación determina los valores correctos o esperados para la respuesta 130 al desafío emitiendo el desafío 128 de temporización criptográfico a la lógica 136 de referencia dedicada en el controlador del dispositivo 106 anfitrión. La lógica 136 de referencia sobre el controlador 106 refleja la lógica 132 de hardware dedicada sobre el dispositivo 104 de suministro y, por lo tanto, se diseña y fabrica específicamente en el controlador 106 para realizar óptimamente el cálculo matemático del desafío 128 de temporización. De esta manera, cuando el algoritmo 126 de sincronización emite el desafío 128 de temporización al dispositivo 104 de suministro, también emite el desafío 128 de temporización a la lógica 136 de referencia. La lógica 136 de referencia realiza los cálculos matemáticos del desafío de la misma manera que se trató anteriormente con respecto a la lógica 132 de hardware dedicada en el dispositivo 104 de suministro. En respuesta al desafío 128 de temporización, la lógica 136 de referencia completa el desafío y proporciona una respuesta de referencia en un tiempo de referencia. Una ventana de tiempo de respuesta de referencia se puede definir, por ejemplo, que esté dentro de un cierto porcentaje (por ejemplo, +/- 5%, +/- 10%) del tiempo de referencia. El algoritmo 126 de autenticación puede usar entonces la respuesta de referencia y la ventana de tiempo de respuesta de referencia como valores esperados para comparar con la respuesta 130 al desafío y el tiempo 131 de respuesta al desafío. Si la respuesta 130 al desafío coincide con la respuesta de referencia y el tiempo 131 de respuesta al desafío cae dentro de la ventana de tiempo de respuesta de referencia, el algoritmo 126 determina que el dispositivo 104 de suministro es un dispositivo auténtico.

La FIG. 3 muestra un ejemplo de un sistema 100 de autenticación encarnado como un sistema 300 de impresión de chorro de tinta. En general, el sistema 300 de impresión comprende los mismos componentes o similares que el sistema 100 de autenticación general, y funciona de la misma manera o de manera similar con respecto a la autenticación de los cartuchos de chorro de tinta sustituibles. En una implementación ejemplo, el sistema 300 de impresión de chorro de tinta incluye un motor 302 de impresión que tiene un controlador 106, un conjunto 304 de montaje, uno o más dispositivos 104 de suministro sustituibles encarnados como cartuchos 306 de suministro de tinta, y al menos una fuente de alimentación 308 que proporciona energía a los diversos componentes eléctricos del sistema 300 de impresión de chorro de tinta. El sistema 300 de impresión incluye adicionalmente un conjunto 310 de transporte de medios.

La FIG. 4 muestra una vista en perspectiva de un cartucho 306 de suministro de chorro de tinta ejemplo que representa un dispositivo 104 de suministro sustituible. Además de uno o más cabezales de impresión 312, el cartucho 306 de chorro de tinta incluye un microcontrolador 112, un grupo de contactos 400 eléctricos y una cámara 402 de suministro de tinta (u otro fluido). En algunas implementaciones, el cartucho 306 puede tener una cámara 402 de suministro que almacena un color de tinta, y en otras implementaciones puede tener un número de cámaras 402 que almacenan cada una un color de tinta diferente. Los contactos 400 eléctricos llevan señales eléctricas desde el controlador 106 a las boquillas 314 en el cabezal de impresión 312 para causar la expulsión de gotas de fluido. Los contactos 400 eléctricos también llevan señales eléctricas entre el controlador 106 y el microcontrolador 112 para facilitar la autenticación del cartucho 306 dentro del sistema 300 de impresión de chorro de tinta. En una implementación ejemplo, el microcontrolador 112 está situado sobre un sustrato de silicio compartido por el cabezal de impresión 312. En otra implementación ejemplo, el microcontrolador 112 está situado en otra parte del cartucho 306 como una tarjeta inteligente autónoma. El microcontrolador 112 es análogo al, e incluye los mismos componentes generales (no todos mostrados en la FIG. 4) del, microcontrolador 112 mostrado en la FIG. 1 y tratado anteriormente. De esta manera, el microcontrolador 112 en el cartucho 306 comprende una memoria 116 y una lógica 132 de desafío dedicada, que funcionan de la misma manera general que se trató anteriormente con respecto al sistema 100 de autenticación de las FIG. 1 y 2.

Con referencia a las FIG. 3 y 4, el cabezal de impresión 312 expulsa gotas de tinta u otro fluido a través de una pluralidad de orificios o boquillas 314 hacia un medio de impresión 316 para imprimir sobre el medio de impresión 316. El medio de impresión 316 puede ser cualquier tipo de material de hoja o rollo adecuado, tal como papel, cartulina, transparencias, Mylar, poliéster, madera contrachapada, tablero de espuma, tela, lienzo y similares. El cabezal de impresión 312 se puede configurar para expulsar tinta a través de las boquillas 314 en una variedad de formas. Por ejemplo, un cabezal de impresión térmica de chorro de tinta expulsa gotas desde una boquilla pasando corriente eléctrica a través de un elemento de calentamiento para generar calor y vaporizar una pequeña porción de la tinta dentro de una cámara de cocción. La burbuja de vapor fuerza una gota de tinta a través de la boquilla 314. En otro ejemplo, un cabezal de impresión de chorro de tinta piezoeléctrico usa un actuador de material piezoeléctrico para generar impulsos de presión que fuerzan a las gotas de tinta a salir de una boquilla. Las boquillas 314 se disponen típicamente en una o más columnas o agrupaciones a lo largo del cabezal de impresión 312 de manera que la expulsión secuenciada adecuadamente de tinta desde las boquillas 314 hace que caracteres, símbolos y/u otros gráficos o imágenes sean impresos en el medio de impresión 316 a medida que el cartucho 306 de chorro de tinta y el medio de impresión 316 se mueven uno con relación al otro.

