(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 739 710**

(51) Int. CI.:

H04L 9/32 (2006.01)
G06Q 20/32 (2012.01)
G06Q 20/38 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **14.10.2011 PCT/FR2011/052408**

(87) Fecha y número de publicación internacional: **26.04.2012 WO12052664**

(96) Fecha de presentación y número de la solicitud europea: **14.10.2011 E 11787705 (0)**

(97) Fecha y número de publicación de la concesión europea: **08.05.2019 EP 2630746**

(54) Título: **Procedimiento y sistema de autenticación**

(30) Prioridad:

20.10.2010 FR 1058585

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.02.2020

(73) Titular/es:

WORLDLINE (100.0%)
80 Quai Voltaire, Immeuble River Ouest
95870 Bezons, FR

(72) Inventor/es:

CAUCHIE, STÉPHANE

(74) Agente/Representante:

STEPHANN, Valérie

DESCRIPCIÓN

Procedimiento y sistema de autenticación

Campo técnico de la invención

La invención se refiere a un procedimiento y sistema de autenticación de una entidad generalmente llamada Probador ante otra actividad llamada Verificador, así como a un programa informático.

La invención se inscribe en el campo de los mecanismos de autenticación que permiten asegurar el acceso de un usuario a unos servicios.

Estado de la técnica anterior

Los mecanismos de autenticación se implementan en general en el marco del acceso a unos servicios a través de canales de comunicaciones llamados de seguridad entre unos dispositivos adecuados para intercambiar datos.

En dichos casos, es esencial tener un medio de reconocimiento mutuo, es decir un medio que permita a la entidad Verificadora, por ejemplo un servidor de autenticación, autenticar a un proveedor, el terminal de un usuario, y que le permita de ese modo tener acceso a los datos o a los servicios deseados.

Existen numerosos ejemplos que necesitan la implementación de este tipo de comunicación de seguridad. Se pueden citar, en concreto, el caso de los terminales móviles o fijos adecuados para utilizarse durante transacciones de tipo bancario, distribuidores automáticos de billetes o también decodificadores de televisión de pago o de unos derechos de acceso a recursos o localizaciones.

En este contexto, se utilizan frecuentemente unos métodos de autenticación que se basan en técnicas criptográficas.

El inconveniente de estos métodos reside en el hecho de que estas dos entidades, es decir el Verificador y el Probador, deben cooperar mutuamente y secretamente.

Esta condición siempre no se verifica. En efecto, una persona malintencionada puede procurarse el dispositivo de tipo Verificador y analizarlo para conocer su estructura interna. A continuación, esta persona es entonces técnicamente capaz de realizar falsos dispositivos de autenticación, porque las claves secretas están presentes en los dos extremos de la red, es decir en el Verificador y en el Probador.

Esta persona puede interceptar igualmente y analizar los intercambios de información entre el Probador y el Verificador y tratar a continuación de reproducir unas autenticaciones ya efectuadas.

Para paliar este inconveniente, se conoce en la técnica anterior un mecanismo de autenticación de tipo desafío/respuesta, en el que el Probador busca asegurar al Verificador, que es aquel que pretende ser probando que posee un secreto.

Para ello, el Verificador somete a un desafío al Probador que debe superarlo. De manera clásica, un protocolo de autenticación de tipo desafío/respuesta comprende el intercambio de datos entre el Verificador, por ejemplo un servidor de autenticación, y un Probador, por ejemplo el terminal del usuario.

El Probador prueba al Verificador que conoce el secreto que el Verificador comparte con el usuario sin enviar este secreto en claro sobre la red. Para ello, el Verificador envía un desafío al proveedor.

El proveedor utiliza este desafío y el secreto suministrado por el usuario para calcular una respuesta que devuelve al Verificador. Por su parte el Verificador ha efectuado una operación con el desafío que ha expedido al proveedor y el secreto que comparte con el usuario. Compara entonces los resultados y considera que el secreto suministrado por el usuario es correcto cuando los resultados son idénticos. El principio del desafío/respuesta impone que el desafío sea único para cada autenticación de manera que cualquiera que escuchara el canal de comunicación que une el Verificador al proveedor no pueda reproducir los datos de autenticación capturados.

