(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 720 077**

(51) Int. CI.:

G06F 21/10 (2013.01)
G06F 21/73 (2013.01)
G06Q 20/02 (2012.01)
G06Q 20/38 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **14.06.2004 PCT/NL2004/000422**

(87) Fecha y número de publicación internacional: **23.12.2004 WO04111752**

(96) Fecha de presentación y número de la solicitud europea: **14.06.2004 E 04748654 (3)**

(97) Fecha y número de publicación de la concesión europea: **16.01.2019 EP 1634140**

(54) Título: **Método y sistema para realizar una transacción y para realizar una verificación de acceso legítimo o uso de datos digitales**

(30) Prioridad:

13.06.2003 WO PCT/NL03/00436

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.07.2019

(73) Titular/es:

WARD PARTICIPATIONS B.V. (100.0%)
De Schaepstal 1
1251 MZ Laren, NL

(72) Inventor/es:

TEL, TEUNIS y
WARD, SCOTT, MACDONALD

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Método y sistema para realizar una transacción y para realizar una verificación de acceso legítimo o uso de datos digitales

La presente invención se refiere a un método y sistema para realizar una transacción electrónica y para realizar una verificación de acceso legítimo o uso de datos digitales según las reivindicaciones independientes 1, 23 y 24.

En la actualidad, se están manejando numerosas transacciones por medios electrónicos en formato digital. Las redes digitales han evolucionado lo que permite a las partes de diferentes tipos en todo el mundo comunicarse entre sí e intercambiar datos e información para alcanzar las transacciones deseadas como se divulga por ejemplo en los documentos US200223215, WO02076127, US200151996, US2002112162 y US2002112171.

Los datos y la información intercambiada en dichas operaciones pueden ser legalmente privilegiados o protegidos, por ejemplo, por derechos de autor. Sin embargo, la información digital se puede copiar y difundir muy fácilmente sin dejar rastro de quién copió y difundió ilegalmente los datos.

Además, en particular en las transacciones que involucran el acceso a una red privada, compromisos financieros, asignaciones y/o pagos, cada una de las partes involucradas en una transacción de este tipo quiere identificar a cualquier otra parte, o al menos, para poder realizar un seguimiento de cualquier otra parte, si después de la finalización de la transacción surge un problema. Para tales fines de identificación, se conoce el uso de identificadores personales, tales como contraseñas, números de identificación personal (PIN) y similares, que solo se conocen por un usuario específico. Sin embargo, al usar identificadores personales en redes públicas como Internet, existe la posibilidad de que otra persona llegue a conocer el identificador personal, lo que le permite a esta otra persona realizar transacciones u obtener acceso a los datos digitales que se presentan a sí mismos como otra persona. Si surge un problema después de completar la transacción, no es posible rastrear al verdadero socio de la transacción, ya que su identificación personal puede haberse usado por un usuario malintencionado de la red pública.

Para una transacción más segura, se ha propuesto en la solicitud de patente europea N.º 1 219 088 usar un servidor de transacciones de una tercera parte de confianza que comprende los perfiles de las partes de la transacción. El servidor de transacciones verifica la identidad de las partes de la transacción usando los datos de autenticación que comprenden una tabla de datos aleatorios para verificar una firma digital. La firma digital se genera a partir de un testigo aleatorio usando un lector de testigos. La tabla de datos aleatorios corresponde a los datos recopilados a partir de dicho testigo aleatorio. Por lo tanto, una firma digital que se origina en el testigo aleatorio y que es diferente para cada transacción posterior es virtualmente imposible de falsificar y, por lo tanto, identifica de manera única a la parte de transacción.

Una desventaja de este sistema y de otros sistemas que emplean hardware adicional es que el hardware adicional, por ejemplo, un testigo y un lector de testigos, deberían suministrarse a cada posible parte de transacción.

Es por tanto un objeto de la presente invención proporcionar un método y un sistema para realizar una transacción electrónica o verificación o identificación electrónica sin necesidad de un hardware adicional.

Al menos se consigue este objeto en la presente invención mediante un método para realizar una transacción electrónica entre una primera parte de transacción y una segunda parte de transacción mediante un dispositivo electrónico operado por la primera parte de transacción. El método comprende proporcionar unos datos de autenticación en una memoria de dicho dispositivo electrónico, cuyos datos de autenticación son inaccesibles para un usuario del dispositivo electrónico; proporcionar un software de autenticación en dicho dispositivo electrónico, siendo los datos de autenticación accesibles para dicho software de autenticación; activar el software de autenticación para generar una firma digital a partir de los datos de autenticación; proporcionar la firma digital a la segunda parte de transacción. En una realización preferida, la segunda parte de transacción proporciona los datos digitales a la primera parte de transacción.

En un aspecto adicional, la presente invención proporciona un método para realizar una verificación del uso legítimo de los datos digitales en un dispositivo electrónico. El método comprende proporcionar los datos de autenticación en una memoria de dicho dispositivo electrónico cuyos datos de autenticación son inaccesibles para un usuario del dispositivo electrónico; proporcionar un software de autenticación en dicho dispositivo electrónico, siendo los datos de autenticación accesibles para dicho software de autenticación; activar el software de autenticación para generar una firma digital a partir de los datos de autenticación; proporcionar la firma digital a una aplicación que accede a los datos digitales que tienen una firma digital embebida en los mismos; y comparar la firma digital embebida en los datos digitales con la firma digital proporcionada.

En otro aspecto, la presente invención proporciona un método para cifrar los datos digitales en un dispositivo electrónico usando una clave de cifrado, comprendiendo el método recopilar los datos específicos de sesión; revisar dichos datos específicos de sesión para obtener unos números de referencia que se refieren a las posiciones en una tabla de autenticación almacenada en dicho dispositivo electrónico; generar dicha clave de cifrado a partir de los

caracteres almacenados en la tabla de autenticación en dichas posiciones; y cifrar dichos datos digitales usando dicha clave de cifrado.

En un aspecto adicional, la presente invención proporciona unos sistemas para realizar dichos métodos.

Sin el uso de ningún hardware adicional, una parte de transacción en una transacción electrónica puede identificarse con prácticamente ninguna posibilidad de uso fraudulento del método. En una transacción de acceso a la red privada, la primera parte de transacción puede identificarse de manera única por su firma digital. Dicha firma digital se proporciona a la segunda parte de transacción que puede almacenar la firma digital. Si surge un problema más adelante, la primera parte de transacción puede rastrearse e identificarse por la firma digital proporcionada a la segunda parte de transacción.

Si los datos digitales se proporcionan a la primera parte de transacción, por ejemplo, unos archivos de protección de derechos de autor tales como de música y similares, que están firmados digitalmente de acuerdo con la presente invención, es decir, una firma digital está embebida en los datos digitales, dichos datos digitales pueden rastrearse, si a continuación se descubre que se han copiado o difundido ilegalmente. La firma digital embebida se puede rastrear de manera única para la primera parte de transacción original que recibió dichos datos digitales firmados digitalmente.

Los datos digitales firmados digitalmente de acuerdo con la presente invención se almacenan en un medio de almacenamiento de un dispositivo que tiene instalado el software de autenticación. La firma se ha generado de acuerdo con los datos de autenticación almacenados en dicho dispositivo y posteriormente embebidos en los datos digitales para proteger los datos y poder rastrear a un usuario malintencionado.

La firma embebida en los datos también puede emplearse para evitar que los datos se usen ilegalmente, ya que la firma puede regenerarse por el dispositivo en cualquier momento. Ya que una firma regenerada debería ser idéntica a la embebida en los datos digitales, una comparación de la firma embebida con la firma regenerada proporciona información sobre si los datos digitales están correctamente instalados en el dispositivo. Si la comparación muestra que las firmas son idénticas, puede accederse a los datos desde el dispositivo y, por ejemplo, puede ejecutarse una aplicación comprendida en dichos datos digitales o puede accederse a dichos datos digitales desde cualquier otra aplicación, por ejemplo, para reproducir música representada por dichos datos digitales. Cuando las firmas no son idénticas, los datos digitales se han instalado ilegalmente, por ejemplo, se han copiado desde otro dispositivo, y el dispositivo no puede acceder a los mismos ni leerlos, y puede generarse una señal de error.

Otros aspectos y características de la presente invención se desvelan en las reivindicaciones dependientes.

La invención y sus aspectos, características y ventajas se apreciarán más fácilmente cuando la misma se entienda mejor haciendo referencia a la siguiente descripción detallada y considerada en relación con los dibujos adjuntos proporcionados a título de ejemplos no limitativos, en los que los dibujos con símbolos de referencia similares designan acciones o partes similares.

La figura 1: ilustra una gráfica de un método de instalación para un nuevo dispositivo de acuerdo con la presente invención.
La figura 2: ilustra una gráfica de un método de instalación para un dispositivo existente de acuerdo con la presente invención.
La figura 3: ilustra esquemáticamente una configuración de ordenador que tiene un software de autenticación y una tabla de autenticación instalados en la BIOS de acuerdo con la presente invención.
La figura 4: ilustra una gráfica de otro método de instalación para un dispositivo existente de acuerdo con la presente invención.
La figura 5A: ilustra esquemáticamente una configuración de ordenador que tiene un software de autenticación y una tabla de autenticación instalados en una memoria accesible para el usuario.
La figura 5B: ilustra esquemáticamente una localización de memoria protegida por dos capas de cifrado.
La figura 6: ilustra una gráfica de un método para generar una firma digital a partir de una tabla aleatoria.
La figura 7: ilustra una gráfica de un método para generar un archivo digital rastreable personalizado de acuerdo con la presente invención.
La figura 8: ilustra una gráfica de una autenticación fuera de línea de derechos digitales de acuerdo con la presente invención.
La figura 9: ilustra una gráfica de un método de autenticación o transacción en línea de acuerdo con la presente invención.
La figura 10: ilustra una gráfica de una autenticación fuera de línea de derechos digitales de datos digitales almacenados en una memoria extraíble de acuerdo con la presente invención.

Haciendo referencia a las figuras 1, 2, 4 y 6 - 9, en los métodos ilustrados en las figuras respectivas, las acciones de diferentes actores se muestran en varias columnas. En la dirección vertical, las acciones de los actores se han organizado en un orden esencialmente cronológico de arriba a abajo. Por lo tanto, las acciones descritas en una fila de una gráfica se realizan esencialmente antes que las acciones en una fila posterior (inferior) de la gráfica, aunque esto no siempre sea necesario, como se indica en algunos casos. Las flechas en las figuras indican un flujo de datos,

que pueden transferirse a través de una conexión adecuada, tal como una conexión por cable, o una conexión inalámbrica, o una combinación de las mismas, usando un protocolo apropiado en una conexión de red.

En este contexto, un método de instalación ha de entenderse como un método para instalar un software en algunos de los actores que participan en el presente método para permitir el seguimiento y la localización de al menos una de las partes de transacción. Además, en este contexto, un nuevo dispositivo se relaciona con cualquier dispositivo electrónico que contenga un sistema básico de entrada salida ("BIOS", "agente de arranque", etc.) con cualquier localización de almacenamiento/memoria segura asociada, por ejemplo, un ordenador, servidor, impresora, asistente personal digital, teléfono móvil, que se está fabricando o que se ha fabricado, pero que aún no se ha entregado a un usuario final, mientras que un dispositivo existente se relaciona con cualquier dispositivo electrónico que contenga un sistema básico de entrada salida que se haya entregado a un usuario final, y puede o no haberse usado por el usuario final. El sistema básico de entrada salida solo se conoce como un sistema para acceder a una localización de memoria en una memoria que está directa o indirectamente conectada al dispositivo electrónico. Sin embargo, como se describe más adelante en el presente documento, el método de acuerdo con la presente invención puede emplear dicho sistema BIOS para almacenar de manera segura ciertos datos digitales y/o dicho sistema BIOS puede estar provisto de un sistema de cifrado. Una localización de almacenamiento segura y/o un sistema de cifrado no son esenciales para el sistema BIOS con respecto a la presente invención.

La figura 1 ilustra una primera realización preferida de la presente invención. Haciendo referencia a la figura 1, se ilustra un método de instalación para un nuevo dispositivo. El método de la figura 1 incluye cinco actores: un proveedor de tablas aleatorias, un tercero de confianza, un fabricante de BIOS, una BIOS y un software de autenticación. Los actores primero, segundo y tercero son entidades físicas, por ejemplo, personas o empresas, mientras que los actores cuarto y quinto son software embebido en un dispositivo.

En la primera columna de la figura 1, se muestran las acciones del proveedor de tablas aleatorias. Este proveedor genera y suministra una tabla aleatoria o, esencialmente, los datos aleatorios al otro actor.

Una tabla aleatoria se define como una tabla que comprende números aleatorios. Una tabla de este tipo puede crearse por un software adecuado como tal. Como alternativa, la solicitud de patente de Estados Unidos N.º 5.354.097 desvela otro método para producir números aleatorios escaneando ópticamente un material conformado de manera aleatoria, tal como un material no tejido. Del mismo modo, puede usarse un patrón bidimensional, patrón que se ha formado mediante la transformación de una cadena de bits como se desvela en la solicitud de patente Europea N.º 1.219.088. A partir de los datos recopilados durante la lectura del material o patrón conformado de manera aleatoria, pueden obtenerse números aleatorios, por ejemplo, usando un algoritmo predeterminado.