El conjunto 304 de montaje coloca el cartucho 306 de chorro de tinta en relación con el conjunto 310 de transporte de medios, y el conjunto 310 de transporte de medios coloca el medio de impresión 316 con relación al cartucho 306 de chorro de tinta. De esta manera, se define una zona 318 de impresión adyacente a las boquillas 314 en un área

entre el cartucho 306 de chorro de tinta y el medio de impresión 316. En una implementación, el motor 302 de impresión es un motor 302 de impresión de tipo exploración. Por tanto, el conjunto 304 de montaje incluye un carro para mover el cartucho 306 de chorro de tinta en relación al conjunto 310 de transporte de medios para escanear el medio de impresión 316. En otra implementación, el motor 302 de impresión es un motor 302 de impresión de tipo no exploración. Por tanto, el conjunto 304 de montaje fija el cartucho 306 de chorro de tinta en una posición prescrita en relación al conjunto 310 de transporte de medios mientras el conjunto 310 de transporte de medios coloca el medio de impresión 316 con relación al cartucho 306 de chorro de tinta.

Como se señaló anteriormente con respecto al sistema 100 de autenticación de la FIG. 1, un controlador 106 incluye típicamente componentes de un sistema informático estándar, tal como un procesador (CPU) 108, una memoria 110, microprograma y otra electrónica. En el sistema 300 de impresión de chorro de tinta de la FIG. 3, el controlador 106 emplea del mismo modo tales componentes para controlar las funciones generales del sistema 300 de impresión y para comunicar con y controlar el cartucho 306 de chorro de tinta, el conjunto 304 de montaje y el conjunto 310 de transporte de medios. Por consiguiente, el controlador 106 recibe los datos 320 de un sistema anfitrión, tal como un ordenador, y almacena temporalmente los datos 320 en una memoria 110. Típicamente, los datos 320 se envían al sistema 300 de impresión de chorro de tinta a lo largo de una trayectoria de transferencia de información electrónica, de infrarrojos, óptica u otra. Los datos 320 representan, por ejemplo, un documento y/o un archivo a ser impreso. Por tanto, los datos 320 forman un trabajo de impresión para el sistema 300 de impresión de chorro de tinta que incluye uno o más comandos de trabajo de impresión y/o parámetros de comando. Usando los datos 320, el controlador 106 controla el cartucho 306 de chorro de tinta para expulsar las gotas de tinta desde las boquillas 314. De esta manera, el controlador 106 define un patrón de gotas de tinta expulsadas que forman caracteres, símbolos y/u otros gráficos o imágenes sobre el medio de impresión 316. El patrón de gotas de tinta expulsadas se determina por los comandos de trabajo de impresión y/o los parámetros de comando a partir de los datos 320.

Además de gestionar las funciones de impresión generales del sistema 300 de impresión de chorro de tinta, el controlador 106 ejecuta un algoritmo 126 de autenticación para determinar si un cartucho 306 de suministro de chorro de tinta es un dispositivo auténtico. Este proceso de autenticación en el sistema 300 de impresión es similar al proceso descrito anteriormente con respecto al sistema 100 de autenticación general de la FIG. 1. La FIG. 5 es un diagrama de flujo de un proceso 500 de autenticación ejemplo en un sistema 300 de impresión u otro sistema 100 de autenticación que determina si un dispositivo 104 de suministro sustituible tal como un cartucho 306 de suministro de chorro de tinta es un dispositivo auténtico. El proceso 500 está asociado con las implementaciones ejemplo tratadas anteriormente con respecto a las FIG. 1-4, y los detalles de los pasos mostrados en el proceso 500 se pueden encontrar en la discusión relacionada de tales implementaciones. Los pasos del proceso 500 se pueden encarnar como un algoritmo que comprende instrucciones de programación almacenadas en un medio no transitorio legible por ordenador/por procesador, tal como la memoria 110 de las FIG. 1 y 3. En diferentes ejemplos, las implementaciones de los pasos del proceso 500 se logran mediante la lectura y ejecución de tales instrucciones de programación mediante un procesador, tal como el procesador 108 de las FIG. 1 y 3. El proceso 500 puede incluir más de una implementación, y diferentes implementaciones del proceso 500 pueden no emplear cada paso presentado en el diagrama de flujo de la FIG. 5. Por lo tanto, aunque los pasos del proceso 500 se presentan en un orden particular dentro del diagrama de flujo, el orden de su presentación no se pretende que sea una limitación en cuanto al orden en el que se pueden implementar realmente los pasos, o en cuanto a si se pueden implementar todos los pasos. Por ejemplo, una implementación del proceso 500 se podría lograr a través de la realización de una serie de pasos iniciales, sin realizar uno o más pasos posteriores, aunque otra implementación del proceso 500 se podría lograr a través de la realización de todos los pasos.