Se conoce, igualmente, una normalización de autenticación de tipo desafío/respuesta, tal como se define por OATH (acrónimo inglés de Open AuTHentication; OCRA basado en RFC 4226 y definido en el sitio de hipertexto siguiente: http://www.ietf.org/id/draft-mraihi-mutual-oath-hotp-variants-11.txt), que prevé la utilización de una contraseña de utilización única ("One Time Password", OTP).

El documento WO 2007/068099 A1 describe un procedimiento de autenticación de un probador ante un verificador.

Sin embargo, un inconveniente principal de dicho sistema está ligado al hecho de que las claves criptográficas que implementan pueden ser robadas por una persona maliciosa que podrá autenticarse entonces a escondidas del

usuario sin que el Verificador pueda detectar una usurpación de ese tipo.

Se conocen otros sistemas de autenticación de la técnica anterior como los que implementan dos elementos de autenticación, refiriéndose un primero a un secreto conocido del usuario y un segundo destinado a demostrar que un dispositivo de hardware en posesión del usuario participa igualmente en cada transacción de autenticación. Así el usuario es capaz de protegerse contra riesgos de usurpación dándose cuenta de que ya no está en posesión del dispositivo de hardware. Sin embargo, uno de los inconvenientes de estos sistemas es que el secreto, generalmente llamado PIN (Personal Identification Number), debido a las capacidades de memoria del ser humano, tiene una entropía reducida. Además, una autenticación de ese tipo es débil porque el secreto es estático.

Exposición de la invención

La invención se dirige a resolver el problema vinculado a las dificultades técnicas encontradas con el fin de mejorar la seguridad de los mecanismos de autenticación.

La invención ofrece ventajas gracias a un procedimiento de codificación y a la utilización de protocolos particulares de proponer un mecanismo de autenticación dinámico y de seguridad, adaptado a canales de comunicación comprendidos entre unos Probadores y un Verificador lógico que tengan velocidades de datos reducidas.

Con este propósito, un aspecto de la invención se refiere a un procedimiento de autenticación de un Probador ante un Verificador que incluye etapas de generación por el Verificador de un desafío en función de una transacción dada y de las características del Probador y el envío de este desafío a dicho Probador, dicho Probador es adecuado para transmitir a dicho Verificador una contraseña de utilización única resultante de la transformación de la respuesta generada por el Probador para dicho desafío.

La contraseña de utilización única generada dinámicamente está en un formato legible para el usuario porque se refiere a una serie de palabras y/o cifras, o también otras representaciones gráficas que el usuario puede memorizar fácilmente y a continuación introducir en el Probador con el fin de su transmisión al Verificador. El procedimiento comprende una etapa de introducción de un código PIN por el usuario sobre el Probador, anteriormente a la generación de la respuesta a dicho desafío. La etapa de generación de una respuesta se realiza a partir de operaciones de cálculos efectuados a la vez en función del desafío recibido, del código PIN introducido y de al menos un elemento de criptografía.

Según unos modos de realización particulares:

- el procedimiento comprende:
  - una etapa previa de descarga de un programa informático a partir de la selección de un enlace de hipertexto comprendido en un mensaje recibido por dicho Probador, y
  - una etapa de activación de dicho programa informático a partir de elementos criptográficos del Verificador y de al menos un secreto compartido entre el Probador y el Verificador;
- el procedimiento comprende una etapa de verificación por el Probador, de la validez de un desafío recibido del Verificador;
- la contraseña de utilización única generada a continuación es esta respuesta cifrada con el fin de ser transmitida al Verificador y
- el secreto compartido es un código de activación generado por el Verificador y transmitido previamente al Probador.

La invención se refiere igualmente a un sistema de autenticación que incluye un Probador y un Verificador, siendo adecuado dicho Verificador para generar un desafío en función de una transacción dada y de las características del Probador y para trasmitir dicho desafío al Probador, siendo adecuado dicho Probador para transmitir a dicho Verificador a través de un canal de comunicación una contraseña de utilización única resultante de la transformación de la respuesta generada para dicho desafío por los medios de tratamiento del Probador.

Según unos modos de realización particulares:

- el Probador se elige entre uno de los elementos siguientes: un terminal móvil, un terminal fijo o una tarjeta de chips;
- el Verificador es un servidor de autenticación y
- el canal de comunicación tiene una velocidad de datos reducida.