La segunda columna de la figura 1 se refiere a acciones de una tercera parte de confianza (TTP), que puede seleccionarse por el proveedor de tablas aleatorias, un fabricante de BIOS y/o el propietario de cualquier aplicación o servicio. La TTP genera una cadena de bits a partir de la tabla aleatoria y otros datos, que se explicarán a continuación. Además, la TTP almacena la cadena de bits y otros datos utilizados para generarla. La cadena de bits generada se envía al fabricante de BIOS.

Se observa que, en otra realización de la presente invención, la cadena de bits puede generarse y almacenarse por otro actor distinto a la TTP. Por ejemplo, en el caso de la identificación de acceso de red, el administrador de red y/o un servidor de red pueden generar y almacenar la cadena de bits de tal manera que cuando un usuario intente acceder a la red privada, el administrador o el servidor de red pueden regenerar la firma digital de dicho usuario. Por lo tanto, el administrador o el servidor de red pueden identificar inequívocamente al usuario antes de que se le conceda acceso a la red.

Las acciones del fabricante de BIOS están representadas en la tercera columna de la figura 1. El fabricante de BIOS instala el software de autenticación en una BIOS y almacena la cadena de bits suministrada por la TTP en la BIOS.

La BIOS que se suministra por el fabricante de BIOS, también es un actor en el método, y sus acciones están representadas por la cuarta columna de la figura 1. La BIOS puede acoplarse a la TTP para recibir un código de descifrado y permitir que el software de autenticación descifre una tabla de autenticación, que a continuación se codificará de nuevo y se almacenará en una parte segura del dispositivo, solo accesible para la BIOS.

La quinta columna de la figura 1 representa las acciones del software de autenticación, que puede suministrarse por el proveedor de tablas aleatorias o por cualquier otra tercera parte y se almacena en la BIOS. El software de autenticación puede acoplarse a la TTP para descifrar la cadena de bits en la BIOS en una tabla de autenticación, cifrar de nuevo la tabla de autenticación y almacenarla en la parte segura del dispositivo, solo accesible para la BIOS. Además, el software de autenticación almacena y activa un algoritmo de firma digital para generar una firma digital específica de sesión o transacción. El software de autenticación se ejecuta preferentemente en un entorno operativo separado en la BIOS o en una consola y es independiente e inaccesible para el sistema operativo (SO) del dispositivo.

Como se indica en la figura 1, el método de instalación de un nuevo dispositivo para su uso con el método de seguimiento y rastreo de acuerdo con la presente invención comienza con la generación de una tabla aleatoria, por

ejemplo, una tabla que comprende los caracteres o números elegidos aleatoriamente, de acuerdo con la celda 2. Los números pueden generarse usando un software que emplea un algoritmo. Como alternativa, como se describe en la solicitud de patente de Estados Unidos N.º 5.354.097, pueden deducirse números aleatorios a partir de un material conformado de manera aleatoria, tal como un material no tejido. Por ejemplo, en un material no tejido, las fibras se disponen en un orden aleatorio debido a la aleatoriedad del proceso de producción. A partir de la geometría de las fibras de los materiales no tejidos pueden calcularse los números. Por ejemplo, un número que puede calcularse, puede ser el ángulo entre dos fibras en una zona del material, o el número de fibras que cruzan una línea imaginaria. Los números calculados serán aleatorios, ya que la geometría del material es aleatoria. Otra forma alternativa, como se describe en la solicitud de patente Europea N.º 1.219.088, para recopilar números aleatorios es transformando una cadena de bits en un patrón bidimensional usando un algoritmo. Como se ha descrito anteriormente, a partir de este patrón bidimensional puede calcularse una tabla de números aleatorios basándose en la geometría del patrón.

El proveedor de tablas aleatorias puede generar la tabla aleatoria y suministrarla a la TTP. Como alternativa, el proveedor de tablas aleatorias solo puede suministrar una pieza del material no tejido o software para generar patrones bidimensionales de acuerdo con la solicitud de patente Europea N.º 1.219.088, a partir de la que la TTP puede generar una o más tablas aleatorias.

De acuerdo con la celda 4, un fabricante de BIOS embebe o instala el software de autenticación en la BIOS. El software de autenticación puede suministrarse por el proveedor de tablas aleatorias, generado por el fabricante de BIOS o suministrado por un tercero.

El software de autenticación tiene preferentemente sus propios números de serie único, identificador de software y/o clave de cifrado privada únicos. Dicho número único puede emplearse ventajosamente en el método de instalación y en un método de seguimiento y rastreo, como se explica a continuación.

Además, de acuerdo con las celdas 6A-6E, la TTP genera una secuencia de bits única, de la siguiente manera. En primer lugar, de acuerdo con la celda 6A, la TTP recopila datos fijos, tal como, por ejemplo, un número de serie único de un dispositivo de hardware, un procesador, o la ID de software única embebida en el software de autenticación en la etapa anterior.

Preferentemente, los datos fijos se refieren a un número u otra cadena de caracteres almacenada en o relacionada con la BIOS específica. Se prefiere que la cadena de bits, que se generará a partir de los datos fijos, entre otros, tenga una fuerte relación con la BIOS en la que se almacena. Una relación tan fuerte de este tipo hace difícil falsificar la cadena de bits.

En la siguiente etapa 6B, la TTP selecciona una tabla aleatoria recibida anteriormente desde el proveedor de tablas aleatorias, o genera una tabla aleatoria usando un marcador, tal como una pieza de material no tejido o usando un patrón aleatorio de dos dimensiones.

La TTP genera, además, una cadena de datos de acuerdo con la celda 6C. Los tres conjuntos de datos, por ejemplo, los datos fijos, la tabla aleatoria y la cadena de datos, se utilizan para generar una cadena de bits que usa un algoritmo predeterminado de acuerdo con la celda 6D. La cadena de bits se almacena en una base de datos de acuerdo con la celda 6E junto con los datos fijos y la cadena de datos, que se han usado para generarla.

La cadena de bits se suministra al fabricante de BIOS, preferentemente en una forma cifrada. El fabricante de BIOS inserta la cadena de bits, como el software de autenticación, en la BIOS de acuerdo con la celda 8. En este punto, puede ensamblarse un ordenador que tenga una BIOS que comprenda un software de autenticación y una cadena de bits. A partir de aquí, el ordenador puede venderse, instalarse y conectarse a una red, tal como Internet.

En la primera puesta en marcha del ordenador de acuerdo con la celda 10 de la BIOS o el software de autenticación usa una conexión a una red, tal como Internet, para establecer una conexión con la TTP. La conexión se realiza para recopilar la cadena de datos, que se necesita para descifrar la cadena de bits y generar una tabla de autenticación. La TTP puede identificar la BIOS o el software de autenticación usando los datos fijos, que son un número único como se ha mencionado anteriormente.

La conexión con la TTP no necesita iniciarse por la BIOS, sino que también puede iniciarse por el software de autenticación, que está embebido en una parte segura de la BIOS, o mediante una aplicación de terceros. La conexión se realiza preferentemente sin la posibilidad de que un usuario o el sistema operativo del ordenador interrumpan el procedimiento.

Cuando se establece una conexión con la TTP, la BIOS o el software de autenticación envían su número de identificación tras la solicitud de la TTP de acuerdo con la celda 12. La TTP devuelve, posiblemente tras la solicitud de la BIOS, la clave de descifrado y el software de autenticación usa la clave de descifrado de acuerdo con la celda 14 para generar una tabla de autenticación a partir de la cadena de bits que se ha embebido en la BIOS de acuerdo con la celda 8.

A continuación, de acuerdo con la celda 16, la tabla de autenticación se codifica por el software de autenticación para evitar que la tabla de autenticación pueda descubrirse (por ejemplo, por una persona). Descubrir la tabla de autenticación debilitaría la protección conferida por el método y, por lo tanto, sería prácticamente imposible.

La codificación se realiza usando un número, que es específico para la BIOS. Cuando la tabla de autenticación se necesita más tarde, el software de autenticación puede descodificarla usando ese número específico de BIOS. El número específico de BIOS puede ser, por ejemplo, un número de serie único o cualquier clave de cifrado ordinaria embebida o generada por la BIOS. El número específico de BIOS se envía al software de autenticación de acuerdo con la celda 18 después de una solicitud del software de autenticación de acuerdo con la celda 16.

La instalación de un nuevo dispositivo se completa de acuerdo con la celda 20. La tabla de autenticación codificada se almacena en una parte segura de la BIOS, donde solo puede recuperarse por la BIOS y no por el sistema operativo. Esta parte segura de la BIOS también puede ser cualquier otra localización segura en el dispositivo. Por ejemplo, puede ser una parte separada del disco duro de un ordenador, cuya parte puede no ser accesible para el sistema operativo, pero solo para la BIOS y/o el software de autenticación. Almacenar la tabla de autenticación en una localización segura disminuye aún más la posibilidad de recuperar la tabla de autenticación.

El dispositivo está ahora configurado. El software de autenticación y una tabla de autenticación codificada se instalan en la BIOS. Además, en una base de datos de un tercero de confianza (TTP), se almacenan los datos que permiten que la TTP genere la misma tabla de autenticación cuando sea necesario.

La figura 2 ilustra una segunda realización preferida. En la segunda realización preferida, el método de instalación se realiza en un dispositivo informático existente. El dispositivo existente no tiene software de autenticación instalado en su BIOS, ni tiene una cadena de bits cifrada almacenada en su BIOS en el momento en que se necesita una firma digital de acuerdo con la presente invención para cualquier fin de seguimiento y rastreo, incluyendo una sesión electrónica específica, por ejemplo, un procedimiento de acceso de red, o una transacción en línea. Por lo tanto, en comparación con un nuevo dispositivo informático, son necesarias otras etapas en el método de instalación descrito anteriormente para instalar el software y la tabla de autenticación necesarios en una localización de memoria segura del dispositivo. Una localización de memoria segura de este tipo puede ser parte de una memoria segura o puede ser una parte cifrada de una memoria no segura, como una memoria accesible por el usuario.

En la figura 2, hay cinco columnas que representan cinco actores: un proveedor de tablas aleatorias, una TTP, una BIOS, un software de autenticación y una aplicación de terceros. Comparado con la figura 1, el fabricante de BIOS no es un actor en el método de instalación para un dispositivo existente, pero se introduce una aplicación de terceros como un actor. La aplicación de terceros es una aplicación en línea, en general, destinada a realizar el acceso lógico en línea o las transacciones en línea. La aplicación de terceros solicita una firma digital del dispositivo existente, que no tiene el software de autenticación y la tabla de autenticación. Por lo tanto, la aplicación de terceros solicita que el dispositivo instale en primer lugar el software de autenticación antes de continuar con la transacción.

De acuerdo con la celda 22, el proveedor de tablas aleatorias genera y suministra una tabla aleatoria, similar a la acción de acuerdo con la celda 2 en la figura 1.

De acuerdo con la celda 24, un dispositivo que tiene una BIOS sin una tabla de autenticación y/o software de autenticación inicia una transacción en línea con una aplicación de terceros. Sin embargo, la aplicación de terceros requiere una autenticación de acuerdo con la presente invención. Por lo tanto, la aplicación de terceros redirige el dispositivo solicitante a la TTP para obtener el software de autenticación y una tabla de autenticación.

La TTP genera y almacena una cadena de bits de acuerdo con las celdas 26A-26E, similar a las celdas 6A-6E de la figura 1. De acuerdo con la celda 26A, la TTP recopila los datos fijos, de acuerdo con la celda 26B se selecciona una tabla aleatoria o un marcador aleatorio, y de acuerdo con la celda 26C, la TTP selecciona una cadena de datos. A partir de estos tres conjuntos de datos, la TTP genera una cadena de bits de acuerdo con la celda 26D y almacena la cadena de bits, los datos fijos y la cadena de datos de acuerdo con la celda 26E. Además, la cadena de bits se envía al dispositivo solicitante junto con el software de autenticación, ambos cifrados.

El software de autenticación y la cadena de bits se ponen en una parte de la BIOS que puede accederse por el sistema operativo. A continuación, de acuerdo con la celda 28B, el dispositivo necesita reiniciarse para almacenar el software de autenticación y la cadena de bits en una parte segura de la BIOS que no es accesible para el sistema operativo.

En este punto, el procedimiento continúa como el método ilustrado en la figura 1 de la celda 10 y más allá. De acuerdo con la celda 30, el dispositivo que tiene un software de autenticación recientemente almacenado y una cadena de bits en su BIOS se pone en contacto nuevamente con la TTP y solicita una clave de descifrado, por ejemplo, la cadena de datos, de acuerdo con la celda 32.

De acuerdo con la celda 34, la clave de descifrado se usa para descifrar el software de autenticación y para descifrar la cadena de bits y generar la tabla de autenticación correspondiente. A continuación, de acuerdo con la celda 36, el

software de autenticación verifica la tabla de autenticación y solicita datos específicos de la BIOS desde la BIOS para cifrar la tabla de autenticación nuevamente.