Con referencia ahora ante todo a las FIG. 1, 3 y 5, un proceso 500 de autenticación comienza en el bloque 502, donde el primer paso mostrado es reconocer un dispositivo de suministro sustituible. El reconocimiento de un dispositivo de suministro sustituible típicamente ocurre en el encendido de un dispositivo anfitrión o la inserción de un nuevo dispositivo de suministro en un dispositivo anfitrión, tal como cuando un sistema de impresión se enciende o cuando un cartucho de suministro de tinta o tóner se sustituye en un sistema de impresión. El dispositivo de suministro sustituible también se puede reconocer cuando el dispositivo de suministro se enciende al comienzo de cada trabajo de impresión. El proceso 500 de autenticación continúa en el bloque 504, donde se emite un desafío de temporización criptográfico. El desafío de temporización se emite desde un dispositivo anfitrión tal como un dispositivo de impresión y se envía a un dispositivo de suministro tal como un cartucho de suministro de impresión. El desafío de temporización comprende una solicitud para realizar un cálculo matemático específico que implica ciertos parámetros de desafío que incluyen una clave de sesión derivada entre un dispositivo anfitrión y un dispositivo de suministro, un número de semilla aleatorio generado por el dispositivo anfitrión, y un recuento o ciclo de cálculo que indica el número de veces que ha de ser realizado el cálculo. Al emitir el desafío de temporización, el dispositivo anfitrión pude comenzar una secuencia de temporización para monitorizar la cantidad de tiempo que tarda en recibir una respuesta al desafío, como se muestra en el bloque 506.

En algunas implementaciones el desafío de temporización también se puede enviar a una lógica de referencia en el dispositivo anfitrión, como se muestra en el bloque 508. Cuando el desafío de temporización se envía a una lógica de referencia en el dispositivo anfitrión, se recibe una respuesta de referencia desde la lógica en una cierta cantidad de tiempo de referencia trascurrido, como se muestra en el bloque 510. En el bloque 512, se puede determinar una ventana de tiempo de referencia incluyendo un intervalo alrededor del tiempo de referencia de un cierto porcentaje. Por ejemplo, una ventana de tiempo de referencia se puede determinar que es el tiempo de referencia, más o menos

el 5% del tiempo de referencia. En algunas implementaciones, como alternativa a enviar el desafío de temporización a una lógica de referencia en el dispositivo anfitrión, el dispositivo anfitrión recupera y accede a datos de caracterización almacenados en el dispositivo de suministro, como se muestra en el bloque 514. En otra implementación, los datos de caracterización se pueden codificar en una memoria del dispositivo anfitrión. Los datos de caracterización incluyen ventanas de tiempo esperadas para recibir una respuesta al desafío desde el dispositivo de suministro que están asociadas con diferentes valores de recuento de cálculo.

Como se muestra en el bloque 516, el proceso 500 de autenticación incluye recibir una respuesta al desafío desde el dispositivo de suministro. La respuesta al desafío se recibe en un cierto tiempo de respuesta al desafío que se puede determinar, por ejemplo, mediante una medición de tiempo en el dispositivo anfitrión. El proceso 500 continúa en el bloque 518 con la comparación de la respuesta al desafío a una respuesta esperada. La respuesta esperada puede ser la respuesta de referencia recibida desde la lógica de referencia en el dispositivo anfitrión. En el bloque 520, el tiempo de respuesta al desafío también se compara con una ventana de tiempo de respuesta esperada para determinar si el tiempo de respuesta al desafío cae dentro de la ventana de tiempo esperado. La ventana de tiempo esperado puede ser la ventana de tiempo de referencia o una ventana de tiempo esperado recuperada a partir de los datos de caracterización almacenados en el dispositivo de suministro o en otra parte.

El proceso 500 de autenticación continúa en el bloque 522 con el dispositivo anfitrión autenticando el dispositivo de suministro cuando la respuesta al desafío desde el dispositivo de suministro coincide con un valor esperado y el tiempo de respuesta al desafío cae dentro de una ventana de tiempo esperado. En el bloque 524 del proceso 500, el dispositivo anfitrión determina que el dispositivo de suministro no es auténtico cuando o bien la respuesta al desafío no coincide con un valor esperado, o bien el tiempo de respuesta al desafío cae fuera de una ventana de tiempo esperado, o ambos.

A continuación se describirán realizaciones adicionales:

Una 1ª realización proporciona un cartucho de suministro de impresión que comprende un microcontrolador para recibir un desafío de temporización y permitir la autenticación del cartucho proporcionando una respuesta al desafío en un tiempo de respuesta al desafío que cae dentro de una ventana de tiempo esperado.

Una 2ª realización proporciona un cartucho como en la 1ª realización, que además comprende una lógica de hardware dedicada en el microcontrolador para realizar un cálculo matemático en respuesta al desafío de temporización, en donde el cálculo produce la respuesta al desafío dentro de la ventana de tiempo esperado.

Una 3ª realización proporciona un cartucho como en la 1ª realización, que además comprende datos de caracterización almacenados en el microcontrolador que incluyen ventanas de tiempo esperadas para completar la respuesta al desafío.

Una 4ª realización proporciona un cartucho como en la 3ª realización, en donde cada ventana de tiempo esperado está asociada con un recuento de cálculo que especifica un número de veces que realiza un cálculo matemático a partir del desafío de temporización.

Una 5ª realización proporciona un cartucho como en la 2ª realización, en donde el desafío de temporización incluye parámetros de desafío que comprenden una clave de sesión, una semilla aleatoria, y un recuento de cálculo que especifica un número de veces que realiza el cálculo matemático.

Una 6ª realización proporciona un cartucho como en la 5ª realización, en donde el cálculo matemático opera sobre la clave de sesión, la semilla aleatoria, y el recuento de cálculo para determinar la respuesta al desafío.

Una 7ª realización proporciona un cartucho como en la 5ª realización, en donde tiempo de respuesta al desafío depende del recuento de cálculo.

Una 8ª realización proporciona un cartucho como en la 5ª realización, que además comprende un ID único y una clave de base a partir de la cual se deriva la clave de sesión.