La invención se refiere igualmente a un programa informático que incluye instrucciones para la ejecución de las etapas del procedimiento de autenticación cuando dicho programa se ejecuta por los medios de tratamiento del Probador.

En un modo de realización, el programa informático se prevé para ser descargado a partir de un enlace de hipertexto de manera que quede archivado en los medios de memoria del Probador.

La invención se define por las reivindicaciones.

Breve descripción de las figuras

Surgirán otras características y ventajas de la invención con la lectura de la descripción que sigue, con referencia a la figura adjunta, que ilustra en la figura 1, una vista esquemática del mecanismo de autenticación según un modo de realización de la invención.

Descripción detallada de un modo de realización

La presente invención prevé controlar el acceso a numerosos servicios condicionando este acceso al resultado de una autenticación.

Se trata en un contexto de ese tipo de verificar que el usuario que desea acceder a un servicio es aquel que pretende ser y que dispone de las autorizaciones necesarias para acceder a ello.

Para hacer esto, el sistema ilustrado en la figura 1, comprende un Probador y un Verificador, ambos unidos por un canal de comunicación. Este sistema comprende igualmente un servidor asociado al Verificador a partir del que el Probador es adecuado para descargar un programa informático tal como se define en la presente invención.

En el ámbito de la invención, el Probador se considera como un elemento no de seguridad tal como un terminal móvil.

En el presente modo de realización se considera que el Probador es un terminal de tipo equipo de comunicación móvil o fijo capaz de comunicar de manera bidireccional con un Verificador por medio de ondas a través de una red de comunicación móvil (o celular) y una red local inalámbrica (de tipo WLAN, WiFi, Bluetooth, Wimax o infrarrojos) o también por medio de un enlace por cable (enlace coaxial, fibra óptica, etc.).

Este terminal se refiere por ejemplo a un teléfono móvil (o celular), a un asistente digital personal (o PDA, o también un teléfono inteligente), a un ordenador portátil, a una tableta digital multimedia o también a cualquier otro equipo informático portátil que pueda archivar y ejecutar un programa informático.

Este término corresponde a todos los equipos que comprenden:

- al menos un microprocesador,
- memoria volátil y/o no volátil y/o en masa,
- medios de introducción, tal como un teclado y/o un ratón y/o pantalla táctil o también a unos medios de mando por voz,
- unos medios de presentación y
- unos medios de comunicación.

Los medios de comunicación de este terminal se refieren por ejemplo a las tecnologías y/o normas siguientes: Bluetooth y/o IrDA (Infrared Data Association), y/o WI-FI (abreviatura de wireless fidelity) y/o Wimax y GPRS (General Packet Radio Service), GSM, UMTS, HSDPA o IMS (IP Multimedia Subsystem), o también Ethernet.

Se observará, en particular, que estos medios de comunicación son compatibles con los del Verificador.

El microprocesador y la memoria volátil y/o no volátil y/o en masa contribuyen a permitir a este terminal ejecutar el código que se refiere a un programa informático. Este código puede ser de tipo Java™.

El Verificador es un servidor de autenticación que incluye en concreto unos medios de tratamiento adaptados para la generación de desafíos y la verificación de las respuestas, a los desafíos recibidos, en la forma de contraseña de utilización única más comúnmente conocidas bajo el término inglés "One Time Password" (OTP).

Este Verificador incluye igualmente unos medios de comunicación compatibles con los de un Probador.

El procedimiento de autenticación según la invención es del tipo desafío/respuesta pudiendo funcionar en modo conectado y no conectado.

Se observará que en el procedimiento de autenticación según la invención la etapa de inscripción (o de activación) se realiza necesariamente en el modo conectado, lo que no es obligatoriamente el caso de las otras etapas sucesivas.

En modo conectado, este procedimiento comprende una etapa previa durante la que el usuario descarga un programa informático a partir de un enlace de hipertexto comprendido en un mensaje recibido por el Probador.

Este mensaje puede ser por ejemplo un mensaje de tipo SMS enviado por el servidor asociado al Verificador, cuando el terminal es un terminal móvil de comunicación.
La activación del envío de este mensaje se inicia por el usuario del terminal durante la sesión preliminar con un servidor asociado al Verificador, durante una etapa de inscripción en el servicio deseado, dando al usuario el acceso a una página web a partir de la que puede efectuar una solicitud de obtención de este programa informático. Recibe entonces simultáneamente un código de activación de este programa, un código de tipo PIN, así como elementos de información que le señalan el envío de este mensaje.

