(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 792 177**

(51) Int. CI.:

H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **29.05.2007 E 07290670 (4)**

(97) Fecha y número de publicación de la concesión europea: **01.04.2020 EP 1868316**

(54) Título: **Procedimiento y dispositivo de autentificación de un usuario**

(30) Prioridad:

13.06.2006 FR 0605240

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.11.2020

(73) Titular/es:

INGENICO GROUP (100.0%)
28-32 Boulevard de Grenelle
75015 Paris, FR

(72) Inventor/es:

NACCACHE, DAVID

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento y dispositivo de autentificación de un usuario

La presente invención se refiere a un procedimiento y un dispositivo de autentificación de un usuario. En particular, la invención se refiere a la producción de contraseñas de un solo uso.

Se conoce la autentificación por contraseña. El usuario mantiene en secreto la contraseña para evitar que un tercero tenga el mismo derecho de acceso. La capacidad de producir la contraseña se considera una prueba y es suficiente para que un organismo o servicio administrativo autorice el acceso del usuario. La técnica de contraseña es parte de las autentificaciones llamadas "débiles".

Un inconveniente de este procedimiento está relacionado con la naturaleza estática de la información de autentificación: un tercero puede descifrar la contraseña, después de lo cual accede con el mismo derecho que el usuario. Los sistemas de contraseña de un solo uso (o "contraseñas de una sola vez", en adelante OTP) proporcionan una solución a este problema, en que las contraseñas son válidas para una sola transacción.

Entre estos sistemas, se conocen sistemas del tipo asíncrono o de desafío/respuesta. Cuando un usuario desea autentificarse con un servidor, este servidor genera un desafío (por ejemplo, aleatorio) y se lo transmite al usuario. El usuario se enfrenta al desafío en un dispositivo de cliente. Este dispositivo genera a continuación la OTP mediante algoritmos de cifrado y “hash”. El usuario transmite la OTP al servidor, que tiene todas las informaciones para verificarla, como consecuencia de lo cual el usuario es autentificado.

Se conocen además los sistemas síncronos, en los que el funcionamiento general sigue siendo el mismo, excepto en que el desafío corresponde a la hora actual (por lo tanto, está implícito) o a un contador interno del dispositivo (por ejemplo, un número incrementado en cada utilización). El dispositivo de cliente es, por ejemplo, un identificador de autentificación (o "token"), que el usuario lleva consigo y que se utiliza para generar contraseñas a partir de las cuales el servidor puede autentificar al usuario. Un identificador de autentificación puede tomar varias formas: tarjeta, calculadora de bolsillo, llavero, etc. Esta última técnica es más simple porque el usuario no necesita enfrentarse al desafío. A cambio, requiere una sincronización entre el dispositivo de cliente y el servidor.

Por ejemplo, el sistema SecurID de RSA comprende un dispositivo de cliente (es decir, un identificador o “token”) que genera contraseñas de un solo uso basadas en el tiempo y en un secreto compartido. Más específicamente, los dispositivos en cuestión contienen una clave simétrica única, combinada con un algoritmo que genera un código cada 60 segundos. Asociado con un código personal del usuario, dicho dispositivo permite obtener una autentificación fuerte. Al ser dinámica la cifra obtenida, es difícil de predecir. Por lo tanto, es difícil para un hacker adivinar el código correspondiente a un momento dado. Se utiliza una tecnología especial para sincronizar cada dispositivo con el servidor de seguridad.

El documento de patente WO 2005/029746 describe igualmente un ejemplo de dispositivo de cliente, o identificador, que produce contraseñas de un solo uso, de tipo temporal, desafío/respuesta o cronológico.

Un primer inconveniente de este sistema es que el dispositivo de cliente produce una contraseña a intervalos regulares, lo que a veces es inútil o incluso incompatible con ciertas aplicaciones. Esto además consume energía.

Otro inconveniente proviene de que un atacante que haya capturado el secreto compartido podría reproducir las contraseñas. Por lo tanto, un riesgo es el ataque en horquilla (también "hi-jacking"). En efecto, la autentificación se realiza en el momento de la conexión. Después de esta autentificación, no se verifica que la autentificación aún sea correcta. Además, es posible desviar una comunicación, por ejemplo, del tipo TCP/IP o una transmisión DTMF. Una vez que se ha completado el desvío, el servidor dialoga con el atacante, y el atacante usa la sesión de la víctima.