De acuerdo con la celda 38, la BIOS envía los datos específicos de la BIOS, por ejemplo, cualquier clave de cifrado común, al software de autenticación en respuesta. El método se completa de acuerdo con la celda 40, en la que se cifra y se almacena la tabla de autenticación en una parte segura de la BIOS. Cualquier dato que quede en el sistema operativo de la transferencia de los datos de autenticación y el software de autenticación se elimina por la BIOS.

Usando este método de instalación, cada dispositivo que tiene una BIOS y es capaz de comunicarse con aplicaciones de terceros externos puede tener el software de autenticación y una tabla de autenticación instalados, por ejemplo, un ordenador personal, un teléfono móvil, un asistente personal digital de mano con capacidades de comunicación inalámbrica o cualquier otro dispositivo que contenga una BIOS, como se ha mencionado anteriormente.

Cuando el software y la tabla están instalados correctamente en la BIOS, pueden iniciarse y realizarse unas sesiones específicas de seguimiento y rastreo o transacciones en línea mediante el método de autenticación y firma digital.

La figura 3 ilustra esquemáticamente una posible configuración de un dispositivo que tiene el software de autenticación y una tabla de autenticación instalados. El dispositivo comprende diversos componentes, comúnmente denominados hardware 42. Los componentes de hardware a modo de ejemplo son un procesador, un disco duro u otra memoria y un teclado.

Todos los dispositivos de hardware se controlan por la BIOS 44. La BIOS 44 es un paquete de software almacenado en una memoria de solo lectura (ROM), que normalmente se encuentra en una placa principal, que es uno de los componentes de hardware de un dispositivo electrónico.

La BIOS 44 controla la mayoría de las instrucciones y datos que fluyen desde un componente a otro. Los datos o instrucciones provenientes de un componente y dirigidos a otro deben pasar por la BIOS 44. La BIOS 44 puede verificar si las instrucciones del otro componente están permitidas o no, ya que cualquier componente no puede accederse por cualquier otro componente.

La BIOS 44 puede comprender una clave de cifrado 46. Una clave de cifrado 46 de este tipo puede usarse para cifrar los datos y solo la otra parte conoce la clave de cifrado 46 que puede ser capaz de descifrar los datos.

El sistema operativo 48 crea un entorno de tiempo de ejecución de las aplicaciones de usuario. Por lo tanto, puede afirmarse que el sistema operativo 48 es una interfaz entre un usuario y el hardware 42. Un usuario puede indicar al sistema operativo 48 que ejecute una aplicación 50. Si la aplicación 50 necesita los datos que están almacenados en el disco duro, la aplicación 50 solicita los datos del sistema operativo 48. A su vez, el sistema operativo 48 solicita los datos a través de la BIOS 44 desde el hardware 42, es decir, el disco duro. Los datos provenientes del hardware 42 pasan a través de la BIOS 44 y del sistema operativo 48 antes de llegar a la aplicación solicitante 50. A través de este protocolo, la BIOS 44 puede controlar la accesibilidad de ciertos datos o dispositivos de hardware 42 y, por lo tanto, el uso de un software específico. Puede prohibir, por ejemplo, que el sistema operativo 48 acceda a ciertas partes de un disco duro o inicie ciertas aplicaciones.

Una consola 52 es un entorno, que ejecuta todos los procesos en el ordenador sin interrupción del usuario. La consola 52 desempeña un papel importante en el inicio del ordenador, ya que indica a los dispositivos de hardware 42 a través de la BIOS 44 que se inicien e informen sobre su estado. En el caso de errores, no solo en el inicio sino también durante el funcionamiento, la BIOS 44 envía los mensajes de error provenientes del hardware 42 a la consola 52. La consola 52 a continuación maneja y corrige los errores. Por lo tanto, la consola 52 ejecuta más o menos autónomamente el ordenador. Un usuario no puede interrumpir ni influir en la consola 52. Por lo tanto, cualquier instrucción proveniente del sistema operativo 48 destinada a la consola 52 puede bloquearse por la BIOS 44.

En o detrás de la consola 52, hay una zona segura 62 solo accesible a la BIOS. La zona segura 62 comprende aplicaciones y localizaciones de almacenamiento, que no se informan al sistema operativo 48. Esto significa que el sistema operativo 48 no sabe que las aplicaciones y los datos en las localizaciones de almacenamiento están presentes y que incluso pueden ejecutarse en un entorno separado. Por ejemplo, cuando un dispositivo de hardware 42 informa un error, la consola 52 puede ejecutar una aplicación de recuperación 56 para manejar el error de tal manera que el dispositivo de hardware 42 se recupere del error y sea capaz de continuar su operación. El sistema operativo 48 probablemente ni siquiera haya notado que ha habido un error.

Una tabla de autenticación puede almacenarse de manera segura en la localización de almacenamiento seguro 60. En una parte del ordenador, comúnmente vista como una parte de la BIOS 44, la tabla de autenticación es inalcanzable para el sistema operativo 48 y por lo tanto para un usuario.

Con la tabla de autenticación almacenada de manera segura en la localización de almacenamiento seguro 60, el software de autenticación 54 debería funcionar en un entorno en la BIOS 44, impidiendo de este modo que la tabla de autenticación sea accesible para el sistema operativo 48 en cualquier momento. Por lo tanto, el software de

autenticación 54 puede instalarse en un entorno de aplicación en la zona segura 62 de tal manera que pueda obtener la tabla de autenticación sin pasar a través de una parte no segura del dispositivo.

La zona de seguridad 62 puede comprender además otras aplicaciones y/o localizaciones de memoria. Por ejemplo, otra localización de memoria 58 puede almacenar un archivo de registro de todas las acciones realizadas por la BIOS 44 en la zona segura 62, o un archivo de registro que almacena cualquier otra acción realizada por cualquier otra aplicación o todo el intercambio de datos de red, por ejemplo, todos los intercambios de datos a través de Internet.

Además, el algoritmo de firma digital se almacena preferentemente en una parte segura de la BIOS 44. Este algoritmo puede protegerse como la tabla de autenticación en la localización de almacenamiento seguro 60, debido a que si ambos se conocen por un usuario, el usuario puede ser capaz de falsificar una firma digital. Al bloquear la tabla de autenticación y el software de autenticación 54 que incluye el algoritmo de firma digital en la zona de seguridad 62 están seguros.

En un tercer método de instalación preferido ilustrado en la figura 4, los datos de autentificación, por ejemplo, la tabla de autenticación, se almacenan en una memoria que es accesible por un sistema operativo del dispositivo y, posiblemente, por un usuario de dicho dispositivo. Para evitar que el usuario pueda obtener los datos de autenticación, lo que debería evitarse como se ha descrito anteriormente, los datos de autenticación se cifran. Por lo tanto, el usuario solo puede obtener datos de autenticación cifrados. Para evitar que los datos de autenticación se vuelvan accesibles para un usuario, los datos de autenticación solo deberían descifrarse en un entorno de procesamiento seguro, tal como un entorno de procesamiento ‘Anillo cero’, que está embebido en una unidad de procesamiento de ordenadores personales de uso común. Un entorno de procesamiento seguro de este tipo solo puede accederse por aplicaciones de software seleccionadas, preferentemente no para aplicaciones de software operadas por el usuario. Además, cualquier usuario no debería poder obtener un algoritmo de descifrado y/o una clave de descifrado.

Se prefiere cifrar los datos de autenticación dos veces, es decir, usando al menos dos capas de cifrado. Si un usuario malintencionado logra descifrar los datos de autenticación una vez, logra de este modo descifrar una primera capa de cifrado, una segunda capa de cifrado aún protege los datos de autenticación.

Preferentemente, una primera capa de cifrado usa un algoritmo de cifrado que emplea una clave de cifrado específica de dispositivo, por ejemplo, una clave de cifrado asociada con números de parte de una o más partes del dispositivo. Un segundo algoritmo de cifrado emplea preferentemente una capa de cifrado asociada con los datos suministrados, tal como una cadena de bits suministrada o un algoritmo de cifrado suministrado. Por lo tanto, la tercera realización preferida es especialmente adecuada para su uso con un dispositivo electrónico provisto previamente de un sistema de cifrado para cifrar datos usando una clave de cifrado específica de dispositivo. Tales dispositivos se conocen en la técnica y están disponibles comercial y comúnmente. En la figura 4, la tercera realización preferida se ilustra en relación con un dispositivo de este tipo.

La figura 4 muestra dos actores en el método de instalación. Un primer actor es una aplicación de terceros. La aplicación de un tercero puede ser una aplicación para realizar una transacción electrónica que necesita datos de autenticación, y si no se encuentran los datos de autenticación en el dispositivo, se inicia una instalación del software de autenticación. Además, puede ser una aplicación o un sistema operativo controlado por un usuario para iniciar una instalación del software de autenticación. El segundo actor en el método de instalación es el software de autenticación. El método puede ampliarse con un tercer actor. Por ejemplo, la BIOS puede habilitarse para cifrar datos usando una clave de cifrado específica de dispositivo. En tal caso, la BIOS puede generar una capa de cifrado de acuerdo con la celda 210 o 212, como se describirá más adelante.

Haciendo referencia ahora a la figura 4, el tercer método de instalación preferido de acuerdo con la presente invención comienza con la obtención e instalación de un paquete de software de autenticación, por ejemplo, obtenido a través de Internet, como se indica en la celda 200.

Después de la instalación del software de autenticación, el software de autenticación obtiene una cadena de bits principal (MBS) de acuerdo con la celda 202. La cadena de bits principal (MBS) puede ser un gran conjunto de caracteres, por ejemplo 2048 números. La MBS puede estar integrada en el paquete de software de autenticación y, en este caso, puede que no sea necesario obtenerla por separado como se indica en la figura 4.

A partir de dicha cadena de bits principal (MBS), de acuerdo con la celda 204, el software de autenticación selecciona una cadena de bits. Dicha cadena de bits comprende por lo tanto una serie de dichos caracteres, por ejemplo, 128 caracteres seleccionados aleatoriamente a partir de la MBS.

El software de autenticación genera los datos de autenticación, por ejemplo, una tabla de autenticación, a partir de la cadena de bits de acuerdo con la celda 206. El software de autenticación se ejecuta en el entorno de procesamiento seguro mencionado anteriormente. Por lo tanto, el algoritmo que genera los datos de autenticación de la cadena de bits está protegido contra usuarios malintencionados que desean obtener los datos de autenticación o dicho algoritmo.

Los datos de autenticación se generan a partir de una cadena de bits que se genera en el dispositivo de la primera parte de transacciones y la cadena de bits y por lo tanto no se conoce por una segunda parte de transacción o tercera parte de confianza (TTP). Por lo tanto, la segunda parte de transacción no puede generar y almacenar (una copia de) los datos de autenticación. Para la identificación de la primera parte de transacción en una transacción, los datos de autenticación deben conocerse por la segunda parte de transacción o una TTP. Por lo tanto, si los datos de autenticación se van a usar para la identificación en una transacción, se devuelve una copia de la cadena de bits al proveedor del paquete de software de autenticación o a otra parte, parte que puede ser una segunda parte de transacción o una TTP de acuerdo con la celda 208.

La cadena de bits puede cifrarse o no, mientras que se devuelve a la otra parte. Si se garantiza que ningún usuario conoce el algoritmo para generar los datos de autenticación a partir de dicha cadena de bits, la cadena de bits real usada para generar los datos de autenticación puede conocerse por cualquier usuario.

Los datos de autenticación generados pueden almacenarse en una memoria accesible para el usuario, tal como, por ejemplo, un disco duro de un dispositivo informático, o en una memoria extraíble, como un disquete o una memoria flash. Como se ha mencionado anteriormente, los datos de autenticación deben protegerse de cualquier usuario, especialmente de un usuario malintencionado. Para ello, los datos de autenticación se cifran por el software de autenticación, preferentemente ejecutándose en un entorno de procesamiento seguro, antes de que los datos de autenticación se almacenen en dicha memoria accesible para el usuario.

De acuerdo con la celda 210, los datos de autenticación se cifran por una primera capa de cifrado, por ejemplo, mediante un algoritmo de cifrado que es parte del paquete de software de autenticación. El algoritmo es seguro de tal manera que no se conoce por ningún usuario. De acuerdo con la celda 212, los datos de autenticación se cifran además mediante una segunda capa de cifrado, por ejemplo, usando una clave de cifrado que está asociada con un número de serie de dispositivo de hardware, o similar, evitando de este modo la copia ilegal a otro dispositivo. Si los datos de autenticación se almacenan en una memoria extraíble, por ejemplo, una memoria flash, la clave de cifrado puede estar asociada con un número de serie de la memoria extraíble. Preferentemente, la clave de cifrado está (también) asociada con un número de identificación de usuario, por ejemplo, un número de identificación personal (PIN) o un número o una plantilla asociada con una huella digital del usuario, o similares.

De acuerdo con la celda 214, los datos de autenticación cifrados se almacenan en la memoria. Por lo tanto, el dispositivo está provisto del software de autenticación y de los datos de autenticación, y garantizándose, mediante el cifrado que los datos de autenticación, que no se conocen por el usuario. El dispositivo se instala para realizar el método de transacción y el método de verificación de uso legítimo de acuerdo con la presente invención.