Una 9ª realización proporciona un cartucho como en la 1ª realización, que además comprende material de impresión seleccionado del grupo que consta de tinta y tóner.

Una 10ª realización proporciona un dispositivo de suministro sustituible que comprende un microcontrolador para derivar una clave de sesión con un dispositivo anfitrión, y para recibir un desafío dependiente del tiempo desde el dispositivo anfitrión que especifica una semilla aleatoria, la clave de sesión, y un ciclo de cálculo; y lógica dedicada dentro del microcontrolador para realizar un cálculo de desafío un número de veces igual al ciclo de cálculo, en donde un primer cálculo usa la semilla aleatoria y la clave de sesión para producir una salida, y cada cálculo posterior usa una salida de un cálculo precedente.

Una 11ª realización proporciona un dispositivo de suministro como en la 10ª realización, que además comprende datos de caracterización almacenados en una memoria del microcontrolador que incluye diferentes ventanas de tiempo para completar los desafíos dependientes del tiempo que dependen de ciclos de cálculo especificados.

Una 12ª realización proporciona un dispositivo de suministro como en la 10ª realización, que además comprende material de impresión a ser depositado en medios de impresión mediante el dispositivo anfitrión.

Una 13ª realización proporciona un dispositivo de suministro como en la 12ª realización, en donde el material de impresión se selecciona del grupo que consta de tóner y de tinta.

Una 14ª realización proporciona Un dispositivo de suministro como en la 11ª realización, en donde el cálculo de desafío comprende una serie de operaciones matemáticas en una secuencia específica.

Una 15ª realización proporciona un dispositivo para facilitar la autenticación de un cartucho de impresión que comprende una memoria y una lógica para recibir desafío independiente del tiempo de un dispositivo anfitrión y permitir la autenticación del cartucho proporcionado una respuesta al desafío en un tiempo de respuesta al desafío que cae dentro de una ventana de tiempo esperado.

Una 16ª realización proporciona un dispositivo como en la 15ª realización, que además comprende lógica para realizar un cálculo en respuesta al desafío independiente del tiempo, en donde el cálculo proporciona la respuesta al desafío dentro de la ventana de tiempo esperado.

Una 17ª realización proporciona un dispositivo como en la 15ª realización, que además comprende datos de caracterización almacenados en la memoria que incluye ventanas de tiempo esperado para completar la respuesta al desafío.

Una 18ª realización proporciona un dispositivo como en la 15ª realización, que además comprende datos de caracterización almacenados en la memoria, los datos de caracterización incluyendo un recuento de cálculo y proporcionando una ventana de tiempo esperado dependiente del recuento de cálculo.

Una 19ª realización proporciona un dispositivo como en la 15ª realización, en donde el tiempo de respuesta al desafío depende de un recuento de cálculo matemático recibido de un dispositivo anfitrión.

Una 20th realización proporciona un dispositivo como en la 15th realización, en donde cada ventana de tiempo esperado está asociada con un recuento de cálculo matemático recibido de un dispositivo anfitrión.

Una 21ª realización proporciona un dispositivo como en la 19ª realización, en donde el recuento especifica un número de veces que realiza un cálculo matemático a partir del desafío independiente del tiempo.

Una 22ª realización proporciona un dispositivo como en la 15ª realización, en donde el desafío independiente del tiempo incluye parámetro de desafío que comprenden una comprende una clave de sesión, una semilla aleatoria, y un recuento de cálculo que especifica un número de veces que realiza el cálculo matemático.

Una 23ª realización proporciona un dispositivo como en la 22ª realización, en donde el cálculo matemático opera en una clave de sesión, la semilla aleatoria y el recuento de cálculo para determinar la respuesta al desafío.

Una 24ª realización proporciona un dispositivo como en la 15ª realización, que además comprende una ID única y clave de base.

Una 25ª realización proporciona un dispositivo como en la 15ª realización, que comprende un microcontrolador que comprende la lógica y la memoria.

Una 26ª realización proporciona un dispositivo como en la 15ª realización, que además comprende material de impresión seleccionado del grupo que consiste en tinta y tóner.

Una 27ª realización proporciona un dispositivo reemplazable que comprende un dispositivo como en una de las realizaciones 15ª a 26ª.

Una 28ª realización proporciona un dispositivo reemplazable como la 27ª realización, en donde la lógica es recibir un desafío dependiente del tiempo del dispositivo anfitrión que especifica una semilla aleatoria, la clave de sesión y un recuento de cálculo, y realizar un cálculo matemático de desafío basado en la semilla aleatoria, la clave de sesión y el recuento de cálculo.

Una 29ª realización proporciona un dispositivo reemplazable como en la 27ª realización, en donde la lógica es responder en un tiempo de respuesta al desafío que es dependiente del recuento de cálculo.

Una 30ª realización proporciona un dispositivo reemplazable como en la 27ª realización, que además comprende la caracterización de datos almacenados en una memoria que incluye ventanas de tiempo diferentes para completar los desafíos dependientes del tiempo que dependen de los recuentos de cálculo especificados.

Una 31ª realización proporciona un dispositivo reemplazable como en la 27ª realización, en donde la memoria almacena una ID y una clave de base.

Una 32ª realización proporciona un dispositivo reemplazable como en la 27ª realización, que además comprende un procesador, el procesador para derivar una clave de sesión para cada comunicación con el dispositivo anfitrión.

Una 33ª realización proporciona un dispositivo reemplazable como en la 27ª realización, en donde la lógica es realizar un cálculo matemático de desafío un número de veces igual al ciclo de cálculo, en donde un primer cálculo matemático usa la semilla aleatoria y la clave de sesión para producir una salida, y cada cálculo posterior usa una salida de un cálculo precedente.