Por lo tanto, existe la necesidad de una solución simple a los inconvenientes mencionados anteriormente. El objeto de la invención es un procedimiento de autentificación de un usuario mediante un servidor, y un dispositivo de autentificación de un usuario correspondiente según las reivindicaciones independientes. Modos de realización preferidos son definidos por las reivindicaciones dependientes.

Según un aspecto de la invención el procedimiento comprende:

- el suministro de un dispositivo de cliente provisto de una función de cifrado de las variables *K, t, x*, en el que:

  - *K* es un secreto compartido por el servidor y el dispositivo de cliente;

  - *t* es una variable dependiente del tiempo; y

  - *x* es una variable que toma al menos dos valores,

- una etapa de cálculo por parte del dispositivo de cliente de un primer valor de la función obtenido para un primer valor de *x*, para la autentificación del usuario por parte del servidor; y

- una etapa de cálculo por parte del dispositivo de cliente de un segundo valor de la función, obtenido para un segundo valor de x, para la verificación de la autentificación del usuario por parte del servidor.

Según otros aspectos, el procedimiento según la invención comprende una o más de las siguientes características:

- el procedimiento según la invención comprende, además, después de la primera etapa de cálculo, las etapas:

  - de suministro del primer valor al servidor;
  - de autentificación del usuario por parte del servidor, utilizando el primer valor proporcionado; y
  - de solicitud del usuario hacia el servidor,

el procedimiento comprende, además, después de la segunda etapa de cálculo, las etapas:

  - de suministro al servidor de al menos parte del segundo valor; y
  - de verificación de la autentificación del usuario por parte del servidor, utilizando dicha al menos una parte del segundo valor;

- el procedimiento de autentificación según la invención comprende, además, entre las etapas de cálculo, una etapa de:

  - recepción por parte del usuario de un desafío por parte del servidor, relativa al menos a una parte del segundo valor de dicha función;

- en una y/u otra de las etapas de cálculo, la función se toma en un valor concatenado de las variables *K, t* y *x*;

- la variable *x* se codifica en un bit; y

- la función incluye una función hash.

Otro aspecto de la invención se refiere a un dispositivo de autentificación de un usuario, provisto de una función de cifrado para las variables *K, t, x*, en la que:

- *K* es un secreto compartido con un servidor;

- *t* es una variable dependiente del tiempo; y

- *x* es una variable que toma al menos dos valores,

comprendiendo el dispositivo:

- medios para calcular los valores de la función para cada uno de dichos al menos dos valores de *x*.

Según otros aspectos, el dispositivo según la invención comprende una o más de las siguientes características:

- el dispositivo según la invención comprende, además:

  - medios para la modificación por el usuario de la variable *x*; y

  - medios para que el usuario active el cálculo por el dispositivo de los valores de la función;

- los medios de modificación y activación están combinados;

- el dispositivo según la invención comprende además medios de visualización de un valor de la función, que comprende secciones de presenta distintas, estando el dispositivo adaptado para presentar partes de un valor de la función en secciones de visualización respectivas.

- los medios de cálculo están adaptados para calcular un valor de la función tomado en un valor concatenado de las variables *K, t* y *x*; y

- la variable *x* se codifica en un bit.

Otras características y ventajas de la invención aparecerán al leer la siguiente descripción detallada de los modos de realización de la invención, dados a modo de ejemplo solamente y con referencia a los dibujos adjuntos, que muestran:

- La Figura 1: un diagrama de flujo que ilustra las etapas del procedimiento según un modo de realización de la invención; y

- La Figura 2: un ejemplo de un dispositivo de cliente según la invención.