La figura 5A ilustra esquemáticamente una realización de un dispositivo electrónico para realizar el método de instalación de acuerdo con la tercera realización de la presente invención. El diagrama esquemático de la figura 5A es similar al diagrama de la figura 3. El dispositivo electrónico ilustrado comprende el hardware 42, una BIOS 44, un sistema operativo 48, una aplicación de usuario 50 y una consola 52. A partir de la siguiente descripción, resultará evidente para los expertos en la materia que la zona segura 62 (como se indica en la figura 3) no es esencial para realizar la tercera realización del método de instalación de acuerdo con la presente invención.

Después de la instalación del paquete de software de autenticación de acuerdo con el método ilustrado en la figura 4, se almacena un paquete de datos cifrados en una localización de memoria 63 que es una parte del hardware 42. La localización de memoria 64 puede accederse por un usuario a través de una aplicación de usuario 50. La aplicación 50 puede solicitar datos de la localización de memoria 63 enviando una solicitud al sistema operativo 48. El sistema operativo 48 puede obtener los datos almacenados en la localización de memoria 63 posiblemente a través de la BIOS 44. El software de autenticación también se instala y se almacena en una localización de memoria accesible para el usuario como se indica. El software de autenticación puede estar cifrado o no.

Los datos almacenados en la posición de memoria 63 son datos de autenticación cifrados. El cifrado de los datos de autenticación hace que los datos sean inutilizables para una aplicación de usuario 50. La figura 5B ilustra el cifrado de los datos de autenticación 63A almacenados en la localización de memoria 63. Los datos de autenticación 63A se cifran dos veces como se ilustra en la figura 4. Una primera capa de cifrado 63B y una segunda capa de cifrado 63C protegen los datos de autenticación 63A. Dichas capas de cifrado 63B y 63C pueden eliminarse mediante el descifrado por la aplicación correspondiente.

Una capa de cifrado puede descifrarse por el software de autenticación 54. La otra capa de cifrado puede ser una aplicación de cifrado/descifrado almacenada en el dispositivo electrónico que usa una clave de cifrado específica de dispositivo. Una aplicación de este tipo puede almacenarse en la BIOS o en una zona segura 58 (como se indica en la figura 3) y puede usar la clave de cifrado 46. En otras realizaciones, puede haber solo una capa de cifrado o puede emplearse cualquier otra aplicación de cifrado/descifrado.

Haciendo referencia de nuevo a la figura 5A, la aplicación 50 puede requerir una firma digital para una transacción electrónica o para la verificación de uso legítimo de los datos digitales. Para ello, el software de autenticación 54 se ejecuta para iniciar el descifrado de los datos de autenticación almacenados en la localización de memoria 63 y para

generar dicha firma digital. A partir de una tabla de autenticación, pueden generarse numerosas firmas digitales. La figura 6 ilustra un método para generar una cierta firma digital a partir de una tabla de autenticación e ilustra cómo pueden generarse numerosas firmas digitales diferentes. El uso de diferentes signos digitales para cada acción minimiza la posibilidad de infracciones o falsificaciones y maximiza la capacidad de rastrear el origen de una copia ilegal.

La figura 6 muestra dos actores, una BIOS y el software de autenticación. El software de autenticación comienza mediante la recopilación de datos de acuerdo con la celda 64. Se requieren diversos componentes. En primer lugar, se genera un componente fijo, que es idéntico para cada instancia en la que se genera una firma digital. Además, se usa un componente variable, que permite que el método genere una cantidad numerosa de firmas digitales diferentes, pero rastreables. Un componente de rastreo de sistema, por ejemplo, una ID de transacción, también depende de la instancia. Dos componentes variables hacen que sea prácticamente imposible obtener la tabla de autenticación a partir de una serie de firmas digitales generadas. Opcionalmente, puede usarse un número de identificación personal (PIN) o una contraseña para identificar al usuario, así como el dispositivo en el que está embebido el software de autenticación.

Cuando se recopilan todos los datos requeridos, el software de autenticación verifica los datos recopilados en una cadena de bits y traduce la cadena de bits en un número de punteros de acuerdo con la celda 66. Usando la clave de cifrado, la BIOS descifra la tabla de autenticación de acuerdo con la celda 68. Los punteros generados de acuerdo con la celda 66 apuntan a posiciones en la tabla de autenticación. Usando los punteros, el software de autenticación recopila una serie de números aleatorios de la tabla de autenticación de acuerdo con la celda 70. A partir de entonces, de acuerdo con la celda 72, la BIOS cifra nuevamente la tabla de autenticación. Finalmente, la firma digital acompañada por los componentes de datos variables que se han usado para generar la firma digital se transfieren a la aplicación solicitante de acuerdo con la celda 74.

Una firma digital generada de acuerdo con la presente invención puede usarse de varias maneras. En primer lugar, puede usarse para seguir y rastrear archivos digitales. En segundo lugar, puede usarse fuera de línea para evitar que se utilice software copiado ilegalmente y, en tercer lugar, la firma digital puede usarse en transacciones y autenticación en línea, por ejemplo, autenticación de acceso de red.

La figura 7 ilustra el método de seguimiento y rastreo de los archivos digitales. La información contenida en un archivo digital puede estar protegida, por ejemplo, por derechos de autor. El software, las películas o la música pueden comprarse y descargarse de Internet. Sin embargo, tales archivos digitales que contienen información protegida pueden copiarse y distribuirse ilegalmente muy fácilmente sin un rastro de quién copió y distribuyó el archivo. La adición de una traza en el archivo digital permite rastrear el origen de la copia ilegal. Por lo tanto, los propietarios legítimos de un archivo digital de este tipo, por ejemplo, un archivo de música, no distribuirán el archivo, pero pueden usarlo en diferentes localizaciones, por ejemplo, en su ordenador en casa y en su reproductor digital portátil, por ejemplo, en un reproductor de MP3.

De acuerdo con la celda 80, una aplicación de terceros recibe una solicitud de un archivo digital, por ejemplo, software o un archivo de música. La aplicación de terceros está destinada a proporcionar archivos digitales protegidos o rastreables y puede ser cualquier aplicación adaptada para los mismos. Puede ser, por ejemplo, una aplicación en línea.

A continuación, de acuerdo con la celda 82, la aplicación de terceros se pregunta si el dispositivo que solicita el software de autenticación está instalado y ejecutándose. De acuerdo con la celda 84, la BIOS responde. Si el software de autenticación no está instalado o ejecutándose, el dispositivo se redirecciona a un tercero de confianza para descargar e instalar el software de acuerdo con la celda 24 de la figura 2.

Si el software está instalado y ejecutándose, la aplicación de terceros inicia la transacción transfiriendo una ID de transacción a la BIOS del dispositivo solicitante de acuerdo con la celda 86. De acuerdo con la celda 88, la BIOS y el software de autenticación generan una firma digital de acuerdo con el método descrito en relación con la figura 6 usando la ID de transacción que recibieron.

La firma digital generada junto con el componente de datos variables, por ejemplo, fecha/hora, se envía a continuación, a la aplicación de terceros. De acuerdo con la celda 90, la aplicación de terceros almacena la firma digital, el componente de datos variables, la ID de transacción, que se auto proporcionó y algunos datos que identifican el dispositivo solicitante, por ejemplo, un número de IP, un número de Ethernet, un número de serie o cualquier otro número único de identificación, en una base de datos.

Además, la firma digital se embebe en el archivo digital solicitado de acuerdo con la celda 92. Esto no necesariamente tiene que realizarse después del almacenamiento de acuerdo con la celda 90, sino que también puede hacerse antes o al mismo tiempo.

La firma digital es preferentemente única para el archivo digital solicitado. Cuando se encuentra una copia ilegal del archivo digital, la aplicación de terceros podrá verificar en su base de datos a qué dispositivo envió ese archivo específico después de leer la firma digital embebida en el archivo.

El archivo con la firma digital embebida en el mismo se envía al dispositivo solicitante de acuerdo con la celda 94, que completa el método.

En una realización adicional, el software de autenticación puede estar provisto de un sistema para firmar una firma digital de acuerdo con la presente invención usando al menos una parte de un número de identificación de software (ID software) o cualquier otra cadena de caracteres de identificación de aplicación, en lo sucesivo en el presente documento denominada como una clave privada. La clave privada se registra en un tercero, por ejemplo, el proveedor de software de autenticación que ha suministrado dicha clave privada. La clave privada puede usarse para firmar de manera única la firma digital y adjuntar la firma digital firmada a la firma digital, que se envía a la segunda parte de transacción. La segunda parte de transacción no es capaz de generar la firma digital firmada sin la clave privada. La segunda parte de transacción solo almacena la firma digital firmada.

La primera parte de transacción puede más tarde reclamar no haber realizado la transacción y no haber generado la firma digital, y por lo tanto puede reclamar que otra parte se ha presentado maliciosamente a sí misma como la primera parte de transacciones mientras que es capaz de generar una firma digital correspondiente. A continuación, la segunda parte de transacción puede verificar la firma digital firmada enviándola al tercero, que puede verificar la firma digital firmada. Basándose en la firma digital firmada, puede determinarse si un usuario malintencionado ha realizado la transacción o si la primera parte de transacción afirma maliciosamente que no ha realizado la transacción.

La figura 8 ilustra un método para proteger los archivos digitales de usarse en otros dispositivos distintos del dispositivo destinado originalmente. Con fines ilustrativos, una aplicación que está firmada digitalmente de acuerdo con la presente invención se describe en relación con la figura 6. Sin embargo, el método también puede usarse para cualquier otro archivo digital firmado, tal como un archivo que contenga música o video.

De acuerdo con la celda 100, una aplicación que tiene una firma digital embebida en la misma se está iniciando en un dispositivo que tiene instalado en su BIOS el software de autenticación. La firma digital embebida se ha generado en dicho dispositivo y, por lo tanto, es específica del dispositivo. Por ejemplo, la aplicación puede haberse obtenido usando el método descrito en relación con la figura 7. En cualquier caso, la aplicación se ha firmado y programado para usarse en el dispositivo específico que tiene instalado el software de autenticación.

La aplicación está programada para comenzar con una verificación de su firma digital embebida. Por lo tanto, la aplicación solicita a la BIOS que verifique su firma digital de acuerdo con la celda 102. Para que la BIOS pueda verificar la firma digital, necesita los componentes de datos que se han usado para generar la firma digital. A continuación, de acuerdo con la celda 104, la aplicación transfiere los componentes de datos a la BIOS. Después de recibir todos los datos necesarios desde la aplicación, la BIOS regenera la firma digital de acuerdo con la celda 106.

Para la verificación, se necesita comparar la firma digital embebida con la firma digital regenerada. Esta comparación puede realizarse por el software de autenticación en la BIOS o por la BIOS. Por lo tanto, de acuerdo con la celda 108, la BIOS recibe y compara la firma digital embebida con la firma digital regenerada.

Si los dos signos digitales son idénticos, la aplicación comienza de acuerdo con la celda 110, de lo contrario, la BIOS evita que se inicie la aplicación, posiblemente informando al usuario de que está intentando usar una copia ilegal de la aplicación.

La figura 9 ilustra un método de transacción en línea. Se accede a una solicitud en línea con una solicitud de una transacción, posiblemente una transacción financiera. Por ejemplo, la transacción puede ser un cliente que desea comprar un artículo en línea. Por lo general, estas transacciones se realizan con una tarjeta de crédito. Sin embargo, el cliente solo proporciona un número de tarjeta de crédito y algunos datos adicionales. Si un cliente declara más tarde que no compró ni usó su tarjeta de crédito, no hay forma de verificarlo comprobando una firma, como en las transacciones comunes con tarjetas de crédito.

Haciendo referencia a la figura 9, de acuerdo con la celda 120, la aplicación en línea recibe una solicitud para una transacción. Tras esta solicitud, la aplicación en línea pregunta a la BIOS del dispositivo solicitante si el software de autenticación de acuerdo con la presente invención está instalado y ejecutándose. De lo contrario, el dispositivo que lo solicita se redirecciona a una TTP para descargar e instalar el software de autenticación y la tabla de autenticación de acuerdo con el método explicado en relación con la figura 2 o la figura 4.

Si el software de autenticación está instalado y ejecutándose, la BIOS responde en consecuencia de acuerdo con la celda 124 y la aplicación en línea entrega una ID de transacción de acuerdo con la celda 126. A continuación, el dispositivo solicitante puede generar una firma digital de acuerdo con el método descrito en relación con la figura 6, de acuerdo con la celda 128. Los componentes de datos variables utilizados para generar la firma digital y la propia

firma digital se transfieren a continuación a la aplicación en línea, que a continuación puede completar la transacción de acuerdo con la celda 130.

La firma digital funciona como una firma en este caso. Si el cliente a continuación reclama, por ejemplo, no haber usado su tarjeta de crédito, el propietario de la aplicación en línea puede verificar la firma digital. La verificación de la firma digital puede realizarse por un tercero de confianza, que suministra la tabla de autenticación al cliente y es capaz de regenerar dicha tabla de autenticación. También puede realizarse usando el dispositivo del cliente para regenerar una firma digital usando los componentes de datos variables almacenados por la aplicación en línea.

