(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 709 223**

(51) Int. CI.:

G06F 21/35 (2013.01)
G06F 21/60 (2013.01)
G06F 21/64 (2013.01)
H04L 9/08 (2006.01)
H04L 9/14 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **10.09.2012 E 12183656 (3)**

(97) Fecha y número de publicación de la concesión europea: **31.10.2018 EP 2568406**

(54) Título: **Procedimiento de utilización, a partir de un terminal, de datos criptográficos de un usuario almacenados en una base de datos**

(30) Prioridad:

09.09.2011 FR 1158042

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.04.2019

(73) Titular/es:

IDEMIA IDENTITY & SECURITY FRANCE (100.0%)
2 place Samuel de Champlain
92400 Courbevoie, FR

(72) Inventor/es:

DAOUPHARS, RAPHAËL;
DESPERRIER, JEAN-MARC y
FOURNIE, LAURENT

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento de utilización, a partir de un terminal, de datos criptográficos de un usuario almacenados en una base de datos

La presente invención se refiere al ámbito técnico de la utilización, de una manera segurizada, de los datos criptográficos de un usuario con vistas a efectuar tratamientos criptográficos mediante estos datos.

En el marco de la presente invención, hay que entender por datos criptográficos del usuario, los datos criptográficos que conviene guardar en secreto para preservar la fiabilidad del tratamiento criptográfico y del proceso en el marco del cual interviene. En el marco, por ejemplo, de un proceso que intervenga en una infraestructura con claves públicas, PKI del inglés Public Key Infrastructure, los datos criptográficos en el sentido de la invención comprenden la clave secreta del usuario que solo debe ser utilizable por este último o con el consentimiento de este último y, eventualmente, conocida por este último por oposición a la clave pública del usuario que puede ser conocida por cualquiera y utilizable por cualquiera sin riesgo de corrupción de los procesos criptográficos que utilizan el par clave pública/clave secreta del usuario.

Para controlar el uso de tales datos criptográficos de un usuario, se conoce la implementación de una tarjeta con chip que comprende un módulo de seguridad en el interior del cual se registran los datos criptográficos del usuario. El acceso a estos datos criptográficos y su utilización en el seno del módulo de seguridad de la tarjeta con chip se controlan entonces mediante un código que solo conoce el usuario que lo introduce en el momento del desbloqueo de la tarjeta con chip. La fiabilidad de una tal tarjeta con chip se ha demostrado sobradamente. Sin embargo, la utilización de una tarjeta con chip impone disponer, a nivel del sistema informático que requiere la utilización de los datos criptográficos del usuario, de un lector de tarjetas con chip y del conjunto de los programas o controladores necesarios para el funcionamiento del lector y el acceso a la tarjeta con chip en sí misma. Sin embargo, esta restricción física e informática no es compatible con la utilización de los sistemas informáticos como los ordenadores portátiles, las tabletas informáticas o los teléfonos inteligentes que raramente ofrecen a posibilidad de utilizar un lector de tarjeta con chip.

Para permitir realizar una firma en un servidor de firma utilizando los datos criptográficos asociados a un usuario específico, el documento US 7.725.723 B2 ha propuesto autentificar a la vez al usuario y al terminal que este utiliza antes de autorizar la firma de los datos transmitidos por el usuario.

Sin embargo, el objetivo que se propone este documento de garantizar que los datos criptográficos estén bajo el control exclusivo del usuario encuentra varias dificultades con los métodos que se proponen en él.

Dado que los datos criptográficos de esta solución están cifrados únicamente mediante el servidor de firma, cualquier otro ataque sobre el servidor de firma, o que utilice el desvío de uno de los administradores de este servidor puede permitir el uso de la clave sin la aprobación de su propietario legítimo.

Más allá de este riesgo, esto tiene otra consecuencia que es la ausencia de un vínculo directo e inmutable que vincule el terminal, el usuario y los datos criptográficos.