Una 34ª realización proporciona un dispositivo reemplazable como en la 27ª realización, que comprende un microcontrolador que incluye la lógica, la memoria y un procesador.

Una 35ª realización proporciona un dispositivo reemplazable como en la 27ª realización, que además comprende material de impresión que se va a depositar en medios de impresión mediante el dispositivo anfitrión.

Una 36ª realización proporciona un dispositivo reemplazable como en la 27ª realización, en donde el material de impresión se selecciona del grupo que consiste en tóner y tinta.

Una 37ª realización proporciona un dispositivo reemplazable como en la 27ª realización, en donde el cálculo de desafío comprende un número de operaciones, que corresponde al recuento de cálculo, en una secuencia específica.

REIVINDICACIONES

1. Un dispositivo de suministro reemplazable que incluye

una CPU (114) y una memoria (116), la memoria (116) almacenando una clave de base (122),

lógica (132) de desafío de hardware dedicada, dedicada para responder a un desafío independiente del tiempo criptográfico (128), estando la lógica (132) de desafío de hardware dedicada configurada para

calcular una respuesta (130) basada en parámetros que incluyen el recuento de cálculo, una clave de sesión relacionada con la clave de base cy una semilla aleatoria, y

proporcionar la respuesta (130) dentro de un tiempo particular de respuesta al desafío (131),

en donde el recuento de cálculo afecta al tiempo de respuesta al desafío (131) de la respuesta (130),

en donde la lógica (132) de desafío de hardware dedicada es para realizar un cálculo de desafío un número de veces igual al recuento o ciclo de cálculo y en donde un primer cálculo usa la semilla aleatoria y la clave de sesión para producir una salida, y cada cálculo posterior usa una salida de un cálculo precedente, y

en donde una última salida del cálculo matemático proporciona la respuesta (130) dentro del tiempo de respuesta al desafío (131) particular.

2. Un dispositivo de la reivindicación 1, en donde la memoria además comprende los datos de caracterización (134) para proporcionar una ventana de tiempo esperado en la que debería entras el tiempo de respuesta al desafío (131), dependiendo del recuento de cálculo.

3. Un dispositivo de la reivindicación 2, en donde el dato de caracterización (134) se asegura usando una firma digital.

4. Un dispositivo de la reivindicación 2 o 3, en donde el dato de caracterización es tal que para un recuento de cálculo x, se puede determinar una ventana de tiempo esperado y, mediante una fórmula de intersección de pendiente ($y = mx + b$).

5. Un dispositivo de una de las reivindicaciones 1 a 4, en donde el cálculo matemático comprende una función básica que define una secuencia de operaciones optimizada para ejecutarse muy rápido en la lógica (132) de desafío de hardware dedicada.

6. Un dispositivo de una de las reivindicaciones 1 a 5, en donde aunque uno o más operandos cambian con cada iteración del cálculo matemático, el cálculo matemático en sí mismo no cambia.

7. Un cartucho de suministro de tinta, que incluye:

el dispositivo de una de las reivindicaciones anteriores, y

contactos eléctricos (400) para llevar señales desde un controlador del dispositivo (116) anfitrión del cartucho (306) de suministro de impresión.

8. Un sistema de autenticación, que comprende:

un dispositivo anfitrión (102); y

un dispositivo (104) de suministro reemplazable según una de las reivindicaciones 1 a 5,

en donde el dispositivo anfitrión (102) está configurado para

emitir el desafío independiente del tiempo (128) criptográfico,

recibir la respuesta al desafío (130) desde el dispositivo (104) de suministro reemplazable (104),

determinar el tiempo de respuesta al desafío (131), y

autenticar el dispositivo (104) de suministro reemplazable usando la respuesta al desafío (130) y el tiempo de respuesta al desafío (131).

9. Un sistema de autenticación de la reivindicación 8, en donde, para determinar el tiempo de respuesta al desafío (131), el dispositivo anfitrión (102) está configurado para

medir el tiempo de respuesta al desafío (131) iniciando una secuencia de temporización cuando se emite el desafío independiente del tiempo (128) criptográfico, y parando la secuencia de temporización una vez que el dispositivo (104) de suministro reemplazable completa y devuelve la respuesta al desafío (130) al dispositivo anfitrión 102.

10. Un sistema de impresión, que comprende el sistema de autenticación de la reivindicación 8 o 9.

11. Un método, que comprende:

respuesta a un desafío independiente del tiempo (128) criptográfico,

calcular, mediante un dispositivo de suministro reemplazable, una respuesta (130) basada en parámetros que incluyen el recuento de cálculo, una clave de sesión relacionada con la clave de base y una semilla aleatoria, y

proporcionar, mediante un dispositivo de suministro reemplazable, la respuesta (130) dentro de un tiempo de respuesta al desafío (131) particular,

en donde el cálculo matemático afecta al tiempo de respuesta al desafío (131) de la respuesta (130).

12. Un método según la reivindicación 11, que comprende:

emitir mediante un dispositivo anfitrión (102), el desafío independiente del tiempo (128) criptográfico,

recibir, en el dispositivo anfitrión (102), la respuesta al desafío (130) desde el dispositivo (104) de suministro reemplazable,

determinar el tiempo de respuesta al desafío (131), y

autenticar el dispositivo (104) de suministro reemplazable (104) usando la respuesta al desafío (130) y el tiempo de respuesta al desafío (131).