Opcionalmente, una determinada aplicación de terceros en línea puede usar una tabla de autenticación en las transacciones con un dispositivo específico, cuya tabla de autenticación está específicamente diseñada para su uso en transacciones con dicha aplicación de terceros en línea. Una tabla de autenticación específica de este tipo tiene la ventaja de que la aplicación de un tercero puede verificar la firma digital ya antes de completar las transacciones y, de ese modo, evitar que surjan problemas.

La tabla de autenticación específica puede obtenerse a partir de la tabla de autenticación almacenada en la BIOS de dicho dispositivo usando un algoritmo conocido para el dispositivo. La tabla de autenticación específica obtenida a partir de la tabla de autenticación original se suministraría a continuación por la TTP a la aplicación en línea. Por lo tanto, el dispositivo sabe cómo obtener la tabla de autenticación específica y la aplicación de terceros en línea conoce una tabla determinada, pero no la tabla original almacenada en la BIOS del dispositivo. De lo contrario, el tercero en línea puede proporcionar una tabla de autenticación separada al dispositivo solicitante. La tabla de autenticación específica se cifra antes de almacenarse con una clave de cifrado específica de la BIOS. Esto garantiza que el tercero suministrador no conozca los datos de autenticación almacenados y, por lo tanto, el tercero no puede usar los datos de manera fraudulenta.

Si la aplicación en línea conoce la tabla de autenticación usada por el dispositivo solicitante para generar una firma digital, el dispositivo solicitante puede ser un dispositivo que se conecta a una red, por ejemplo, una red privada corporativa. El dispositivo solicitante debe identificarse por la red corporativa antes de que se conceda el acceso a la red corporativa. Al conectarse, el dispositivo solicitante envía una firma digital que se ha generado usando componentes de datos fijos y componentes de datos variables. Los componentes de datos fijos pueden comprender una contraseña o un número de identificación personal (PIN). Los componentes de datos fijos se conocen por la red corporativa y no es necesario enviarlos a través de la conexión de red no segura; solo los componentes de datos variables utilizados se envían a través de la conexión no segura. Por lo tanto, la red corporativa puede regenerar la firma digital del dispositivo de conexión después de recibir los componentes de datos variables utilizados. Este método tiene la ventaja de que no se envía una contraseña o PIN a través de una conexión no segura y que la firma digital identifica tanto al dispositivo (tabla de autenticación) como al usuario (PIN o contraseña).

Además de garantizar una transacción o autenticación de red como se ha ilustrado anteriormente, también puede verificarse el hardware usado en el entorno operativo. Por ejemplo, si un primer ordenador se comunica con un segundo ordenador, el propio segundo ordenador puede identificarse de una manera similar, usando datos similares, como se usan en una transacción, como se ha descrito anteriormente. Si la tabla de autenticación del segundo ordenador se conoce en el primer ordenador, el primer ordenador puede verificar la identificación del segundo ordenador. Un procedimiento similar es factible cuando uno de los ordenadores se comunica con una impresora, siempre que las tablas de autenticación se almacenen de manera segura en los dispositivos.

La figura 10 ilustra un método para autenticar a un usuario para acceder a datos digitales que se almacenan en una memoria extraíble y portátil tal como una memoria flash. Los datos digitales pueden almacenarse en la memoria extraíble usando el método de cifrado para proteger (autentificar) los datos como se ha ilustrado y descrito en relación con la figura 4, es decir, los datos se cifran usando al menos una, preferentemente al menos dos capas de cifrado, de las que una capa está relacionada con el software de autenticación instalado de acuerdo con la figura 4. La memoria extraíble debe conectarse con un dispositivo electrónico en el que se haya instalado el software de autenticación de acuerdo con dicho método ilustrado en la figura 4 con el fin de descifrar la capa de cifrado relacionada con dicho software de autenticación.

Haciendo referencia a la figura 10, los datos digitales se almacenan en una memoria extraíble y portátil. Los datos digitales se cifran en otro dispositivo electrónico, por ejemplo, un dispositivo informático en el trabajo, mientras que el dispositivo electrónico que intenta acceder a los datos digitales es un dispositivo de ordenador en el hogar.

El software de autenticación para el acceso a los datos digitales se instala en ambos dispositivos informáticos, por ejemplo, en el hogar y en el trabajo, de acuerdo con el método de instalación de la figura 4. Los datos digitales deben leerse por una aplicación de usuario, como un editor de texto, una aplicación de hoja de cálculo, una aplicación de audio o video, o similares. En otro caso, los datos digitales pueden ser una aplicación de software que debe ejecutarse por el dispositivo electrónico.

Después de conectar la memoria portátil y extraíble con el dispositivo electrónico, un usuario inicia la aplicación de usuario. Desde la aplicación de usuario, se realiza un intento para acceder a los datos digitales de acuerdo con la celda 220. Sin embargo, los datos digitales están cifrados.

A continuación, de acuerdo con la celda 222, el software de autenticación se inicia para descifrar los datos digitales. Los datos digitales se transfieren al software de autenticación. De acuerdo con la celda 224, el software de autenticación descifra una primera capa de cifrado usando un algoritmo de descifrado, por ejemplo, embebido en el software de autenticación. Dicho algoritmo de descifrado es idéntico en cada dispositivo que está provisto del software de autenticación.

Para evitar que cualquier dispositivo que está provisto del software de autenticación pueda descifrar los datos digitales, los datos digitales pueden estar protegidos con una segunda capa de cifrado. Para el descifrado de la segunda capa de cifrado, se requiere una clave de descifrado. Dicha clave de descifrado puede estar asociada con un número de serie de la memoria portátil, garantizando que los datos digitales solo puedan descifrarse si los datos digitales se almacenan en dicha memoria portátil. Por lo tanto, una copia de los datos digitales en cualquier otra memoria se convierte en indescifrable. Del mismo modo, la clave de descifrado puede asociarse con un número de identificación personal (PIN) que hace que los datos digitales sean inutilizables sin el PIN. En otra realización más, la clave de descifrado puede asociarse con una huella digital de un usuario, haciendo inutilizables los datos digitales sin la presencia de ese usuario específico.

La clave de descifrado puede estar asociada con cualquier característica de identificación tal como un número de serie, un PIN o una huella digital mediante un algoritmo de verificación protegido o puede ser idéntico al número de serie o PIN. Sin embargo, la verificación de la característica proporciona una capa de seguridad adicional, especialmente cuando la verificación se realiza en el entorno de procesamiento seguro.

De acuerdo con la celda 226, se recopilan los datos para generar la clave de descifrado y se genera la clave de descifrado. A continuación, de acuerdo con la celda 228, se descifra la segunda capa de cifrado. Ahora los datos digitales son adecuados para el acceso por la aplicación de usuario. Por lo tanto, en la celda 230, los datos digitales se proporcionan a la aplicación de usuario y en la celda 232, la aplicación de usuario accede y usa los datos digitales. Después del uso y posiblemente la alteración de los datos digitales, los datos digitales se almacenan nuevamente en la memoria extraíble usando el algoritmo de cifrado del software de autenticación y la clave de descifrado usada para acceder a los datos digitales.

Anteriormente se ha descrito que el algoritmo de descifrado es idéntico en cada dispositivo que está provisto del software de autenticación. Sin embargo, el algoritmo de descifrado/cifrado también puede ser diferente para cada dispositivo o puede ser idéntico para cada dispositivo que se instale usando un paquete de software de autenticación obtenido por un usuario específico. Por lo tanto, los datos digitales solo pueden ser accesibles en un dispositivo que se haya instalado anteriormente por dicho usuario específico.

En tal caso, es necesario proporcionar determinados datos de autenticación a la parte de transacción que suministra dicho software de autenticación, ya que el algoritmo específico de usuario debe estar embebido en el paquete de software antes de que el paquete de software se suministre al usuario específico con el fin de proteger el algoritmo.

En una realización adicional más, los datos digitales pueden cifrarse usando una clave de cifrado que se genera de acuerdo con la presente invención, es decir, idéntico al método para generar una firma digital. La figura 6 ilustra cómo puede generarse una firma digital de acuerdo con la presente invención mediante la recopilación de datos específicos de sesión, tales como datos fijos, datos variables, datos personales y/o datos específicos de dispositivo. La verificación de dichos datos específicos de sesión puede generar números de referencia, refiriéndose a las posiciones en la tabla de autenticación almacenadas de manera segura de acuerdo con la presente invención. La recopilación de los caracteres almacenados en la tabla de autenticación en dichas posiciones genera una cadena de bits que comprende diversos caracteres. Dicha cadena de bits puede comprender cualquier número de caracteres y dicho número puede depender de los datos específicos de la sesión. Los datos cifrados con una clave de cifrado que tienen un número desconocido de bits son prácticamente imposibles de descifrarse por otra persona que no tenga derecho a acceder a dichos datos.

Para descifrar los datos, se requiere la clave de cifrado. Para obtener la clave de cifrado, se necesitan la tabla de autenticación y los datos específicos de la sesión. Teniendo una tabla de autenticación almacenada e instalada en un dispositivo de acuerdo con la presente invención, los datos pueden almacenarse de manera segura en una memoria de dicho dispositivo. Los datos pueden descifrarse fácilmente cuando se accede usando dicho dispositivo. Sin embargo, una copia de dichos datos cifrados en cualquier otro dispositivo se vuelve prácticamente inaccesible.

Si se almacenan tablas de autenticación idénticas en dos o más dispositivos separados, los datos cifrados pueden intercambiarse entre dichos dos o más dispositivos. Si los datos cifrados se transfieren de un dispositivo a otro, junto con los datos específicos de la sesión, el otro dispositivo puede regenerar la clave de cifrado y descifrar los datos. Dicho método de cifrado y descifrado es especialmente útil para la comunicación segura entre dichos dos o más dispositivos a través de una red de acceso público, tal como Internet.

En una realización, un servidor de red está provisto de todas las tablas de autenticación de los dispositivos cliente conectados a dicho servidor. Un cliente que intenta acceder al servidor y a la red de dicho servidor se autentica mediante su firma digital y, a partir de ese momento, todos los datos intercambiados pueden cifrarse usando una firma digital. Si un cliente envía datos a otro cliente, los datos pueden cifrarse y transferirse al servidor junto con los datos específicos de la sesión. El servidor descifra los datos usando los datos específicos de la sesión y la tabla de autenticación del primer cliente. A continuación, el servidor vuelve a cifrar los datos, usando ahora la tabla de autenticación del otro cliente que usa la misma u otra información específica de la sesión. A continuación, los datos cifrados se transfieren al otro cliente junto con los datos específicos de la sesión correspondiente, que descifra los datos usando su tabla de autenticación.

Haciendo referencia nuevamente a la figura 10, los datos digitales almacenados de manera segura en el dispositivo de memoria portátil y extraíble pueden ser una tabla de autenticación de acuerdo con la presente invención. Por lo tanto, los datos digitales cifrados que usan la tabla de autenticación pueden descifrarse en cualquier dispositivo cuando el dispositivo de memoria portátil y extraíble está conectado a dicho dispositivo y dicho dispositivo está provisto del software de autenticación de acuerdo con la figura 10.

REIVINDICACIONES

1. Método para realizar una transacción electrónica entre una primera parte de transacción y una segunda parte de transacción usando un dispositivo electrónico operado por la primera parte de transacción, teniendo el dispositivo electrónico un sistema operativo (48) que crea un entorno de tiempo de ejecución para aplicaciones de usuario y un software de autenticación (54) que se ejecuta en un entorno operativo separado, independiente de e inaccesible a dicho sistema operativo (48), teniendo el dispositivo electrónico una memoria que comprende ubicaciones de almacenamiento, siendo accesible parte de la memoria al sistema operativo (48), siendo parte de la memoria un área segura (62) cuyas ubicaciones de almacenamiento no se reportan al sistema operativo (48), comprendiendo el método:

proporcionar unos datos de autenticación (63A) en el área segura (62) de dicho dispositivo electrónico cuyos datos de autenticación (63A) son inaccesibles para un usuario de dicho dispositivo electrónico, en donde dicha área segura (62) es inaccesible a dicho sistema operativo (48) de dicho dispositivo electrónico, haciendo así que los datos de autenticación (63A) sean inaccesibles a dicho usuario;
proporcionar un software de autenticación (54) en dicho dispositivo electrónico, siendo los datos de autenticación (63A) accesibles para dicho software de autenticación (54), en donde el software de autenticación (54) se almacena en el área segura (62) inaccesible a dicho sistema operativo (48);
activar el software de autenticación (54) para generar una firma digital a partir de los datos de autenticación (63A), en donde el software de autenticación (54) se ejecuta en un entorno de procesamiento seguro inaccesible para dicho sistema operativo (48) proporcionando la firma digital a la segunda parte de transacción.

2. Método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde los datos de autenticación se proporcionan por la segunda parte de transacción, que almacena los datos de autenticación junto con los datos que identifican a la primera parte de transacción.

3. Método de acuerdo con la reivindicación 2, en donde la segunda parte de transacción usa los datos de autenticación almacenados para obtener los datos de autenticación específicos de transacción de acuerdo con un algoritmo específico.

4. Método de acuerdo con la reivindicación 3, en donde la segunda parte de transacción verifica la firma digital proporcionada por la primera parte de transacción usando los datos de autenticación almacenados en la segunda parte de transacción.