La invención proporciona un procedimiento y un dispositivo de autentificación de un usuario, basado en una función de

cifrado que utiliza un secreto compartido y una variable de tiempo, para la producción de contraseñas de un solo uso. La función también depende de una variable adicional, cuyo valor puede cambiar el usuario, si es necesario. Este cambio en el valor interviene, por ejemplo, después de un desafío del servidor, que puede ocurrir como consecuencia de una solicitud del usuario. Por una parte, el momento en que se cambia la contraseña no es predecible. Por otro lado, el valor del argumento cambia y, por lo tanto, el valor de la función. Dadas las propiedades habituales de las funciones de cifrado, un ataque por horquilla es mucho más difícil que con un sistema OTP convencional. El usuario puede comunicar preferiblemente solo una parte de la nueva contraseña y esto, de acuerdo con un desafío de servidor simplificado. Esto mejora sustancialmente la ergonomía del sistema. El principio subyacente al procedimiento según la invención permite verificar simplemente la autentificación del usuario, en particular para otorgar una solicitud de este último.

Con referencia a la figura 1, el procedimiento proporciona una etapa de cálculo (etapa S30) por un dispositivo de cliente de un primer valor de una función $f(K, t, x)$.

La variable K es un secreto compartido por el servidor y el dispositivo de cliente. Normalmente se trata de una clave secreta, es decir, una clave única que los dos corresponsales son normalmente los únicos que saben. Como se sabe en la técnica, la seguridad del cifrado depende de la confidencialidad atribuida a esta clave común.

La variable t depende de una forma u otra del tiempo. Es típicamente una variable de tiempo actual. Para evitar problemas de sincronización durante la verificación posterior en el lado del servidor, se pueden asignar intervalos de tiempo, por ejemplo, como se conoce en la técnica. También es posible implementar la variable t como un número incrementado en cada conexión (por lo tanto, que evoluciona con el tiempo). Se conocen otras diversas técnicas para implementar el secreto y la variable de tiempo en la técnica.

Según la invención, la función depende además de la variable x, que toma al menos dos valores. Con este fin y según una variante, esta variable puede codificarse en un bit, que se ejemplificará a continuación.

La función f es una función típicamente adaptada al cifrado o “hash” o incluso al código de autentificación del mensaje (o MAC para el código de autentificación del mensaje). Es preferiblemente una función “hash” o, de lo contrario, duplicada de una función “hash” (por ejemplo, MD5, SHA o evoluciones de estas últimas), que comprende un algoritmo “hash”. Como se conoce en la técnica, dicha función hace corresponder los valores de un gran conjunto de valores a un intervalo reducido de valores. El algoritmo permite crear una "huella" digital de un mensaje inicial.

Más precisamente, para una función “hash” f, se requiere que: $f(n) \neq f(m)$ implique $n \neq m$ y $f(n) = f(m)$ implique muy probablemente que $n = m$. Si el conjunto del que se extrae n es mayor que el conjunto de los valores tomados por f, esta última propiedad es difícil de evaluar. De hecho, en un contexto criptográfico, se busca una función f tal que para todos los n del que se conoce el “hash” $f(n)$, entonces es muy difícil (es decir, técnicamente imposible o muy improbable) calcular un m tal que $f(n) = f(m)$.

En una realización particularmente simple y eficiente, la función se toma como un valor concatenado de las variables K, t y x. El cálculo efectuado puede corresponder así al de:

$$f(C = t\ K\ x) \equiv f(K,t,x)$$

La variable x puede ser, por ejemplo, un bit adicional, tomado en cuenta al nivel del hash. La codificación de x en un bit adicional es particularmente simple y ventajosa, ya que es suficiente para proporcionar dos valores posibles para la variable x.

Como ejemplo, la variable de tiempo se puede codificar en un octeto, como el número 11001010. El secreto o la clave pueden tener, por ejemplo, el valor de la cadena **10110010101001111010101011000010 10** (aquí en negrita para distinguirlo de otros valores). Entonces se podrá intentar formar:

(i)

$$f(K,t,x = 0) = f(11001010\mathbf{10110010101001111010101011000010 10}0);$$

o

(ii)

$$f(K,t,x = 1) = f(11001010\mathbf{10110010101001111010101011000010 10}1).$$

La etapa de cálculo anterior se realiza para un primer valor de x, por ejemplo, $x = 0$.

Esta etapa de cálculo es, si es necesario, seguida de una etapa de suministro (etapa S40) de un resultado de $f(K,t,x = 0)$ hacia el servidor. Este resultado puede proporcionarse por cualquier medio al servidor, dependiendo de la configuración de hardware considerada. En particular, este resultado puede ser enviado por el dispositivo de cliente después de la validación del usuario, cuando este dispositivo está conectado al servidor (por ejemplo, a través de un puerto USB, a través de un ordenador de cliente conectado al servidor por Internet). En una variante, este resultado es presentado por el dispositivo de cliente, gracias a lo cual este resultado puede ser comunicado al servidor por el propio usuario, en

particular cuando el dispositivo no está conectado.