13. Un método según la reivindicación 12, en donde determinar el tiempo de respuesta al desafío time (131) comprende:

medir el tiempo de respuesta al desafío (131) iniciando una secuencia de temporización cuando se emite el desafío independiente del tiempo (128) criptográfico, y parar la secuencia de temporización una vez que el dispositivo (104) de suministro reemplazable completa y devuelve la respuesta al desafío (130) al dispositivo anfitrión 102.

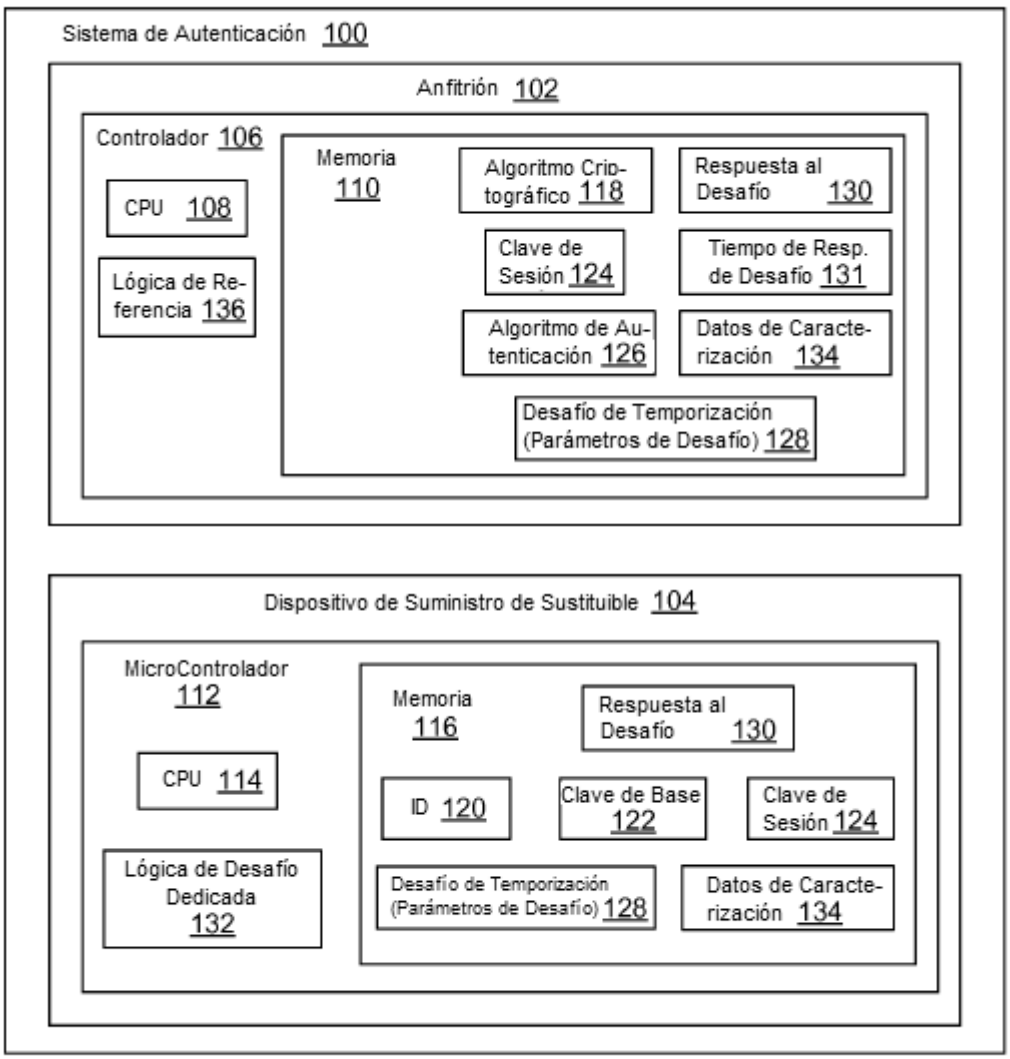

FIG. 1

134

Recuento de Cálculo	Ventana de Tiempo de Resp. al Desafío
A	Q - R mseg
B	S - T mseg
10.000	50 - 55 mseg
C	U - V mseg
•	•
•	•
•	•