La ausencia de un tal vínculo significa que cualquier debilidad en el servidor que condujera a una posibilidad de identificación errónea del terminal, de identificación errónea del usuario, o de error en el vínculo entre el usuario identificado y el dato criptográfico al que tiene acceso, o en caso de se presenten limitaciones en las claves que pueden utilizarse a partir de un terminal dado, de error entre el vínculo entre el terminal y la o las claves autorizadas desde este terminal, da la posibilidad inmediatamente a un usuario equivocado de utilizar los datos criptográficos. La misma posibilidad puede contemplarse para un usuario que no utilice el terminal correcto, y que puede ser así un atacante que consiga robar el secreto del usuario sin llegar a robarle el terminal.

Además, los diversos medios de autentificación propuestos en el documento que se basa en secretos idénticos presente a la vez a nivel del usuario o del terminal y del servidor tampoco permiten aportar propiedades de no repudio, que garanticen que solo los secretos en posesión exclusiva del usuario o de su terminal hayan podido permitir abrir legítimamente el canal.

Para intentar superar esta dificultad, el documento propone en concreto utilizar un servidor de autentificación que transmite únicamente un elemento derivado del secreto al servidor de firma y no el secreto en sí mismo. El usuario o el terminal calculan entonces el valor derivado antes de enviarlo al servidor que lo compara con el que ha recibido.

Pero un atacante que haya conseguido tomar posesión del valor derivado almacenado en el servidor puede contentarse con enviarlo directamente y ser autentificado con éxito. Como el servidor no recibe el secreto original no puede garantizar realmente que el usuario está realmente en su posesión. Por tanto, este método no aporta verdaderamente una ventaja real respecto del envío directo por una y otra parte del secreto y en particular no permite el no repudio de la autentificación.

Así que, por lo tanto, la mayoría de los métodos de autentificación enseñados por el documento vuelve a la comparación directa de un secreto enviado por el usuario con el almacenado en el servidor, o bien a la utilización de

un método de autentificación externa física previamente proporcionado al usuario. Esto presenta el mismo inconveniente que el uso de una tarjeta con chip.

Además, según este documento, el terminal no está vinculado de manera exclusiva a un usuario específico. Esto significa que *a priori* es posible utilizar la clave de cualquier usuario del que no se haya podido obtener un elemento de identificación a partir de cualquier terminal reconocido por el sistema. Esto es un resultado del objetivo de itinerancia, en inglés «roaming», sobre la utilización de la clave dada por el documento, pero debilita altamente la seguridad que debería aportarse por la doble autentificación del terminal y del portador.

El documento propone una implementación en la que el secreto que el usuario debe utilizar para autentificarse se le envía mediante un mensaje de tipo SMS. Para implantar una doble autentificación real con este tipo de medio, el usuario debe disponer a la vez de este teléfono por un lado para recibir el SMS, y de otro terminal utilizado en la conexión, porque la doble autentificación no es real si se utiliza el mismo elemento físico para recibir el código y para la autentificación del terminal.

Por tanto, la solución descrita no puede utilizarse para aportar un nivel de seguridad utilizando un elemento terminal único, sin requerir ninguna otra fuente material.

Además, los ejemplos de ataques recientes en los que los defraudadores han conseguido obtener en lugar del usuario legítimo el envío por parte del operador telefónico de una tarjeta SIM de sustitución asociada a un mismo número de teléfono y así poder recibir el mensaje de autentificación en lugar del usuario han demostrado la debilidad de este tipo de solución que en realidad no autentifica físicamente el terminal del usuario, sino su número de teléfono. Con este tipo de ataque, la seguridad de la parte de autentificación del usuario descrita puede verse comprometida, y el acceso al terminal o a una copia del secreto fijo que porta son suficientes entonces para utilizar los datos criptográficos del usuario, sin que los medios propuestos por el documento aporten una solución.

En definitiva y vistos los ataques conocidos actualmente, la solución solo aporta un nivel de seguridad elevado de la autentificación del usuario cuando está disponible un medio físico de autentificación externo, lo que representa una limitación importante en su implantación.

El documento US2003/0204732 A1 divulga también un método que permite a un usuario acceder desde un cliente en red a un secreto criptográfico almacenado en forma cifrada en un servidor. Este método utiliza un cifrado a partir de una clave establecida sobre la base de un secreto del servidor y de una contraseña presente en una ficha de seguridad del usuario. Este método requiere por tanto también la utilización de una ficha material.