5. Método de acuerdo con la reivindicación 1, en donde el software de autenticación tiene sus propios número de serie, ID de software y/o clave de cifrado privada únicos.

6. Método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde los datos de autenticación se cifran por la segunda parte de transacción usando una clave de cifrado antes de que se proporcionen los datos de autenticación a la primera parte de transacción.

7. Método de acuerdo con la reivindicación 6, en donde el software de autenticación recupera una clave de descifrado asociada con la clave de cifrado y descifra los datos de autenticación en su primer uso.

8. Método de acuerdo con la reivindicación 1, en donde el software de autenticación se instala en un entorno de aplicación en la zona segura de tal manera que pueda obtener los datos de autenticación sin pasar a través de una parte no segura de dicho dispositivo electrónico.

9. Método de acuerdo con la reivindicación 1, en donde los datos de autenticación y el software de autenticación incluyendo el algoritmo de firma digital se bloquean en el área segura.

10. Método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde los datos de autenticación se cifran, cuando los datos de autenticación se almacenan en dicha área segura, siendo inaccesible una clave de descifrado para descifrar los datos de autenticación para dicho usuario y para cualquier software operado por usuario, haciendo así que los datos de autenticación sean inaccesibles para dicho usuario.

11. Método de acuerdo con una cualquiera de las reivindicaciones anteriores, en donde el software de autenticación se ejecuta para iniciar el descifrado de los datos de autenticación almacenados en el área segura para generar dicha firma digital.

12. Método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde los datos de autenticación se cifran usando al menos dos capas de cifrado.

13. Método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde los datos de autenticación se cifran usando una clave de cifrado que está asociada con un número de serie de dispositivo de hardware.

14. Método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde los datos de autenticación se cifran usando una clave de cifrado que está asociada con un número de identificación de usuario, en particular un número de identificación personal, PIN o un número o una plantilla asociada con una huella digital del usuario o similar.

15. Método de acuerdo con la reivindicación 12, en donde al menos una capa de cifrado es descifrable usando una clave de cifrado asociada con uno o más números de serie de los componentes de hardware de dicho dispositivo electrónico.

16. Método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde al menos una capa de cifrado puede descifrarse por el software de autenticación.

17. Método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde otra capa de cifrado es una aplicación de cifrado/descifrado almacenada en el dispositivo electrónico usando una clave de cifrado específica de dispositivo.

18. Método de acuerdo con la reivindicación 17, en donde la aplicación de cifrado/descifrado se almacena en un Sistema Básico de Entrada-Salida, BIOS o en un área segura.

19. Método de acuerdo con la reivindicación 12, en donde una segunda capa de cifrado se descifra usando una clave de descifrado asociada con cualquier característica de identificación, en particular un número de serie, un número de identificación personal, PIN o una huella digital de un usuario.

20. Método de acuerdo con cualquiera de las reivindicaciones 14 a 19, en donde los datos de autenticación se descifran en un entorno de procesamiento seguro inaccesible para dicho usuario y para cualquier software operado por un usuario.

21. Método de acuerdo con la reivindicación 1, que comprende además identificar al usuario del dispositivo electrónico antes de activar el software de autenticación.

22. Método de acuerdo con una cualquiera de las reivindicaciones anteriores, en donde el software de autenticación tiene una clave de cifrado privada para cifrar datos digitales.

23. Sistema para realizar una transacción electrónica entre una primera parte de transacción y una segunda parte de transacción usando un dispositivo electrónico operado por la primera parte de transacción, teniendo el dispositivo electrónico un sistema operativo que crea un entorno de tiempo de ejecución para las aplicaciones de usuario y un software de autenticación que se ejecuta en un entorno operativo separado, independiente de e inaccesible a dicho sistema operativo, teniendo el dispositivo electrónico una memoria que comprende ubicaciones de almacenamiento, siendo accesible parte de la memoria al sistema operativo, siendo parte de la memoria un área segura cuyas ubicaciones de almacenamiento no se reportan al sistema operativo, comprendiendo el sistema:

medios para proporcionar unos datos de autenticación en el área segura de dicho dispositivo electrónico cuyos datos de autenticación son inaccesibles para un usuario del dispositivo electrónico, en donde dicha área segura es inaccesible para dicho sistema operativo de dicho dispositivo electrónico, haciendo de este modo que los datos de autenticación sean inaccesibles para dicho usuario;
medios para proporcionar un software de autenticación en dicho dispositivo electrónico, siendo los datos de autenticación accesibles para dicho software de autenticación, en donde el software de autenticación se almacena en el área segura inaccesible para dicho sistema operativo;
medios para activar el software de autenticación para generar una firma digital a partir de los datos de autenticación, en donde el software de autenticación se ejecuta en un entorno de procesamiento seguro inaccesible para dicho sistema operativo;
medios para proporcionar la firma digital a la segunda parte de transacción.

24. Dispositivo electrónico para realizar una transacción electrónica entre una primera parte de transacción y una segunda parte de transacción, en donde el dispositivo electrónico se opera por la primera parte de transacción, teniendo el dispositivo electrónico un sistema operativo que crea un entorno de tiempo de ejecución para las aplicaciones de usuario y un software de autenticación que se ejecuta en un entorno operativo separado, independiente de e inaccesible a dicho sistema operativo, teniendo el dispositivo electrónico una memoria que comprende ubicaciones de almacenamiento, siendo accesible parte de la memoria al sistema operativo, siendo parte de la memoria un área segura cuyas ubicaciones de almacenamiento no se reportan al sistema operativo, almacenando el área segura datos de autenticación que son inaccesibles a un usuario del dispositivo electrónico, en donde dicha área segura es inaccesible a dicho sistema operativo de dicho dispositivo electrónico, haciendo así que los datos de autenticación sean inaccesibles a dicho usuario; comprendiendo el dispositivo electrónico:

una memoria que almacena un software de autenticación, siendo los datos de autenticación accesibles para dicho software de autenticación, en donde el software de autenticación se almacena en el área segura inaccesible para dicho sistema operativo;

medios para activar el software de autenticación para generar una firma digital a partir de los datos de autenticación, en donde el software de autenticación se ejecuta en un entorno de procesamiento seguro inaccesible para dicho sistema operativo; y
medios para proporcionar la firma digital a la segunda parte de transacción.

25. Dispositivo electrónico de acuerdo con la reivindicación 24, en donde el dispositivo electrónico es un ordenador personal, un teléfono móvil, un asistente digital personal de mano con capacidades de comunicación inalámbrica o un dispositivo que contiene una BIOS.

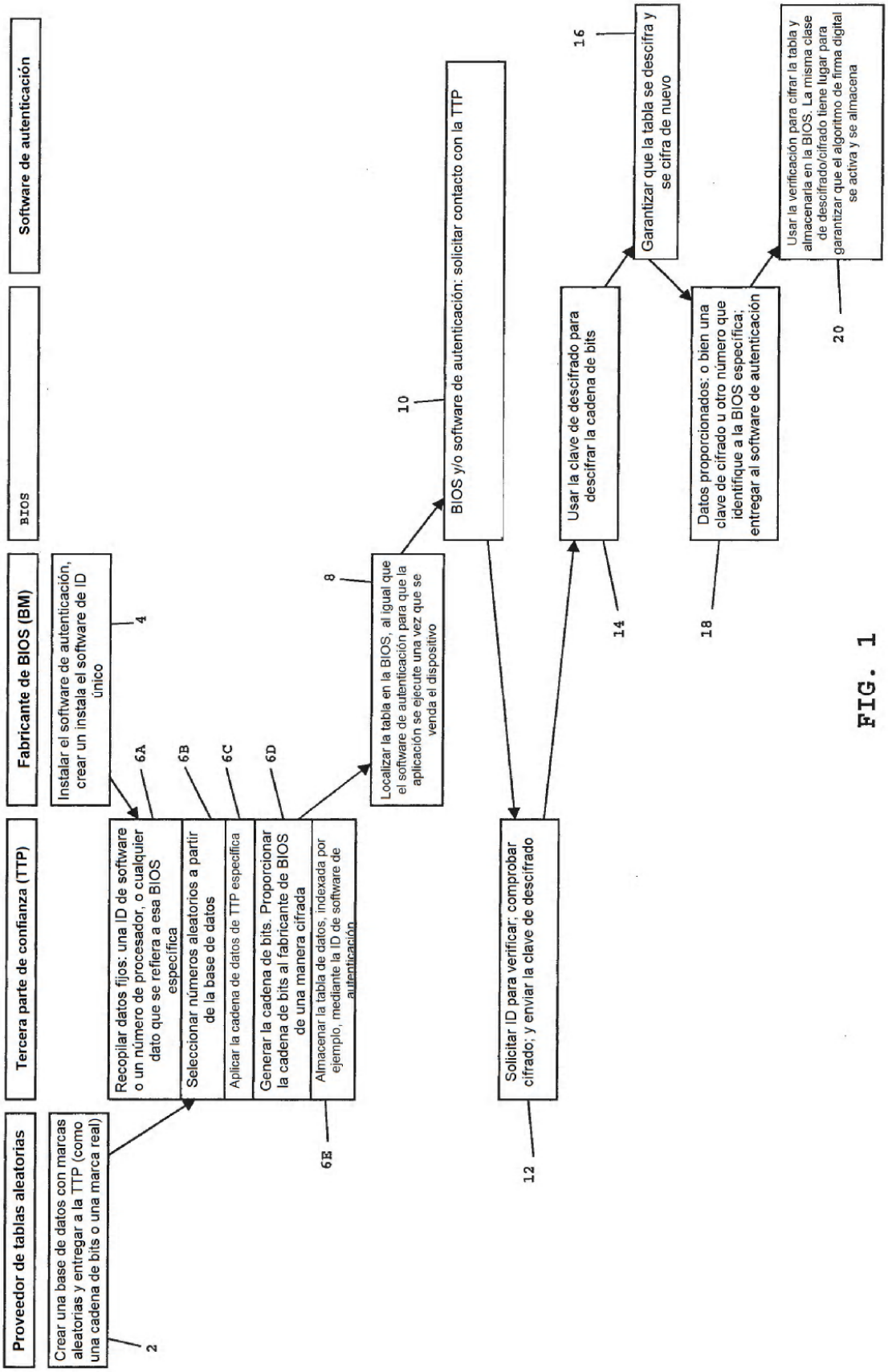
Proveedor de tablas aleatorias
Tercera parte de confianza (TTP)
Fabricante de BIOS (BM)
BIOS
Software de autenticación
Crear una base de datos con marcas aleatorias y entregar a la TTP (como una cadena de bits o una marca real)
2
Instalar el software de autenticación, crear un instala el software de ID único
4
Recopilar datos fijos: una ID de software o un número de procesador, o cualquier dato que se refiera a esa BIOS específica
6A
Seleccionar números aleatorios a partir de la base de datos
6B
Aplicar la cadena de datos de TTP específica
6C
Generar la cadena de bits. Proporcionar la cadena de bits al fabricante de BIOS de una manera cifrada
6D
Almacenar la tabla de datos, indexada por ejemplo, mediante la ID de software de autenticación
6E
Localizar la tabla en la BIOS, al igual que el software de autenticación para que la aplicación se ejecute una vez que se venda el dispositivo
8
BIOS y/o software de autenticación: solicitar contacto con la TTP
10
Solicitar ID para verificar; comprobar cifrado; y enviar la clave de descifrado
12
Usar la clave de descifrado para descifrar la cadena de bits
14
Garantizar que la tabla se descifra y se cifra de nuevo
16
Datos proporcionados: o bien una clave de cifrado u otro número que identifique a la BIOS específica; entregar al software de autenticación
18
Usar la verificación para cifrar la tabla y almacenarla en la BIOS. La misma clase de descifrado/cifrado tiene lugar para garantizar que el algoritmo de firma digital se activa y se almacena
20