FIG. 2

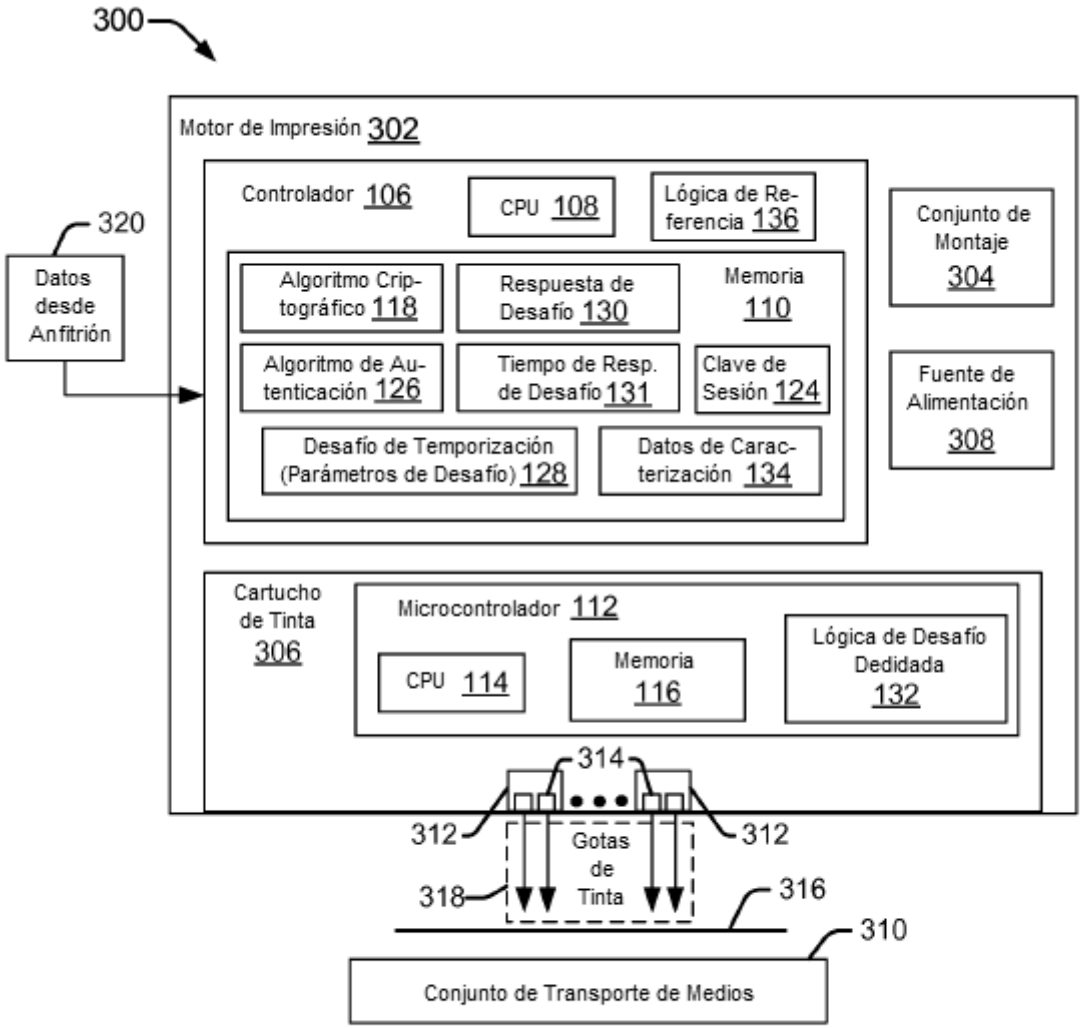
300
Motor de Impresión 302
Controlador 106
CPU 108
Lógica de Referencia 136
Conjunto de Montaje 304
320
Datos desde Anfitrión
Algoritmo Criptográfico 118
Respuesta de Desafío 130
Memoria 110
Algoritmo de Autenticación 126
Tiempo de Resp. de Desafío 131
Clave de Sesión 124
Fuente de Alimentación 308
Desafío de Temporización (Parámetros de Desafío) 128
Datos de Caracterización 134
Cartucho de Tinta 306
Microcontrolador 112
CPU 114
Memoria 116
Lógica de Desafío Dedidada 132
314
312
312
Gotas de Tinta
318
316
310
Conjunto de Transporte de Medios