Ha surgido por tanto la necesidad de un nuevo procedimiento de utilización de datos criptográficos de un usuario que, por un lado, ofrezca garantías de seguridad equivalentes e incluso superiores a las de una tarjeta con chip pero que no presente las mismas limitaciones materiales en lo que respecta al dispositivo informático que requiere la utilización de datos criptográficos del usuario y, por otro lado, que permita aportar una solución a los fallos de los procedimientos según la técnica anterior mencionados anteriormente.

Para alcanzar este objetivo, la invención se refiere a un procedimiento de utilización, mediante un módulo de seguridad, de los datos criptográficos de un usuario almacenados en una base de datos, mediante un terminal para uso del usuario y que comunica con el módulo de seguridad a través de una red de comunicación, procedimiento que comprende las etapas siguientes:

- una secuencia de autentificación que comprende las siguientes etapas sucesivas:

    - autentificación mutua entre el módulo de seguridad y el terminal, que se basa en un protocolo de criptografía asimétrica, que establece un canal de seguridad entre el módulo de seguridad y el terminal;

    - en caso de autentificación mutua positiva del módulo de seguridad y del terminal, autentificación mutua del módulo de seguridad y del usuario;

- en caso de autentificación mutua positiva entre, por un lado, el módulo de seguridad y el terminal y, por otro lado, el módulo de seguridad y el usuario:

    - obtención de los datos criptográficos del usuario mediante el módulo de seguridad en la base de datos, los datos criptográficos están almacenados en la base de datos en una forma cifrada mediante al menos una primera clave de cifrado establecida a partir de al menos una clave secreta del terminal y del elemento de autentificación del usuario y de una segunda clave de cifrado del elemento de autentificación del usuario y de una segunda clave de cifrado propia del módulo de seguridad, el cifrado mediante la segunda clave de cifrado interviene después del cifrado mediante la primera clave de cifrado;

    - cálculo por el terminal de la primera clave de cifrado;

    - envío a través del canal segurizado mediante el terminal al módulo de seguridad, de la primera clave de cifrado;

    - utilización de los datos criptográficos del usuario mediante el módulo de seguridad después del descifrado,

mediante el módulo de seguridad de los datos criptográficos del usuario al menos mediante en primer lugar la segunda clave de cifrado y después de la primera clave de cifrado.

Según la invención, la utilización de los datos criptográficos del usuario solo es posible en caso de autentificación positiva del usuario **y** de autentificación positiva del terminal, así como de autentificación positiva del módulo de seguridad. El cúmulo de estas dos autentificaciones permite una seguridad muy alta.

Efectivamente, la autentificación es un proceso que requiere la utilización de un dato que, normalmente, solo es susceptible de estar poseído por el elemento que hay que autentificar. Este dato generalmente es secreto o solo puede obtenerse a partir del elemento que hay que autentificar. La identificación se distingue de la autentificación en que para la identificación se utiliza un dato, generalmente denominado identificador, que no es necesariamente secreto y puede ser ampliamente conocido o divulgado. De este modo, la identificación sola no ofrece una gran garantía de seguridad, en la medida en que un identificador puede ser utilizado por un tercero que haya tenido acceso dado el carácter público o casi público de este identificador. En un par identificador/autentificador, el identificador puede utilizarse como índice que permite encontrar el autentificador que se va a utilizar para proceder a la operación de autentificación. Así, la autentificación puede considerarse en ciertos casos, como la combinación de una identificación y de la verificación de la posesión de un secreto o de una información particularmente difícil de obtener. Debe observarse que, en un sistema electrónico utilizado por una sola persona, la autentificación solo puede hacer intervenir la verificación del conocimiento del secreto o de la información considerada difícil de obtener.

En el caso de la autentificación de un usuario, a menudo se utiliza como dato de autentificación una contraseña y una frase conocida solo por el usuario también denominado PIN, del inglés Personal Identification Number. Para permitir una memorización fácil, la contraseña es generalmente corta y solo comprende un número limitado de caracteres, por ejemplo, entre cuatro y seis. Así la contraseña PIN puede encontrarse fácilmente en el contexto de un ataque por fuerza bruta. Para caracterizar esta debilidad se dice que la contraseña PIN presenta una baja entropía.