Durante esta etapa de activación, el Verificador genera unos parámetros utilizados en el procedimiento de autenticación, ejecutando a partir de estos medios de tratamiento las operaciones de cálculo adecuadas para implementar un código que se refiere a una primitiva "initSystem":

$$initSystem: 1^k \rightarrow \pi_{verificar} = \{K_{1,\dots,V,verificar} \times W\}$$

En la que:

- k, un parámetro de seguridad;
- *W*, un conjunto de parámetros del sistema, y
- $K_{1,\dots,V,verificar}$, el conjunto de los elementos criptográficos de tipo claves maestras simétricas, y las claves asimétricas.

El conjunto *W* de los parámetros del sistema define particularmente:

- el tamaño del diccionario de palabras y,
- el tamaño del almacén de claves asimétricas del Probador

Durante esta etapa de activación se inicializan entonces las credenciales del Verificador, es decir: las claves asimétricas que aseguran la confidencialidad y las claves simétricas maestras que permiten la deducción de las claves de los Probadores para la autenticación de este y la verificación de los desafíos.

El programa informático descargado se archiva a continuación en los medios de memoria del Probador durante una etapa de instalación y se activan a continuación.

Durante la etapa de activación, o también de inscripción del Probador, los medios de tratamiento del Probador son adecuados para realizar operaciones de cálculo para la implementación del código de programación relativo a una primitiva "enroll":

$$enroll: \pi_{verificar} \times P \rightarrow \{K_{1,\dots,P,probar} \times W\}$$

En la que:

- $\pi_{verificar}$, corresponde a los parámetros $K_{1,\dots,V,verificar}$, del Verificador,
- *P,* identificador del Probador que se desea autenticar (identificador que sirve datos para la deducción de las claves criptográficas simétricas de dicho Probador)
- *W*, conjunto de parámetros del sistema,
- $K_{1,\dots,V,probar}$, el conjunto de los elementos criptográficos de tipo claves derivadas simétricas y las claves asimétricas.

De este modo, Esta etapa de activación permite efectuar la inscripción del Probador con el fin de que sea conocido por el Verificador y que este último pueda autenticarlo posteriormente.

Durante esta etapa se define:

- el conjunto de las claves simétricas de autenticación respectivamente de verificación: clave calculada por derivación a partir de las claves maestras de autenticación, respectivamente de verificación y
- el diccionario común con el Verificador.

El programa informático activado se implementa por los medios de tratamiento del Probador en el marco de la autenticación del usuario del Probador con el fin de que este pueda aprovechar un servicio tal como un servicio de pago durante una transacción.

El procedimiento según la invención prevé un protocolo particular de autenticación en el marco de los intercambios

de datos entre el Verificador y el Probador.

Para hacer esto, el Verificador generará un desafío contextual en una transacción dada y en función de las características del Probador.

Este contexto transaccional se refiere a datos que contribuyen a su unicidad (por ejemplo; ficha de fechado, identificación de los actores, valores monetarios, valores aleatorios, ...).
Las características del Probador se refieren a:

- su identificador (por ejemplo: número de teléfono en el caso de un terminal de telefonía móvil o también la dirección física MAC) suministrado previamente al Verificador.
- claves públicas del Probador y
- claves de informaciones relativas a los dispositivos utilizados.

Este desafío generado por el Verificador se dirige a hacer única la transacción entre este Verificador y el Probador.

El desafío se genera entonces por el Verificador durante operaciones de cálculo realizadas por sus medios de procesamiento para la implementación de un código relativo a la primitiva "*genChallenge*":

$$genChallenge: T \times P \times K \rightarrow Ch$$

En la que:

- T, corresponde a los datos relativos a la transacción
- *P,* se refiere a la identificación del proveedor que se desea autenticar,
- *K,* corresponde a un elemento criptográfico tal como la clave simétrica de autenticación y de verificación maestras y
- *Ch,* se refiere al desafío.

Durante esta etapa se genera entonces un desafío y se podrá verificar por el Probador que es emitido por el Verificador.

Para ello el procedimiento utiliza una primitiva de deducción de la clave con la clave maestra de verificación y el identificador del Probador, como diversificador, con el fin de determinar la clave de verificación deducida de dicho Probador.