FIG. 3

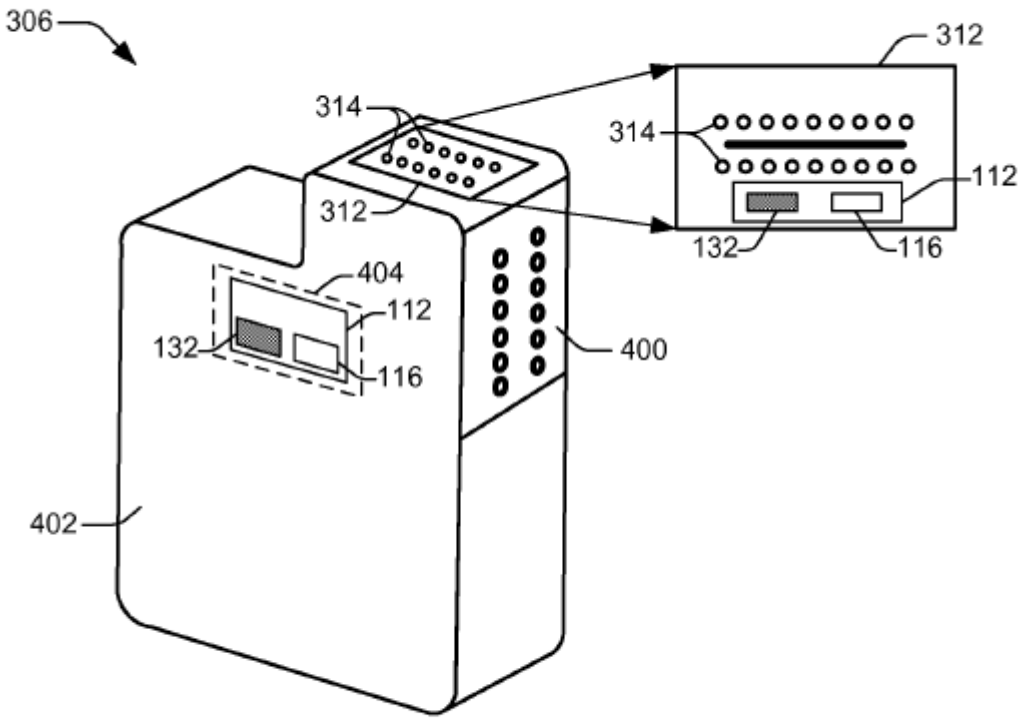

FIG. 4

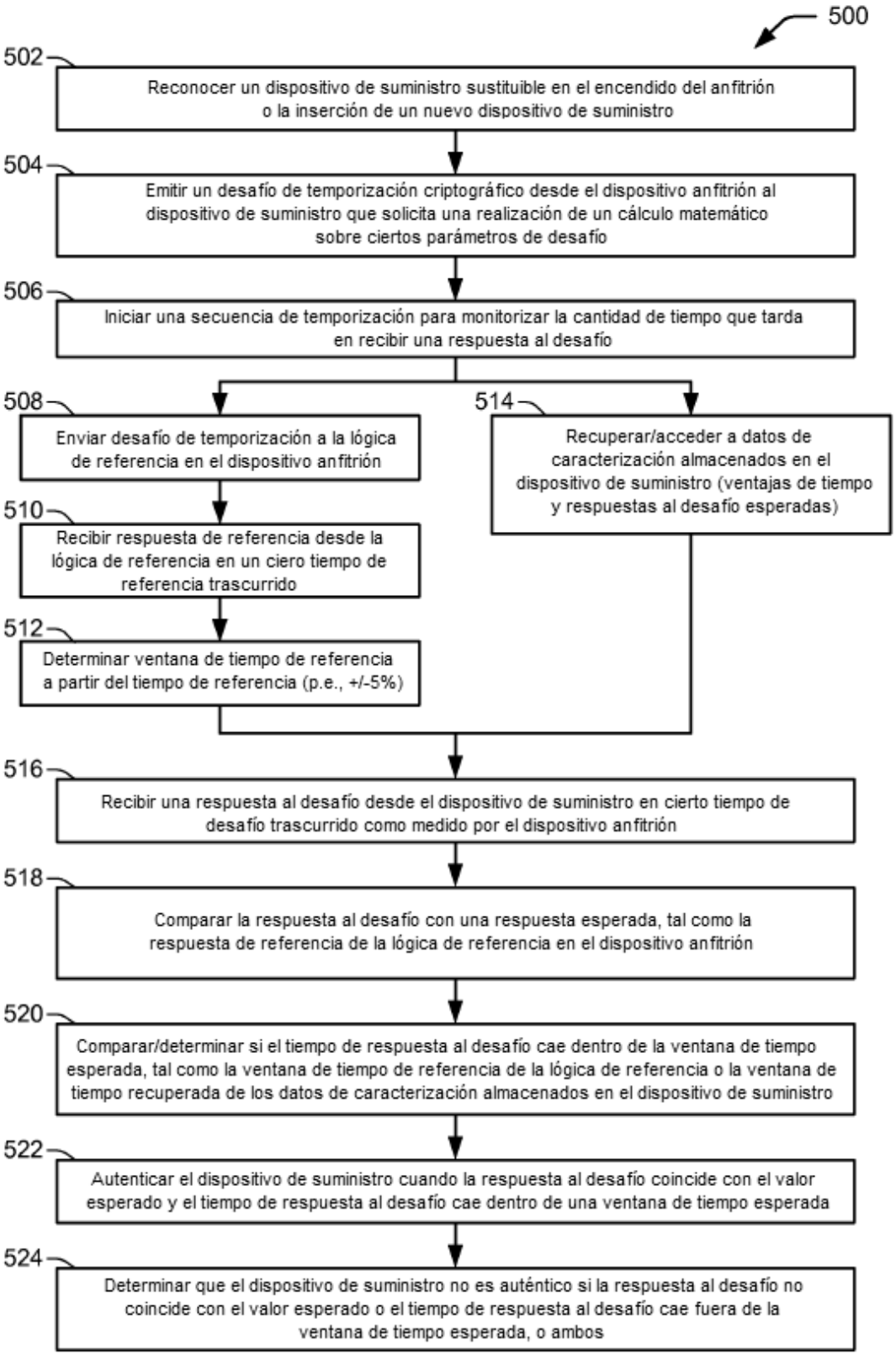
500
502
Reconocer un dispositivo de suministro sustituible en el encendido del anfitrión o la inserción de un nuevo dispositivo de suministro
504
Emitir un desafío de temporización criptográfico desde el dispositivo anfitrión al dispositivo de suministro que solicita una realización de un cálculo matemático sobre ciertos parámetros de desafío
506
Iniciar una secuencia de temporización para monitorizar la cantidad de tiempo que tarda en recibir una respuesta al desafío
508
Enviar desafío de temporización a la lógica de referencia en el dispositivo anfitrión
510
Recibir respuesta de referencia desde la lógica de referencia en un ciero tiempo de referencia trascurrido
512
Determinar ventana de tiempo de referencia a partir del tiempo de referencia (p.e., +/-5%)
514
Recuperar/acceder a datos de caracterización almacenados en el dispositivo de suministro (ventajas de tiempo y respuestas al desafío esperadas)
516
Recibir una respuesta al desafío desde el dispositivo de suministro en cierto tiempo de desafío trascurrido como medido por el dispositivo anfitrión
518
Comparar la respuesta al desafío con una respuesta esperada, tal como la respuesta de referencia de la lógica de referencia en el dispositivo anfitrión
520
Comparar/determinar si el tiempo de respuesta al desafío cae dentro de la ventana de tiempo esperada, tal como la ventana de tiempo de referencia de la lógica de referencia o la ventana de tiempo recuperada de los datos de caracterización almacenados en el dispositivo de suministro
522
Autenticar el dispositivo de suministro cuando la respuesta al desafío coincide con el valor esperado y el tiempo de respuesta al desafío cae dentro de una ventana de tiempo esperada
524
Determinar que el dispositivo de suministro no es auténtico si la respuesta al desafío no coincide con el valor esperado o el tiempo de respuesta al desafío cae fuera de la ventana de tiempo esperada, o ambos

FIG. 5