En el caso de la autentificación de un dispositivo electrónico, el tamaño del dato de autentificación no es un problema y es posible utilizar un dato que presente un gran tamaño y por tanto sea difícil de encontrar en el caso de un ataque por fuerza bruta. El dato de autentificación del terminal presenta por tanto una gran entropía respecto del dato de autentificación del usuario.

La utilización en combinación de la autentificación del usuario y de la autentificación del terminal que utiliza, tal como propone la invención, permite obtener una autentificación que presenta una mayor entropía que la autentificación que resulta de la utilización únicamente de la contraseña del usuario. Según la invención, la etapa de control de la autenticidad del terminal se produce antes de la obtención de los datos criptográficos del usuario por el módulo de seguridad. Así, se evita que los datos criptográficos del usuario transiten hacia el módulo de seguridad antes de que la autentificación del terminal se haya realizado de forma positiva.

En el sentido de la invención, conviene entender por autentificación asimétrica un protocolo en el que una entidad A prueba su identidad a otra entidad B sin revelar información que permita a B usurpar la identidad de A. En la práctica, estos protocolos se utilizan en forma de un intercambio de tipo «desafío/respuesta» a partir de un algoritmo criptográfico asimétrico (RSA, curva elíptica) o de divulgación de conocimiento nulo. Estos protocolos garantizan el no repudio de la prueba de autentificación, porque solo la entidad A es capaz de realizar la secuencia criptográfica que demuestra su identidad.

En el caso de la invención, hay autentificación del terminal, del usuario y del módulo de seguridad, todas estas autentificaciones intervienen antes de la transmisión de la primera clave secreta. Hay que señalar que la autentificación del módulo de seguridad induce una gran fiabilidad del procedimiento según la invención superior a la que resultaría solamente de la autentificación del terminal y del usuario. De hecho, si el servidor se equivoca en la autentificación del usuario, la clave del usuario no será descifrable. En cambio, si hay un error en la autentificación del servidor, los medios para descifrar la clave privada del usuario, a saber, la primera clave de cifrado, se envían a la entidad equivocada.

Según la invención, los intercambios de datos entre el terminal y el módulo de seguridad se realizan en el marco de una comunicación segurizada establecida durante la autentificación mutua lo que aumenta la resiliencia de la invención frente a los ataques o las fugas. Esta autentificación mutua puede efectuarse por ejemplo en el marco de un protocolo SSL, del inglés Secure Sockets Layer, también denominado TLS, del inglés Transport Layer Security. Esta autentificación mutua también puede realizarse en el marco de un protocolo de divulgación nula que utilice una prueba de conocimiento de la clave secreta del terminal y/o una prueba de conocimiento de la contraseña del usuario.

Según la invención, la primera clave de cifrado se establece a partir de al menos la clave secreta del terminal y de la contraseña del usuario. La primera clave de cifrado es establecida entonces por el terminal en cada solicitud de utilización de los parámetros criptográficos del usuario. La primera clave de cifrado así establecida permite garantizar que se está en presencia del terminal y del usuario y que el usuario ha dado, mediante la introducción de su contraseña, su consentimiento para la utilización de sus datos criptográficos. De hecho, el descifrado de los datos

criptográficos del usuario solo puede realizarse mediante la primera clave de cifrado que solo puede establecerse mediante la clave secreta del terminal y de la contraseña del usuario. El correcto descifrado de los datos criptográficos del usuario demuestra efectivamente la posesión de la clave secreta del terminal y el conocimiento de la contraseña del usuario lo que corresponde a una autentificación del terminal y del usuario.

Además, el almacenamiento de los datos criptográficos del usuario en la base de datos en una forma cifrada mediante la primera clave de cifrado establecida a partir de al menos una clave secreta del terminal y del elemento de autentificación del usuario, permite, por un lado, garantizar que esta primera clave de cifrado tenga una gran entropía a través de la utilización de la clave secreta del terminal y, por otro, a través de la utilización del elemento de autentificación del usuario, garantizar que la primera clave de cifrado solo se calcula en presencia del usuario lo que garantiza el no repudio por parte del usuario de la utilización de sus datos criptográficos.

Esta primera clave de cifrado constituye por tanto un elemento esencial de la seguridad de la solución, y la primera fase de autentificación del terminal y del usuario tiene por objeto de la misma manera, si no más, autentificar el servidor respecto del terminal y del usuario, y viceversa, antes de transmitir este secreto.