Esta última clave permite entonces al Verificador firmar (por ejemplo MAC acrónimo de "Message Authentication Code", que significa código de autenticación del mensaje, por ejemplo el algoritmo HMC-SHA1 o cualquier otro algoritmo de autenticación de mensajes) la transacción para la que se va a autenticar el Probador.

Se comprende que si este procedimiento de autenticación fuera:

- sin desafío, entonces habría una posibilidad de reproducción y
- sin desafío firmado entonces tendría la posibilidad de autenticación del Verificador, pero un atacante podría solicitar una autenticación a un Probador sin que este pueda estar seguro de la identidad del usuario solicitante (Verificador o atacante). Esto evita unos ataques "man in the middle"

El desafío generado por el Verificador se trasmite a continuación al Probador.

El Probador verificará en un primer momento la validez del desafío recibido. Para hacer esto los medios de tratamiento del Probador ejecutarán el código que se refiere a la primitiva "*verifChallenge*":

$$verifChallenge: Ch \times K \rightarrow \{0,1\}$$

En la que:

- *Ch,* el desafío recibido por el Probador,
- *K,* un elemento criptográfico que corresponde a la clave simétrica de verificación calculada durante la etapa de inscripción y
- {0,1}, resultado susceptible de ser obtenido 0 o 1.

Si el resultado obtenido es 0, entonces el desafío recibido no es válido, en el caso contrario el resultado será igual a 1.

Cuando el desafío no es válido el procedimiento de autenticación se aborta. De este modo, puede verificarse la procedencia del desafío. En efecto, el Probador verifica gracias a la utilización de la clave simétrica de verificación

que el Verificador emitió correctamente el desafío en curso.

Cuando el Probador se refiere a un terminal, este desafío se comunica entonces al usuario a partir de los medios de presentación de este terminal.

Una vez efectuada esta verificación y siendo válido el desafío, el Probador a través de sus medios de presentación invita al usuario a introducir un código. Se considera en el presente modo de realización de este código es por ejemplo un código de tipo código PIN.
Esta invitación a introducir un código PIN se realiza a partir de la ejecución por los medios de tratamiento de un código relativo a la primitiva "*askPIN*":
AskPIN: U → Pwd
En la que:

- U, se refiere al usuario y
- Pwd, el código PIN a introducir.

Esta introducción del código PIN desencadena entonces, la generación por los medios de tratamiento del Probador de una respuesta. Esta respuesta se refiere a los datos criptográficos producidos por el Probador y corresponden a la respuesta esperada por el Verificador para un desafío dado.

Esta respuesta se genera por tanto a partir de operaciones de cálculo realizadas por los medios de tratamiento del Probador ejecutando el código relativo a la primitiva "*genResponse*" siguiente:

$$genResponse: Ch \times Pwd \times K \times W \rightarrow Rp$$

En la que:

- *Ch,* el desafío recibido por el Probador;
- Pwd, el código PIN introducido;
- *K,* un elemento criptográfico tal como la clave simétrica de autenticación recibida durante la fase de inscripción;
- *W*, un conjunto de parámetros del sistema, y
- *Rp,* la respuesta al desafío dado.

Se observará que la generación por el Probador de la respuesta no es "marshallizada", es decir no transmisible en el canal de comunicación en el estado.

Para hacer esto, el proveedor utiliza un procedimiento de firma o MAC con la clave de autenticación (HMAC-SHA1 por ejemplo). Dicho Probador puede firmar entonces el desafío recibido, con el PIN del usuario.

De ese modo el procedimiento de autenticación tiene en cuenta a la vez el desafío y el PIN. En el presente modo de realización, el Probador no es una tarjeta de chips de tipo SIM porque en estas condiciones el código PIN estaría controlado localmente y por tanto atacable.

La respuesta obtenida se transcribe a continuación bajo el formato de la contraseña de utilización única, más comúnmente conocida con el término inglés "One Time Password" (OTP). Esta transcripción en OTP de la respuesta permite convertir la respuesta a un formato que pueda ser más fácilmente memorizable por un usuario que la de una respuesta en un formato complejo, propia de los datos criptográficos.

De ese modo se facilita la transmisión por el usuario con el Probador, de esta respuesta en el formato OTP.