FIG. 1

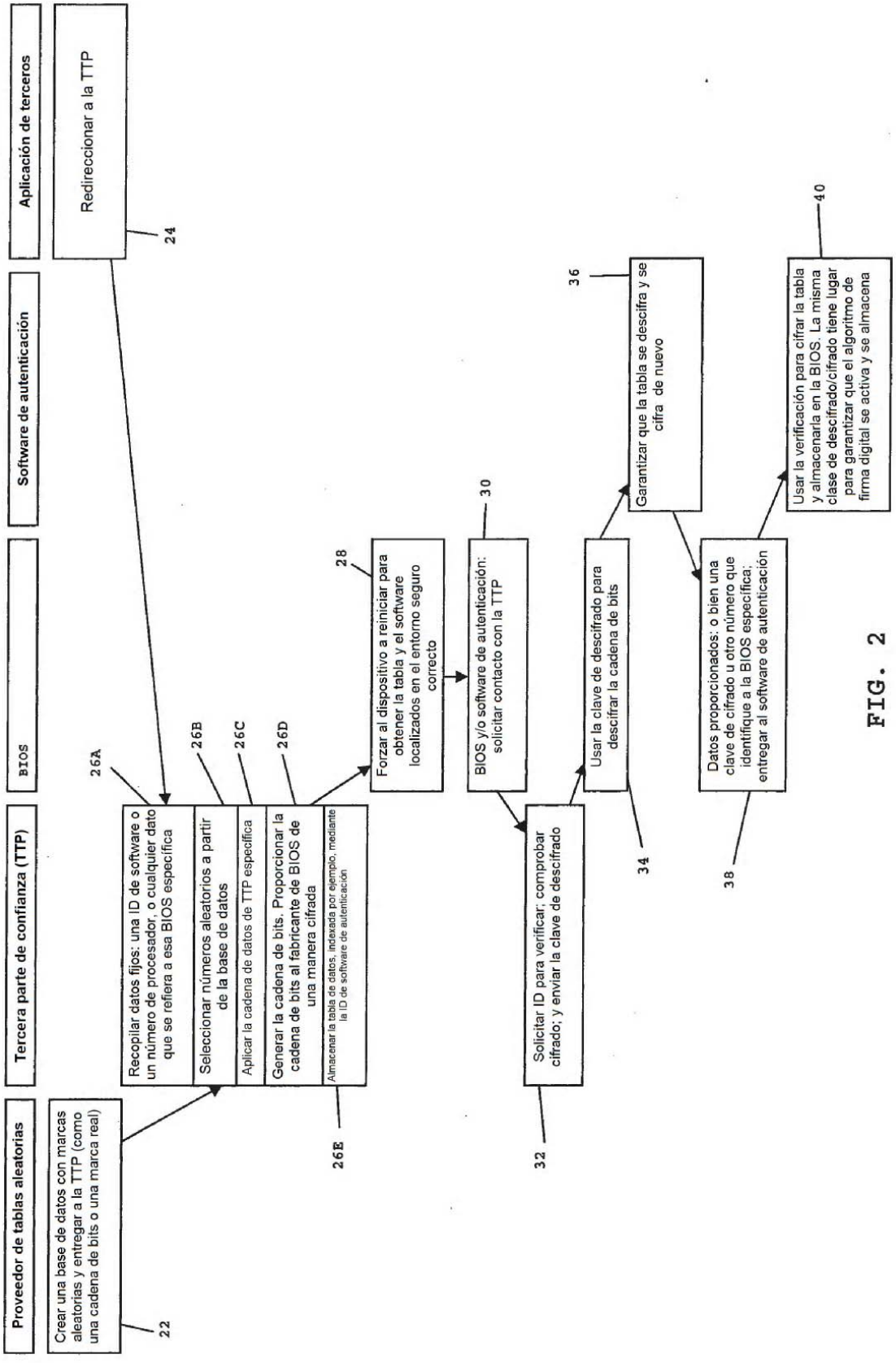
Proveedor de tablas aleatorias
Tercera parte de confianza (TTP)
BIOS
Software de autenticación
Aplicación de terceros
Crear una base de datos con marcas aleatorias y entregar a la TTP (como una cadena de bits o una marca real)
22
Recopilar datos fijos: una ID de software o un número de procesador, o cualquier dato que se refiera a esa BIOS específica
26A
Seleccionar números aleatorios a partir de la base de datos
26B
Aplicar la cadena de datos de TTP específica
26C
Generar la cadena de bits. Proporcionar la cadena de bits al fabricante de BIOS de una manera cifrada
26D
Almacenar la tabla de datos, indexada por ejemplo, mediante la ID de software de autenticación
26E
Redireccionar a la TTP
24
Forzar al dispositivo a reiniciar para obtener la tabla y el software localizados en el entorno seguro correcto
28
BIOS y/o software de autenticación: solicitar contacto con la TTP
30
Solicitar ID para verificar; comprobar cifrado; y enviar la clave de descifrado
32
Usar la clave de descifrado para descifrar la cadena de bits
34
Garantizar que la tabla se descifra y se cifra de nuevo
36
Datos proporcionados: o bien una clave de cifrado u otro número que identifique a la BIOS específica; entregar al software de autenticación
38
Usar la verificación para cifrar la tabla y almacenarla en la BIOS. La misma clase de descifrado/cifrado tiene lugar para garantizar que el algoritmo de firma digital se activa y se almacena
40

FIG. 2

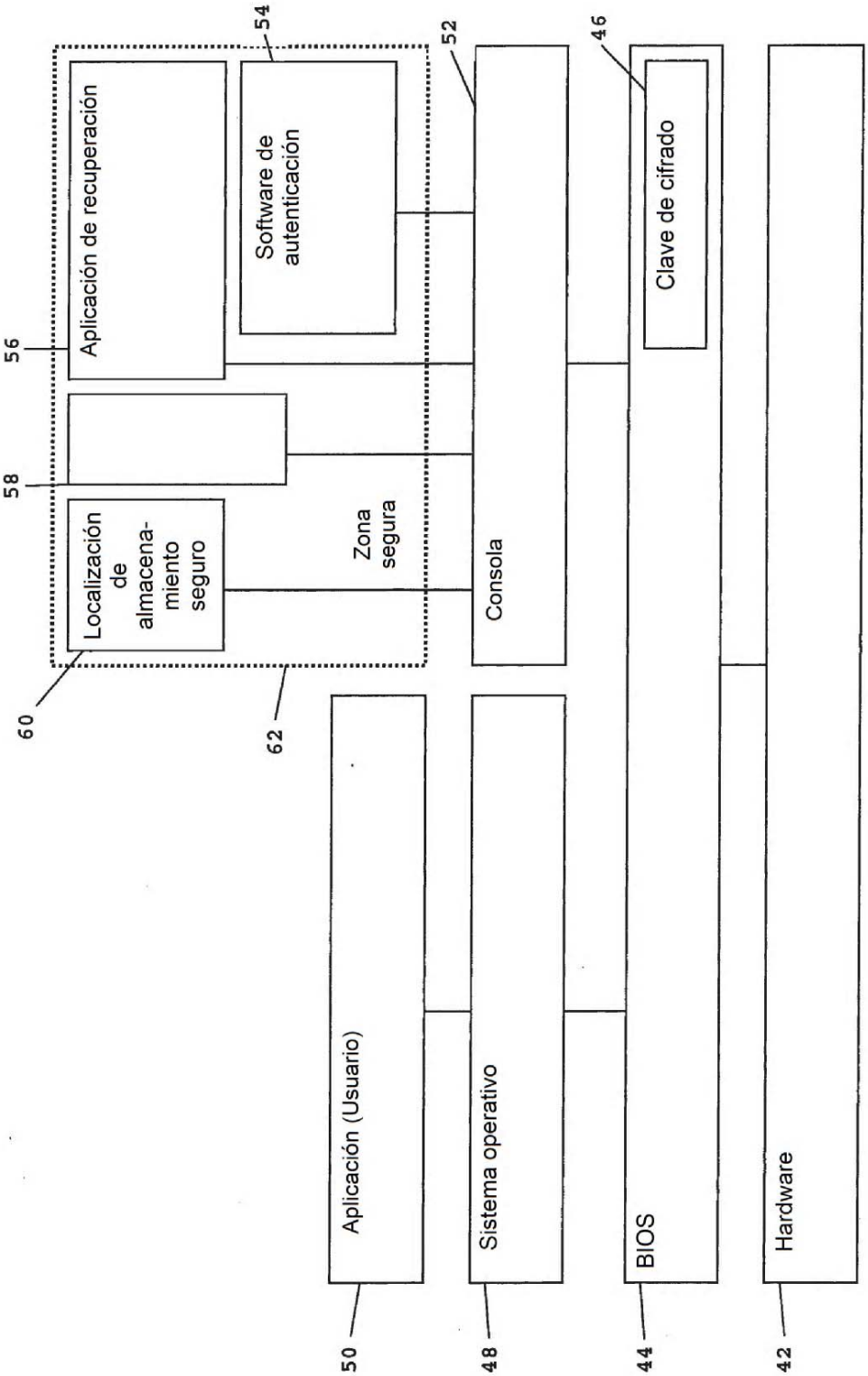
Aplicación de recuperación
Software de autenticación
Localización de almacena-miento seguro
Zona segura
Consola
Clave de cifrado
Aplicación (Usuario)
Sistema operativo
BIOS
Hardware
42
44
46
48
50
52
54
56
58
60
62

FIG. 3

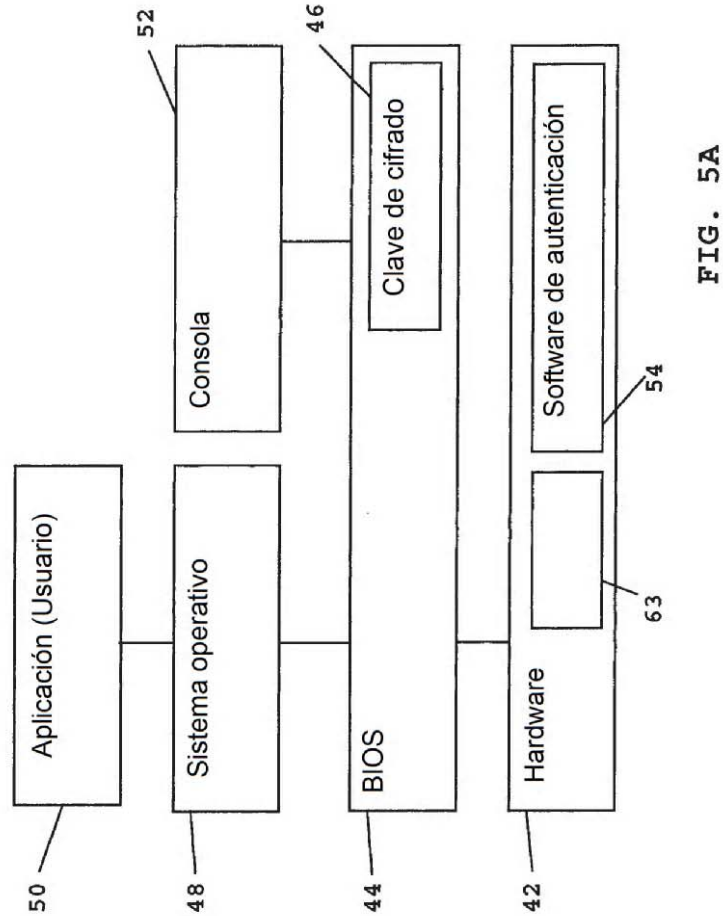

FIG. 5A

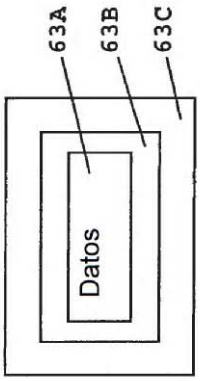

FIG. 5B

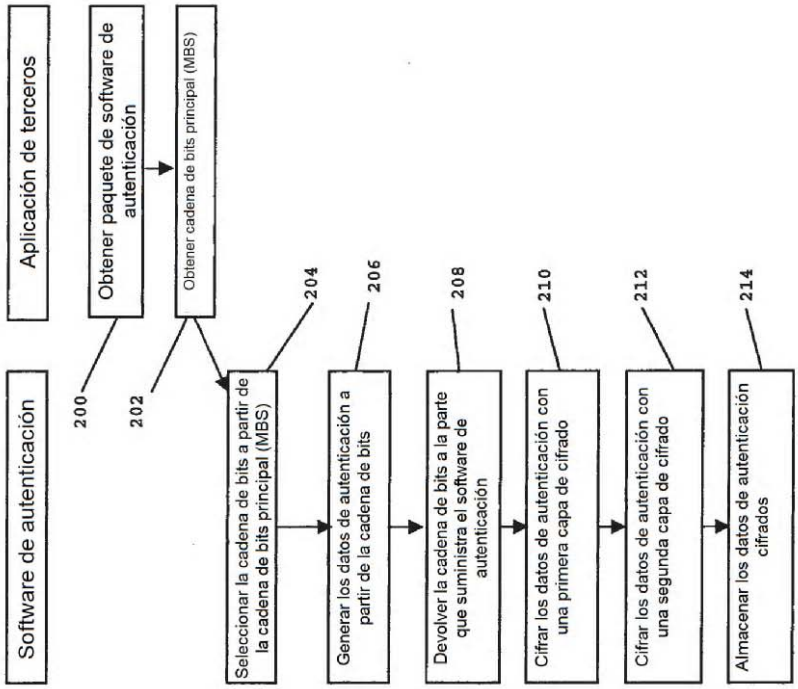

FIG. 4

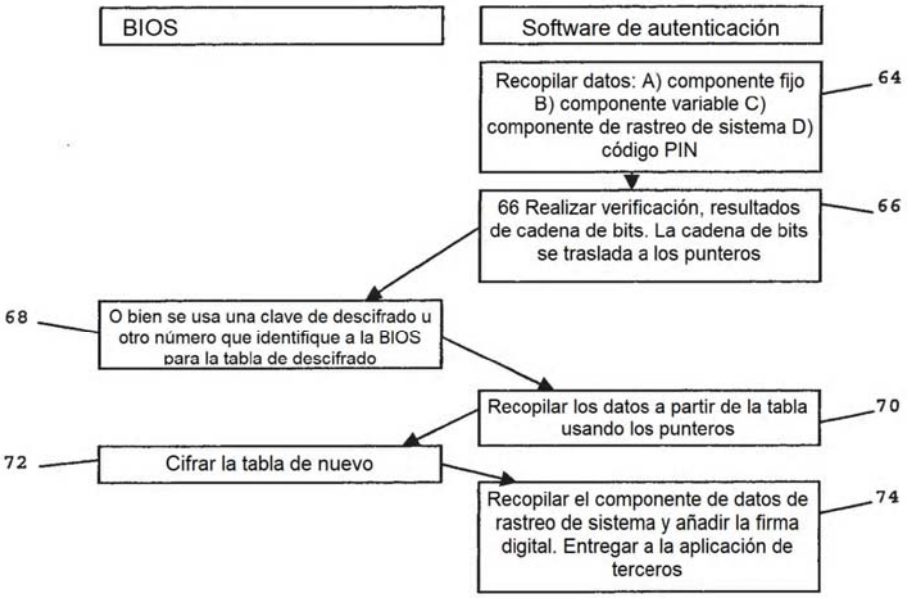
BIOS
Software de autenticación
Recopilar datos: A) componente fijo B) componente variable C) componente de rastreo de sistema D) código PIN
64
66 Realizar verificación, resultados de cadena de bits. La cadena de bits se traslada a los punteros
66
68
O bien se usa una clave de descifrado u otro número que identifique a la BIOS para la tabla de descifrado
Recopilar los datos a partir de la tabla usando los punteros
70
72
Cifrar la tabla de nuevo
Recopilar el componente de datos de rastreo de sistema y añadir la firma digital. Entregar a la aplicación de terceros
74