Según la invención, los datos criptográficos del usuario se cifran por tanto mediante dos etapas de cifrado sucesivas:

- una primera etapa de cifrado de los datos criptográficos del usuario mediante una clave de cifrado elegida entre la primera clave de cifrado y la segunda clave de cifrado;

- una segunda etapa de cifrado del resultado cifrado de la primera etapa de cifrado mediante la clave de cifrado que no se utilizó en la primera etapa.

El almacenamiento de los datos criptográficos del usuario en forma cifrada por último mediante la clave del módulo de seguridad en la base de datos que no está necesariamente integrada al módulo de seguridad evita tener que segurizar la base datos en la medida en que solo el módulo de seguridad puede realizar el descifrado mediante su clave de cifrado que presenta una entropía muy alta. Así, es posible considerar un almacenamiento de datos criptográficos del usuario en el mismo terminal. Un tal almacenamiento local permite al usuario controlar perfectamente la destrucción de los datos criptográficos si lo desea.

Asimismo, la utilización de un módulo de seguridad que comunica con el terminal a través de una red de comunicación permite ahorrarse la presencia de un tal módulo de seguridad en el terminal y facilita por tanto la aplicación del procedimiento según la invención.

En el sentido de la invención, el terminal para el uso del usuario del puede ser cualquier sistema informático móvil o fijo que comprenda, por un lado, una interfaz hombre máquina que permita la transmisión de información del terminal al usuario e inversamente del usuario al terminal y, por otro lado, una interfaz de comunicación con una red de comunicación. El terminal para uso del usuario puede, por ejemplo, ser una estación fija de trabajo, un ordenador personal, un ordenador portátil, una tableta ordenador o incluso un teléfono móvil inteligente también denominado «smartphone», sin que esta lista sea limitativa o exhaustiva.

Por red de comunicación, conviene entender cualquier red de comunicación que permita la transmisión o el intercambio de datos digitales o informáticos entre dos sistemas informáticos diferentes sin importar la distancia que los separe. En el sentido de la invención, el término red de comunicación se refiere tanto, sin que esta lista sea limitativa ni exhaustiva, a:

- las redes locales también denominadas LAN, del inglés Local Area Network, por cable y/o por ondas hercianas;

- las redes amplias también denominadas WAN, del inglés Wide Area Netword, por cable y/o por ondas hercianas;

- la red de Internet;

- las redes de telefonía móvil o fija;

y su combinación, sea cual sea el modo de acceso a estas redes y los protocolos utilizados en estas últimas.

Por módulo de seguridad conviene entender un sistema informático segurizado que comprende un número limitado de instrucciones susceptibles de ser puestas en práctica en el marco de su utilización normal de manera que se limiten los riesgos de uso indebido o de corrupción.

Según la invención, el módulo de seguridad puede ser un módulo de seguridad informático o un módulo de seguridad físico o incluso una combinación de módulo de seguridad informático y físico. Por ejemplo, sin que esta lista sea limitativa ni exhaustiva, se puede considerar:

- un programa informático operado por un sistema de operación reforzado, alojado en un servidor segurizado físicamente o una carcasa inviolable (en inglés Tamper resistant);

- un módulo físico segurizado HSM (del inglés Hardware Security Module) especializado o programable;

- la combinación de los dos, de manera que se realicen las etapas de autentificación mediante un programa segurizado y las etapas de uso de la clave secreta mediante un material segurizado.

La autentificación hace intervenir generalmente una comparación entre un elemento de autentificación transmitido por el sujeto que se va a autentificar y un elemento de autentificación poseído por el sistema que procede a la autentificación. Según una característica de la invención, las etapas de control de autenticidad se realizan mediante:

- al menos un elemento de autentificación del terminal;

- y al menos un elemento de autentificación del usuario;

los elementos de autentificación, obtenidos mediante el módulo de seguridad en la base de datos, están almacenados en la base de datos en una forma cifrada mediante una clave de cifrado propia del módulo de seguridad. Hay que señalar que esta clave de cifrado no es necesariamente la misma que la segunda clave de cifrado utilizada para el cifrado de los datos criptográficos del usuario.