La codificación de la respuesta en OTP se realiza en un formato que se refiere a una serie de palabras fácilmente memorizable por el usuario; Esto tiene como efecto incrementar la velocidad del canal de transmisión.

En efecto, unos estudios han demostrado que el ser humano es capaz de retener una frase que incluya hasta 12 palabras. La OTP generada en la presente invención es susceptible de adaptarse a esta capacidad del ser humano.

Considerando el tamaño del canal definido por la función:

$$VELOCIDAD: MENSAJE \times P \rightarrow \mathrm{N}^{+}$$

Las codificaciones existentes en una forma legible para el usuario definen el conjunto siguiente: *MENSAJE* = {*Numérico,Alfanumérico*}. La velocidad máxima que se puede esperar de un mensaje se define a continuación:

- *Numérico*: 8 cifras tienen una entropía de 26 bits;
- *Alfanumérico*: 8 cifras tienen una entropía de 40 bits

Para hacer esto, una función biyectiva *codificación*(□), se implementa por el Probador tomando en la entrada una respuesta (*rp* ∈ *Rp*) y unos parámetros (*W*), que devuelve una frase o serie de palabras que respetan la capacidad de memorización citada más arriba.

La transición de la respuesta en OTP se realiza a partir de la implementación del código relativo a la primitiva "*marshall*" durante operaciones de cálculo efectuadas por los medios de tratamiento del Probador.
Esta primitiva "*marshall*" es la siguiente: *marshall:Rp × W → OTP*

En la que:

- *Rp,* la respuesta al desafío dado,
- *W*, un conjunto de parámetros del sistema, y
- *OTP,* contraseña de utilización pública,

De este modo, la respuesta al desafío anteriormente calculado se codifica en una OTP con el fin de que sea transmisible sobre un canal de velocidad limitada.

La OTP generada se transmite entonces al Verificador, durante una etapa de introducción por un usuario de esta OTP en una interfaz generada por el Probador durante por ejemplo una transacción.

Antes de esta transmisión al Verificador, puede cifrarse esta OTP por ejemplo partir de una clave asimétrica, con el fin de que un atacante no pueda determinar el PIN en el caso en que este tuviera acceso a las claves simétricas (ataque sobre el dispositivo del Probador).

El Probador cifra la respuesta gracias al procedimiento siguiente:

- determinación de una clave de sesión, a partir del concepto de pre- "shared key" asimétricas generadas por el Probador durante la inscripción y completada después de cada utilización, las claves públicas se transmiten al Verificador en modo conectado. Estas pre- "shared key" se destruyen después de cada utilización para evitar los ataques a posteriori;
- desplazamiento de la clave privada del Probador con un delta aleatorio. Este desplazamiento se aplica sobre las bi-claves debido a sus propiedades matemáticas de las primitivas utilizadas y
- cifrado de la respuesta y del delta aleatorio con un procedimiento de cifrado por flujo (sin sobrecarga).

En la recepción, el Verificador realiza el descifrado de esta OTP cifrada y efectúa la decodificación de la OTP descifrada a partir de la ejecución por sus medios de tratamiento de la primitiva "*unmarshall*" de manera que obtenga la respuesta generada por el Probador para el desafío dado:

$$unmarshall: OTP \times W \rightarrow Rp$$

En la que:

- P, identificador del Probador (acceso a las claves públicas de este)
- *OTP,* contraseña de utilización única y
- *W*, conjunto de parámetros del sistema.

Con el fin de obtener la respuesta al desafío generada por el Probador, el Verificador determinar la clave de sesión utilizada gracias a su clave privada y la clave pública del usuario. Esta clave de sesión sirve para descifrar la respuesta y el delta de desplazamiento. El delta se aplica a la clave pública del Probador.
Se observará que todos los métodos OTP tienen un método llamado de "unmarshalling".

Sin embargo la utilización de un procedimiento de cifrado/descifrado/desplazamiento asimétrico permite asegurar la confidencialidad de la respuesta (y por tanto del PIN) en modo desconectado.

La respuesta así obtenida forma entonces el objeto de una verificación con el fin de validar la autenticación del Probador y por extensión del usuario.