El procedimiento según la invención comprende entonces una etapa de autentificación (etapa S50) del usuario, usando un resultado de un cálculo equivalente al cálculo anterior. Concretamente, el servidor conoce el secreto, el tiempo o el intervalo de tiempo y, por lo tanto, tiene la información necesaria para autentificar al usuario, una primera vez. Tal principio es conocido en la técnica, excepto que aquí, el argumento es transformado por la variable *x*, y en consecuencia el valor de la función *f*.

Preferiblemente, durante una solicitud (etapa S80) del usuario hacia el servidor o, alternativamente, después de esta solicitud (etapa S70), el usuario comunica al servidor al menos una parte de un segundo valor de función *f* calculada por el dispositivo de cliente para un segundo valor de *x* (por ejemplo, $x = 1$ anterior). La modificación del valor de *x* puede ser realizada por el propio usuario. Este punto se describirá con referencia a la Figura 2.

El servidor puede verificar entonces la autentificación según el propio principio de autentificación. Por lo tanto, el acceso posterior a la solicitud del usuario puede estar subordinado a la verificación de autentificación por parte del servidor.

Obsérvese que, según este principio, no es necesario que el dispositivo informe al usuario de cada nueva contraseña susceptible de ser producida para $x = 0$. El usuario solo tiene que solicitar el dispositivo cuando no es necesario. Por lo tanto, el usuario puede, por ejemplo, solicitar o controlar el dispositivo una primera vez para autentificarse ($x = 0$) y luego solicitarlo una segunda vez para la edición de una nueva contraseña ($x = 1$), lo que permite al servidor verificar la autentificación.

Un ejemplo de aplicación es el de un usuario que gestiona una cuenta bancaria de forma remota. El usuario es autentificado una primera vez (como en la etapa S50) por el servidor bancario. Esta autentificación le permite acceder a informaciones relativas a su cuenta bancaria. Luego, cuando el usuario desea realizar una operación en su cuenta (solicitud del usuario), el servidor puede someter la validación de esta operación (es decir, conceder la solicitud) con la condición de que el usuario responda correctamente a un desafío que emana del servidor.

El servidor emite un desafío relativo a $f(K,t,x = 1)$. Este desafío es recibido por el usuario (etapa S90).

Preferiblemente, el servidor podría emitir un desafío relacionado solo con parte del resultado de $f(K,t,x = 1)$, por ejemplo, que no se relaciona más que con dos dígitos de dicho resultado (lo que, en la práctica, proporciona una protección suficiente para la verificación de la autentificación). Por lo tanto, el usuario solo tiene un número reducido de caracteres para comunicar a servidor. La ergonomía del procedimiento resulta así mejorada.

Además, la parte del resultado que se comunicará al servidor puede ser elegida aleatoriamente por este último. Por ejemplo, el servidor puede solicitar que se le comuniquen las dos primeras cifras o las dos cifras siguientes, etc. del resultado y esto, según un sorteo aleatorio (por lo tanto, no predecible). Esto reduce aún más la posibilidad de piratería. Con este fin, se describirá un dispositivo particularmente ventajoso con referencia a la figura 2.

Cuando el usuario responde correctamente al desafío, se le puede conceder su solicitud (etapa S140).

La figura 2 muestra un ejemplo de dispositivo 10 de cliente según la invención. Este dispositivo permite la autentificación de un usuario, así como la verificación de esta autentificación, como se ilustra anteriormente.

Este dispositivo está provisto de medios para calcular valores de la función *f(K,t,x)* de esta función para uno y otro de dichos al menos dos valores de *x*. El dispositivo también comprende medios 16 de modificación por el usuario de la variable *x*. Estos medios son, por ejemplo, en forma de un simple botón. Una presión de este botón permite cambiar de $x = 0$ a $x = 1$.

El dispositivo 10 comprende además medios 16 de activación por parte del usuario del cálculo por el dispositivo de los valores de la función; así como medios 20 de visualización de un valor de la función. Estos medios pueden ser, por ejemplo, una pantalla de cristal líquido.