Según la invención, como elemento de autentificación del usuario puede utilizarse bien una contraseña conocida por el usuario solamente o bien un dato biométrico que solo sea posible conocer en presencia del usuario como por ejemplo una huella digital o una imagen de la retina. Según la invención, también pueden utilizarse al menos dos elementos de autentificación del usuario como una contraseña y un dato biométrico.

Según la invención, el elemento de autentificación del terminal puede ser de cualquier naturaleza apropiada. Puede utilizarse por ejemplo un elemento de autentificación del terminal establecido en parte al menos a partir de una clave secreta del terminal almacenada en el terminal. Una tal clave secreta podrá ser ventajosamente una clave de más de 128 bits y preferentemente una clave fuerte de más de 256 bits que ofrezca una entropía importante. El elemento de autentificación del terminal puede comprender entonces la clave secreta en sí misma. Para evitar las divulgaciones de la clave secreta del terminal, el elemento de autentificación se establece, de preferencia, a partir de la clave secreta del terminal sin comprender la clave secreta en sí misma. Así, el elemento de autentificación del terminal puede comprender una prueba de posesión de la clave secreta del terminal destinada a ser utilizada en el marco de un protocolo de autentificación de divulgación nula. La utilización de un tal protocolo de autentificación de divulgación nula, también denominado de divulgación nula de conocimiento, en inglés Zero Knowledge Protocole, permite evitar que la clave secreta se divulgue durante la fase de autentificación.

La implementación preferida de la invención a través de un protocolo de autentificación de tipo «augmented zero knowledge» tiene la ventaja por tanto de basar la autentificación del servidor en elementos de autentificación directamente vinculados uno al secreto del terminal y el otro al secreto del usuario, sin divulgar jamás estos secretos durante un intento de autentificación, antes de transmitirle la primera clave establecida a partir de estos dos elementos conjuntamente. En esta implementación, la seguridad de los elementos de autentificación también es importante y es preferible protegerlos mediante una clave de cifrado propia del módulo de seguridad.

Para facilitar la operación de autentificación, también se puede utilizar un elemento de identificación del terminal que comprenda un identificador del terminal Tid. Un tal elemento de identificación puede utilizarse entonces como índice en la base de datos para encontrar los datos de autentificación utilizados por el módulo de seguridad.

Según la invención, el elemento de autentificación del usuario puede ser de cualquier naturaleza apropiada y, por ejemplo, comprender datos biométricos. Según una forma preferida de realización de la invención, se utiliza un elemento de autentificación del usuario establecido en parte al menos a partir de una contraseña introducida por el usuario. Para preservar la confidencialidad de la contraseña, el usuario la introduce en el terminal en el momento de la autentificación del usuario.

El elemento de autentificación del usuario puede comprender la contraseña en sí misma. Sin embargo, para evitar las divulgaciones de la contraseña del usuario, el elemento de autentificación del usuario se establece de preferencia a partir de la contraseña del usuario sin incluir la contraseña. Así, el elemento de autentificación del usuario puede comprender una prueba de conocimiento de la contraseña destinada a ser utilizada en el marco de un protocolo de autentificación de divulgación nula.

La autentificación del módulo de seguridad por el terminal de seguridad puede realizarse por cualquier medio apropiado conocido por el experto en la materia. Esta autentificación puede realizarse por ejemplo mediante un certificado emitido por una autoridad de certificación tercera. La autentificación del módulo de seguridad también puede realizarse mediante un protocolo de divulgación nula. A este respecto, la prueba de conocimiento establecida a partir de la clave secreta del terminal y/o de la contraseña del usuario, poseída y utilizada por el módulo de seguridad para autentificar el terminal y el usuario en el marco de un protocolo de divulgación nula también puede utilizarse por el terminal para autentificar el módulo en el marco de un protocolo de divulgación nula. Efectivamente, el terminal en posesión de su clave secreta y, en su caso, de la contraseña introducida por el usuario puede calcular la prueba de conocimiento poseída por el módulo de seguridad y asegurarse por tanto de que el módulo de seguridad está en efecto en posesión de dicha prueba de conocimiento.

Según la invención, la base de datos puede grabarse en el módulo de seguridad. Sin embargo, según una variante

de la invención, para evitar «saturar» el módulo de seguridad, la base de datos se registra en un servidor de datos diferente del módulo de seguridad, este servidor de datos comunica con el módulo de seguridad a través de una red de comunicación. Este servidor puede ser entonces el terminal mismo.