Para hacer esto, el Verificador efectúa unas operaciones de cálculo a partir de sus medios de tratamiento que se dirigen a la implementación de un código relativo a la primitiva "verifResponse":

$$verifResponse: Rp \times Ch \times Pwd \times K \rightarrow \{0,1\}$$

En la que:

- *Rp,* la respuesta al desafío dado
- *Ch,* el desafío para la transacción en curso;

- *K,* un elemento criptográfico tal como la clave simétrica de autenticación deducida para el Probador.
- Pwd, el código PIN introducido por el usuario del Probador y
- {0,1}, resultado susceptible de ser obtenido 0 o 1.

Si el resultado obtenido es 0, entonces el Probador no está autenticado, en caso contrario el resultado será igual a 1.

Se observará, por otro lado que la utilización, en la invención, de las claves públicas a nivel del Verificador no genera ninguna sobrecarga suplementaria para un módulo de hardware de seguridad del tipo HSM que genera, almacena y protege unas claves criptográficas, debido a la modificación parcial de las claves públicas y privadas.

En efecto, el cifrado por clave asimétrica de la respuesta protege a esta última. Además, el Verificador debe almacenar unas claves públicas suplementarias, fuera de lo que son unas claves públicas y por tanto no sensibles.

De este modo, se entiende que la invención no está limitada a los ejemplos de realización descritos e ilustrados. No está limitada además a estos ejemplos de ejecución ni a las variantes descritas.

REIVINDICACIONES

1. Procedimiento de autenticación de un Probador ante un Verificador que incluye etapas de generación por el Verificador de un desafío en función de una transacción dada y de las características del Probador y el envío de este desafío a dicho Probador, dicho procedimiento está caracterizado por que dicho Probador es adecuado para transmitir a dicho Verificador una contraseña de utilización única resultante de la transformación de la respuesta generada por el Probador para dicho desafío en un formato que pueda ser fácilmente memorizable por un usuario, generándose dicha respuesta por el Probador a partir de operaciones de cálculo efectuadas a la vez en función del desafío recibido, de un código PIN introducido durante una etapa anterior y de un elemento de criptografía.

2. Procedimiento de autenticación según la reivindicación anterior que comprende:

1. una etapa previa de descarga de un programa informático a partir de la selección de un enlace de hipertexto comprendido en un mensaje recibido por dicho Probador y
2. una etapa de activación de dicho programa informático a partir de elementos criptográficos del Verificador y de al menos un secreto compartido entre el Probador y el Verificador.

3. Procedimiento según una de las reivindicaciones anteriores, que comprende una etapa de verificación de la validez del desafío recibido.

4. Procedimiento según una de las reivindicaciones anteriores, en el que la contraseña de utilización única se cifra antes de ser transmitida al Verificador.

5. Procedimiento según la reivindicación 2, en el que el secreto compartido es un código de activación generado por el Verificador y transmitido previamente al Probador.

6. Sistema de autenticación que incluye un Probador y un Verificador, siendo adecuado dicho Verificador para generar un desafío en función de una transacción dada y de las características del Probador y para trasmitir dicho desafío al Probador, caracterizado por que el Probador es adecuado para transmitir a dicho Verificador a través de un canal de comunicación una contraseña de utilización única resultante de la transformación de la respuesta generada para dicho desafío por los medios de tratamiento del Probador en un formato que pueda ser fácilmente memorizable por un usuario, generándose dicha respuesta por el Probador a partir de operaciones de cálculo efectuadas a la vez en función del desafío recibido, de un código PIN introducido durante una etapa anterior y de un elemento de criptografía.

7. Sistema según la reivindicación anterior, en el que el Probador se elige entre uno de los elementos siguientes: un terminal móvil y un terminal fijo.

8. Sistema según una de las reivindicaciones 6 o 7, en el que el Verificador es un servidor de autenticación.

9. Sistema según una de las reivindicaciones anteriores 6 a 8, en el que dicho canal de comunicación tiene una velocidad de datos reducida.

10. Procedimiento de autenticación de un Probador ante un Verificador que incluye unas etapas de recepción de un desafío generado por el Verificador en función de una transacción dada y de las características del Probador y enviada a dicho Probador por el Verificador, dicho procedimiento está caracterizado por que dicho Probador es adecuado para transmitir a dicho Verificador una contraseña de utilización única resultante de la transformación de la respuesta generada por el Probador para dicho desafío en un formato que pueda ser fácilmente memorizable por un usuario, generándose dicha respuesta por el Probador a partir de operaciones de cálculo efectuadas a la vez en función del desafío recibido, de un código PIN introducido durante una etapa anterior y de un elemento de criptografía.