Por lo tanto, en un modo de realización, el dispositivo puede presentar por defecto una contraseña correspondiente al secreto y a la variable de conexión o de tiempo actual (por ejemplo, un intervalo de tiempo actual). Esta contraseña puede permitirle ser autentificado por el servidor en un momento dado. Más tarde, en respuesta a un desafío del servidor, el usuario presiona este botón. Entonces se cambia el valor de *x*.

Preferiblemente, los medios 16 de modificación y de activación 16 se combinan. De esta manera, cuando el usuario presiona el botón 16, hace aparecer simultáneamente el resultado del cálculo de $f(K,t,x = 1)$.

Preferiblemente también, los medios de visualización comprenden secciones 23 – 25 de visualización distintas. Estas secciones pueden obtenerse, por ejemplo, delimitando secciones en la pantalla 20 de visualización o previendo pantallas separadas. El experto en la materia, por ejemplo, buscará espaciar la visualización de los caracteres entre las secciones, para facilitar su lectura.

Además, el dispositivo está adaptado para presentar partes de un valor de la función en las respectivas secciones 23, 24, 25 de visualización. Por lo tanto, el usuario tiene un dispositivo ergonómico, en conexión con el procedimiento descrito

anteriormente. Como se describió anteriormente, el servidor puede hacer recaer el desafío sobre una de estas secciones. Por ejemplo, el desafío puede ser: "Introduzca las dos cifras presentadas en la sección A". Después de este desafío y en el ejemplo de la figura, el usuario deberá introducir el número 89.

Con referencia al ejemplo de aplicación descrito anteriormente, desafíos típicos, asociados con operaciones en una cuenta bancaria podrían ser:

- para leer su saldo, presione el botón de derivación 16 e introduzca el número que aparece debajo de la letra C; y

- para solicitar un nuevo talonario de cheques, presione el botón de derivación 16 e introduzca el número que aparece debajo de la letra B.

Alternativamente, el dispositivo podría incluir una pantalla de LCD con diez secciones de visualización distintas, puestas en correspondencia con letras, por ejemplo, ABCDEFGHIJ.

En una variante, el desafío puede ser implícito. Por ejemplo, una operación de transferencia desde la cuenta bancaria del usuario está implícitamente asociada con el suministro del número presentado en la sección A, según un procedimiento preestablecido o llevado a la atención del usuario por defecto. En este caso, el usuario proporciona al servidor el número correspondiente (por ejemplo, tomando este número en un cuadro de solicitud) al mismo tiempo que proporciona la solicitud.

Según otra variante, el dispositivo comprende además medios 12 para la conexión al servidor, para transmitir un valor de la función hacia el servidor, por ejemplo, un puerto USB 12. Por lo tanto, el suministro de valores de la función de $f(K,t,x)$ puede transmitirse directamente desde el dispositivo de cliente, cuando éste está conectado al servidor, por ejemplo, a través de un ordenador personal del usuario y de la red Internet.

Si es necesario, solo los valores de $f(K,t,x = 0)$ pueden enviarse al servidor para la autentificación. Al contario, el dispositivo puede diseñarse de modo que los valores de $f(K,t,x = 1)$ solo estén disponibles para visualización, para mayor seguridad.

Según otra variante, el dispositivo podría estar provisto de dos secciones de visualización principal distintas (por ejemplo, dos pantallas de LCD distintas). Una mostraría los valores de $f(K,t,x = 0)$, mientras que la otra podría mostrar los valores de $f(K,t,x = 1)$. De esta forma, los valores de $f(K,t,x = 0)$ y de $f(K,t,x = 1)$ están disponibles en la visualización y el usuario puede ver cada uno de estos valores en cualquier momento. Por lo tanto, no se necesita activar el cálculo de $f(K,t,x = 1)$ mediante una acción específica. El dispositivo no tiene que estar provisto de botón. Además, dentro de cada una de las secciones de visualización principales, el dispositivo podría presentar partes de los valores de la función f en subsecciones de visualización distintas, a la manera de las secciones de visualización 23, 24, 25.

La invención se aplicará así ventajosamente a terminales de pago. Por ejemplo, se podría intentar hacer corresponder un desafío con una cantidad de una transacción realizada por medio de éste, por ejemplo, en un comerciante.