Según otra característica de la invención, el módulo de seguridad está integrado en un servidor de seguridad remoto diferente del servidor de datos y del terminal.

Según otra característica más de la invención, la base de datos comprende al menos los siguientes datos asociados a un usuario:

- un elemento de identificación del usuario;

- un elemento de autentificación del usuario;

- un elemento de identificación de al menos un terminal asociado al usuario;

- un elemento de autentificación del terminal;

- los datos criptográficos del usuario.

Para garantizar su confidencialidad, al menos los siguientes datos:

- el elemento de autentificación del usuario;

- el elemento de autentificación del terminal;

- los datos criptográficos del usuario;

están presentes en la base de datos en una forma cifrada mediante al menos una clave de cifrado del módulo de seguridad.

Para garantizar su integridad, al menos los siguientes datos:

- la asociación entre el identificador y el autentificador del usuario,

- la asociación entre el identificador y el autentificador del terminal;

- la asociación entre el identificador y los datos criptográficos del usuario, pueden estar presentes en la base datos en forma firmada mediante una clave de firma del módulo de seguridad.

Según la invención, los datos criptográficos del usuario pueden utilizarse en diferentes procesos y en concreto para garantizar el tratamiento de los diferentes tipos de datos. Según una forma de aplicación de la invención, el módulo de seguridad utiliza los datos criptográficos del usuario para efectuar tratamientos criptográficos en datos que hay que tratar recibidos a través de la red de comunicación y segurizados por el canal segurizado establecido durante la autentificación mutua entre el módulo de seguridad y el terminal.

En el sentido de la invención, los datos que hay que tratar pueden comprender por ejemplo datos utilizados en el marco de un proceso de firma digital de un documento electrónico. Así, los datos que hay que tratar pueden comprender una huella digital del documento electrónico.

Según una característica de la invención, el terminal utiliza un módulo del cliente que gestiona al menos las comunicaciones con el módulo de seguridad, la introducción del elemento de autentificación del usuario, la secuencia de autentificación y el cálculo de la primera clave de cifrado.

Según otra característica de la invención, el módulo del cliente está adaptado para:

- conservar el valor del elemento de autentificación del cliente desde el momento de su introducción por el usuario y hasta el cálculo de la primera clave de cifrado;

- borrar el valor del elemento de autentificación después del cálculo de la primera clave de cifrado;

- borrar el valor de la primera clave de cifrado después de su envío al módulo de seguridad.

Según otra característica más de la invención, el módulo del cliente está adaptado para impedir el acceso al valor del elemento de autentificación del cliente y al valor de la primera clave de cifrado por otro recurso u otro programa, del terminal o externos al terminal, diferente al módulo de seguridad.

Siempre según otra característica de la invención, el módulo del cliente garantiza la transmisión de los datos que hay que tratar al módulo de seguridad.

El módulo del cliente puede realizarse de cualquier manera apropiada y en concreto ser un módulo informático y/o

físico con seguridad reforzada para resistir a los ataques que intentaran «escuchar» la introducción del elemento de autentificación del usuario y el resultado del cálculo de la primera clave de cifrado.

Por supuesto, las diferentes características, variantes y formas de aplicación del procedimiento según la invención pueden asociarse unas con otras según diversas combinaciones en la medida en que no sean incompatibles o excluyentes unas de otras.

Además, otras muchas características de la invención se desprenden de la descripción anexa realizada en referencia a los dibujos que ilustran formas no limitativas del procedimiento, conforme a la invención, de utilización de datos criptográficos de un usuario.

- La figura 1 ilustra de manera esquemática un posible contexto de aplicación de la invención.

- La figura 2 ilustra de manera esquemática las diferentes etapas de una primera forma del procedimiento, según la invención, de utilización de datos criptográficos de un usuario en el marco del contexto ilustrado en la figura 1 para la firma numérica de un documento electrónico.

- La figura 3 ilustra de manera esquemática otro contexto posible de aplicación de la invención.