11. Programa informático que incluye instrucciones para la ejecución de las etapas del procedimiento de autenticación según la reivindicación 10 cuando dicho programa se ejecuta por los medios de tratamiento del Probador.

12. Programa informático según la reivindicación anterior, previsto para ser descargado a partir de un enlace de hipertexto de manera que se archive en los medios de memoria del Probador.

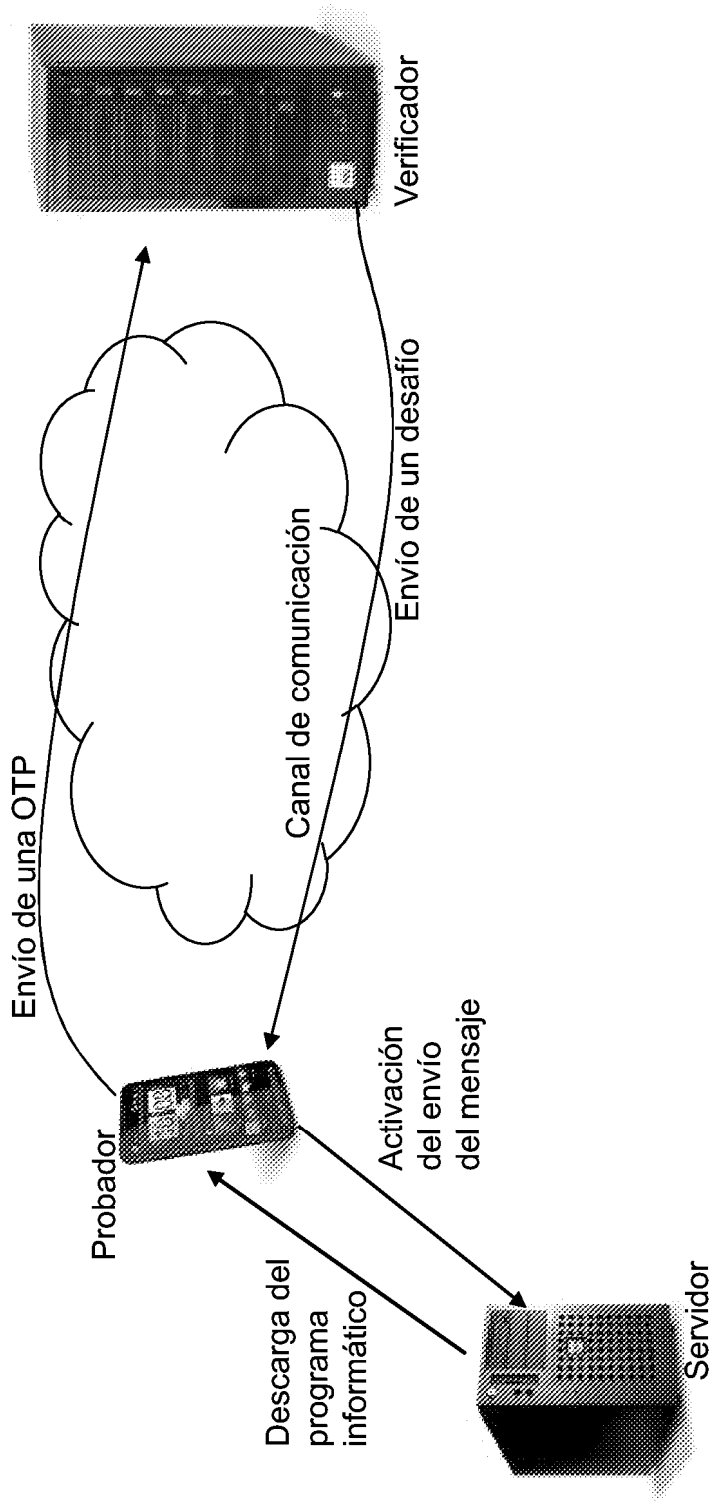
Verificador
Envío de un desafío
Canal de comunicación
Envío de una OTP
Probador
Activación
del envío
del mensaje
Descarga del
programa
informático
Servidor

FIGURA 1