La invención tampoco se limita a las variantes descritas anteriormente, pero es susceptible de numerosas otras variaciones fácilmente accesibles para el experto en la materia. Como ejemplo, es posible implementar una función de hash con tolerancia a los errores. También es posible someter el uso del dispositivo de cliente a la validación de una contraseña personal estática, etc.

REIVINDICACIONES

1. Un procedimiento de autentificación de un usuario por un servidor, que comprende:

- el suministro de un dispositivo de cliente provisto de una función de cifrado para las variables K, t, x, en la que:

  - K es un secreto compartido por el servidor y dispositivo de cliente;

  - t es una variable dependiente del tiempo; y

  - x es una variable que toma al menos dos valores,

- una primera etapa de cálculo (S30) por parte del dispositivo de cliente de un primer valor de la función obtenida para un primer valor de x, para la autentificación del usuario por el servidor;

- una etapa de suministro (S40) de dicho primer valor de dicha función al servidor;

- una etapa de autentificación (S50) del usuario por parte del servidor, utilizando dicho primer valor suministrado;

- una etapa de solicitud (S70, S80) del usuario hacia el servidor para efectuar una operación sobre una cuenta bancaria;

- una segunda etapa de cálculo (S80, S110) por el dispositivo de cliente de un segundo valor de la función, obtenido para un segundo valor de x, para la validación de dicha operación por parte del servidor;

- una etapa de suministro (S110, S80) al servidor de al menos una parte de dicho segundo valor de dicha función;

- una etapa de validación de dicha operación (S130) por parte del servidor, utilizando dicha al menos una parte de dicho segundo valor de dicha función; y

- una etapa de tratamiento de dicha operación (S140) después de dicha validación de la operación.

2. El procedimiento de autentificación según la reivindicación 1, caracterizado por que, en uno y/o el otro de las etapas de cálculo (S30), (S80, S110), se toma la función en un valor concatenado de las variables K, t y x.

3. El procedimiento de autentificación según una cualquiera de las reivindicaciones 1 y 2, caracterizado por que la variable x está codificada en un bit.

4. El procedimiento de autentificación según una cualquiera de las reivindicaciones 1 a 3, caracterizado por que la función comprende una función “hash”.

5. Dispositivo de autentificación de un usuario, provisto de una función de cifrado de las variables K, t, x, en la que:

- K es un secreto compartido con un servidor bancario;

- t es una variable dependiente del tiempo; y

- x es una variable que toma al menos dos valores,

comprendiendo el dispositivo

- medios de cálculo de un primer valor de la función obtenido para un primer valor de x, para la autentificación del usuario por parte del servidor;

- medios de suministro de dicho primer valor de dicha función al servidor;

- medios de emisión de una solicitud del usuario hacia el servidor para efectuar una operación sobre una cuenta bancaria;

- medios de cálculo de un segundo valor de la función, obtenido para un segundo valor de x, para la validación de dicha operación por parte del servidor y para el tratamiento de dicha operación después de dicha validación de dicha operación; y

- medios de suministro al servidor de al menos una parte de dicho segundo valor de dicha función;

6. El dispositivo según la reivindicación 5, caracterizado por que el dispositivo comprende, además:

- medios (16) de modificación por parte del usuario de la variable x; y

- medios (16) de activación por parte del usuario del cálculo por el dispositivo de valores de la función.

7. El dispositivo según la reivindicación 6, caracterizado por que los medios (16) de modificación y de activación se

combinan.

8. El dispositivo según la reivindicación 5, 6 o 7, caracterizado por que el dispositivo comprende además medios (20) de visualización de un valor de la función, que incluyen secciones (23 - 25) de visualización distintas, estando el dispositivo adaptado para presentar partes de un valor de la función en secciones (23 – 25) de visualización respectivas.

9. El dispositivo según una de las reivindicaciones 5 a 8, caracterizado por que los medios de cálculo están adaptados para calcular un valor de la función tomada en un valor concatenado de las variables K, t y x.

10. El dispositivo según una de las reivindicaciones 5 a 9, caracterizado por que la variable x está codificada en un bit.