FIG. 6

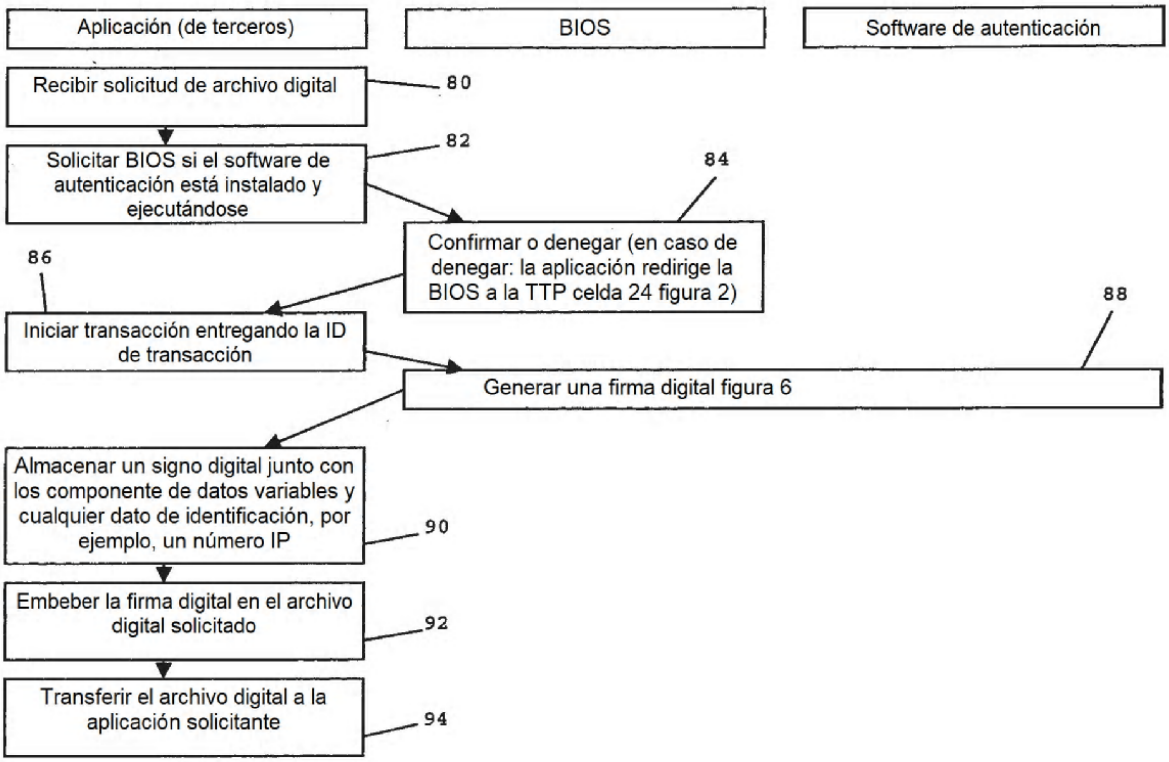
Aplicación (de terceros)
BIOS
Software de autenticación
Recibir solicitud de archivo digital
80
Solicitar BIOS si el software de autenticación está instalado y ejecutándose
82
84
Confirmar o denegar (en caso de denegar: la aplicación redirige la BIOS a la TTP celda 24 figura 2)
86
Iniciar transacción entregando la ID de transacción
88
Generar una firma digital figura 6
Almacenar un signo digital junto con los componente de datos variables y cualquier dato de identificación, por ejemplo, un número IP
90
Embeber la firma digital en el archivo digital solicitado
92
Transferir el archivo digital a la aplicación solicitante
94

FIG. 7

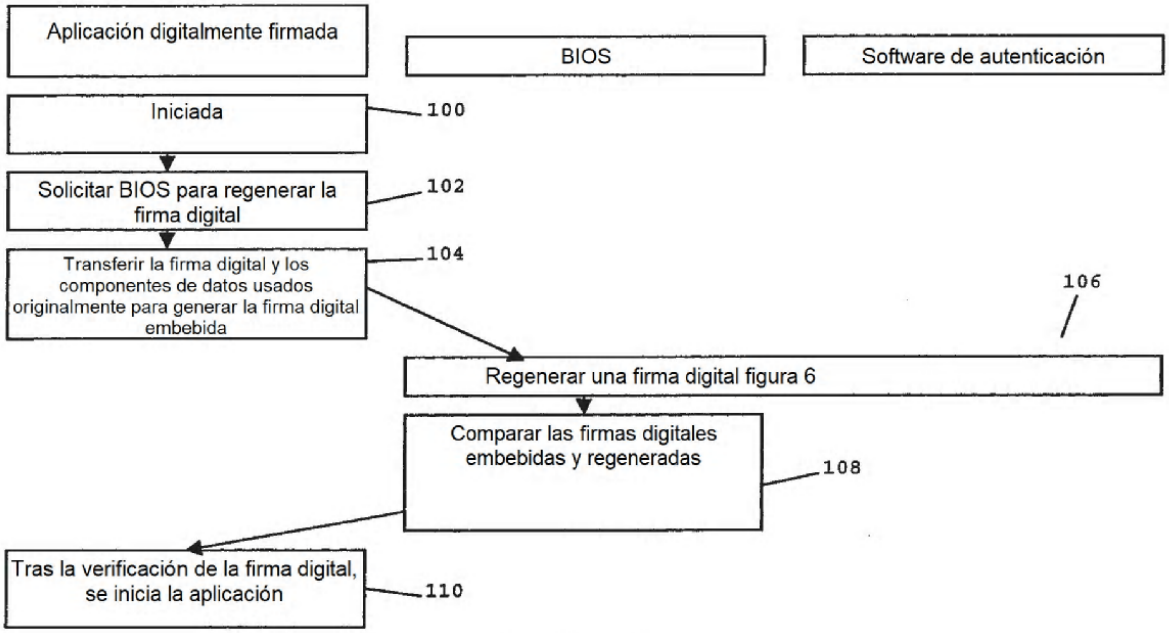
Aplicación digitalmente firmada
BIOS
Software de autenticación
Iniciada
100
Solicitar BIOS para regenerar la firma digital
102
Transferir la firma digital y los componentes de datos usados originalmente para generar la firma digital embebida
104
106
Regenerar una firma digital figura 6
Comparar las firmas digitales embebidas y regeneradas
108
Tras la verificación de la firma digital, se inicia la aplicación
110

FIG. 8

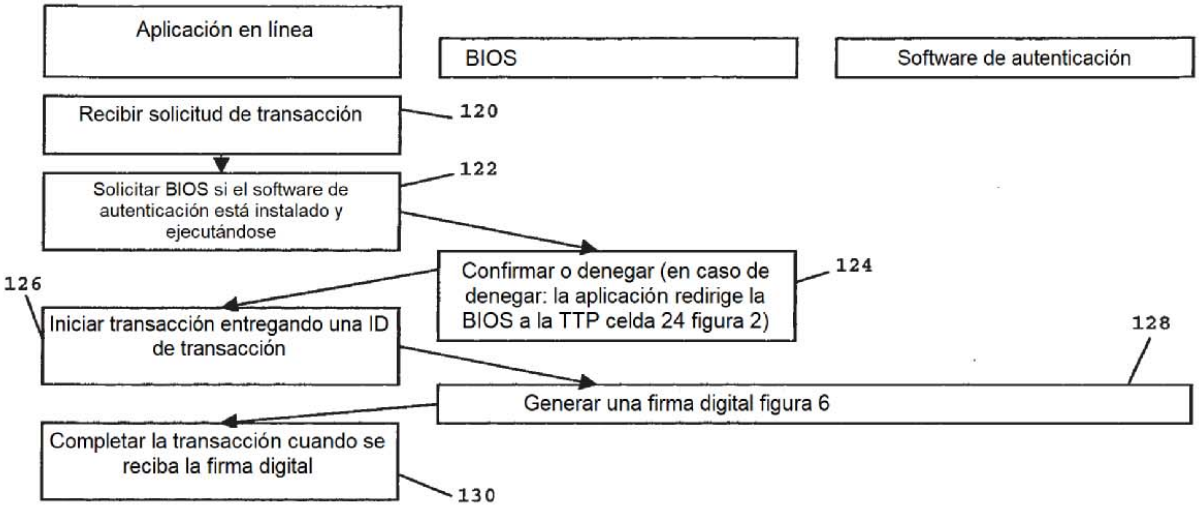
Aplicación en línea
BIOS
Software de autenticación
Recibir solicitud de transacción
120
Solicitar BIOS si el software de autenticación está instalado y ejecutándose
122
Confirmar o denegar (en caso de denegar: la aplicación redirige la BIOS a la TTP celda 24 figura 2)
124
126
Iniciar transacción entregando una ID de transacción
128
Generar una firma digital figura 6
Completar la transacción cuando se reciba la firma digital
130

FIG. 9

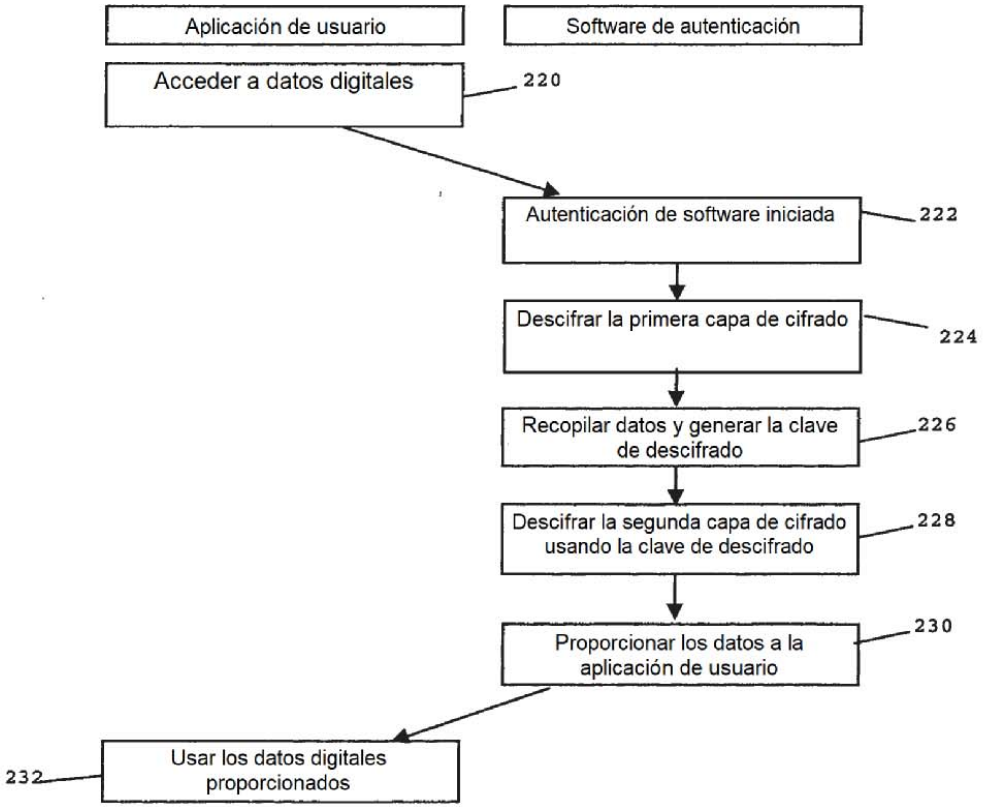
Aplicación de usuario
Software de autenticación
Acceder a datos digitales
220
Autenticación de software iniciada
222
Descifrar la primera capa de cifrado
224
Recopilar datos y generar la clave de descifrado
226
Descifrar la segunda capa de cifrado usando la clave de descifrado
228
Proporcionar los datos a la aplicación de usuario
230
Usar los datos digitales proporcionados
232

FIG. 10