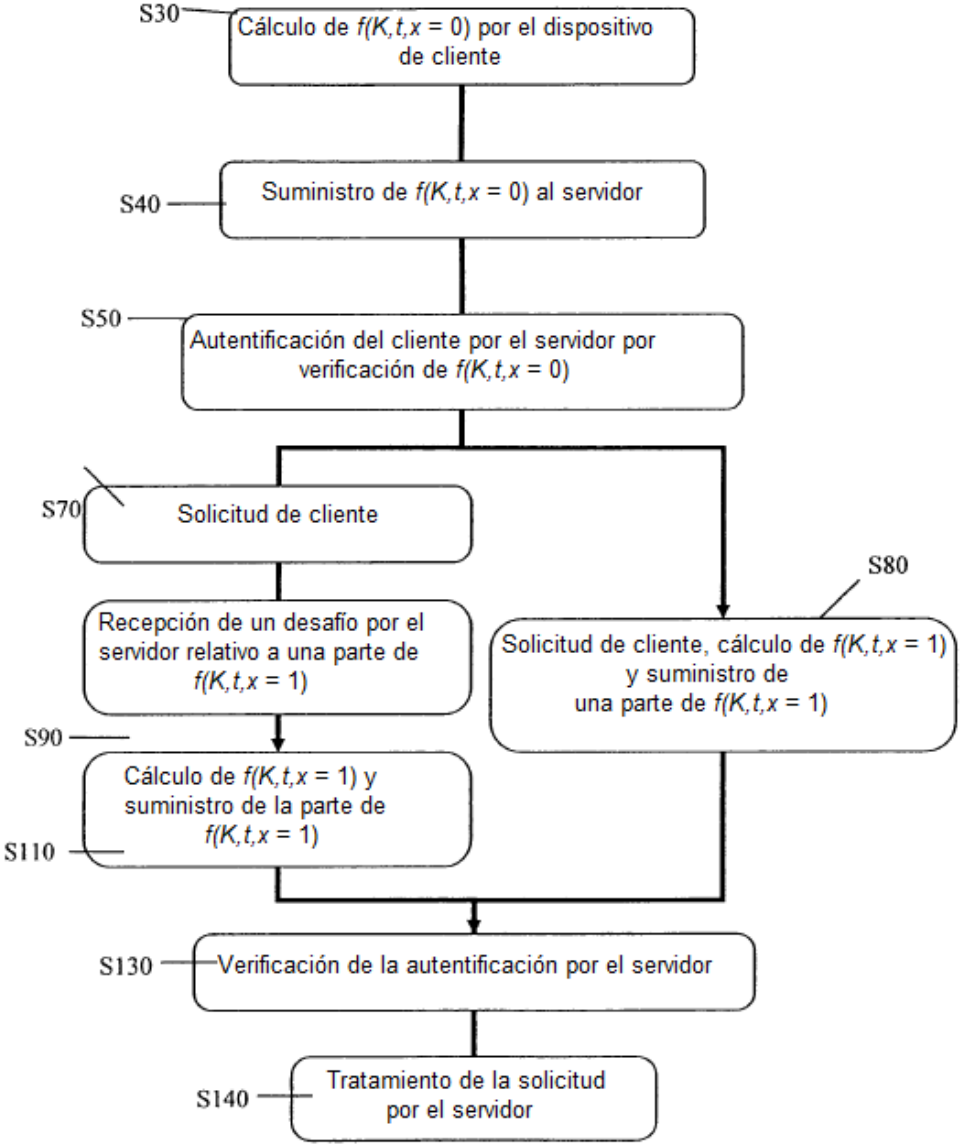
S30
Cálculo de f(K,t,x = 0) por el dispositivo de cliente
S40
Suministro de f(K,t,x = 0) al servidor
S50
Autentificación del cliente por el servidor por verificación de f(K,t,x = 0)
S70
Solicitud de cliente
S80
Recepción de un desafío por el servidor relativo a una parte de f(K,t,x = 1)
Solicitud de cliente, cálculo de f(K,t,x = 1) y suministro de una parte de f(K,t,x = 1)
S90
Cálculo de f(K,t,x = 1) y suministro de la parte de f(K,t,x = 1)
S110
S130
Verificación de la autentificación por el servidor
S140
Tratamiento de la solicitud por el servidor

Fig. 1

Fig. 2