- La figura 4 ilustra de manera esquemática las diferentes etapas de una segunda forma del procedimiento, según la invención, de utilización de datos criptográficos de un usuario en el marco del contexto ilustrado en la figura 3 para la firma numérica de un documento electrónico.

Hay que señalar que en estas figuras los elementos estructurales y/o funcionales comunes, así como las etapas comunes a las diferentes variantes o formas pueden presentar las mismas referencias.

La invención busca permitir a un usuario utilizar datos criptográficos que le pertenezcan para proceder a diferentes operaciones que necesiten del uso de estos datos criptográficos sin recurrir a una tarjeta con chip conectada al terminal T. A continuación, se describirá un uso de los datos criptográficos del usuario para la ejecución de una firma digital. Sin embargo, según la invención, los datos criptográficos del usuario podrían utilizarse para cualquier otro proceso tal como del descifrado de datos que hayan sido previamente cifrados mediante una clave pública del usuario o el cifrado y descifrado simétrico mediante una clave simétrica protegida por la invención.

En el contexto ilustrado en la figura 1, el usuario U dispone del acceso o del uso de un terminal T formado, por ejemplo, por un ordenador personal que comprende una interfaz hombre máquina. Según el ejemplo ilustrado, la interfaz hombre máquina se compone de una pantalla E, táctil o no, asociada a un teclado C, así como a un dispositivo señalador S como por ejemplo un ratón. El terminal T está conectado además a una red de comunicación R como, por ejemplo, pero no exclusivamente la red de Internet. El terminal T posee una clave secreta Tsk que le es propia y que por ejemplo está grabada en un módulo de seguridad del terminal T. Este módulo de seguridad puede ser un módulo físico o un módulo informático y por ejemplo un almacén informático de claves como los que proporcionan los sistemas de explotación o los navegadores. La clave secreta del terminal Tsk será de preferencia una clave fuerte de un tamaño superior o igual a 128 bits y de manera más particularmente preferida de un tamaño superior o igual a 256 bits. El usuario U trabaja por ejemplo mediante el terminal T en un documento que desea firmar. Para ello, debe utilizarse, según un proceso bien conocido por el experto en la materia, una clave privada o secreta Usk propia del usuario U. Esta clave secreta Usk pertenece a un par clave secreta Usk/clave pública Upk en el marco de una infraestructura de claves públicas. La clave secreta del usuario Usk es un ejemplo de datos criptográficos del usuario que deben ser conservados de manera protegida en la medida en que una divulgación o un compromiso de la clave secreta Usk pondría en duda la confianza que puede otorgarse a las firmas digitales asociadas al usuario U. Por supuesto, hay muchos otros datos criptográficos que podrían utilizarse en el marco de la invención.

La invención propone garantizar la protección de tales datos criptográficos Usk del usuario U, por un lado, grabándolos en una forma cifrada en una base de datos BD y, por otro lado, garantizando su utilización en un módulo de seguridad SM remoto del terminal T después de la autentificación del usuario U y del terminal T de uso de este último.

El módulo de seguridad SM puede realizarse de cualquier manera apropiada y, por ejemplo, comprender un servidor de seguridad que comprenda módulos de seguridad físicos HSM y que utilice programas informáticos de seguridad y/o módulos de seguridad informática. El módulo de seguridad SM está conectado a la red de comunicaciones R. El módulo de seguridad SM comprende además al menos una clave de cifrado SMk que le es propia y que es el único que la posee. El tamaño de la clave de cifrado SMk es superior o igual a 128 bits y, de preferencia, superior o igual a 256 bits.

La base de datos BD está, según el ejemplo ilustrado, grabada en un servidor de datos SD que está conectado a la red de comunicaciones R. En el caso presentado, el servidor de datos SD es diferente del módulo de seguridad SM, pero la base de datos y/o el servidor de datos podrían estar integrados en el módulo de seguridad.

La base de datos comprende al menos un registro para el usuario U y de preferencia varios registros asociados a

varios usuarios.

Para un usuario dado U el registro correspondiente comprende, por ejemplo, los siguientes datos:

- un elemento de identificación del usuario Uid;

- un elemento ZK(PIN) de autentificación del usuario U;

- un elemento de identificación Tid de al menos un terminal asociado al usuario U;

- un elemento ZK(Tsk) de autentificación del terminal;

- los datos criptográficos Usk del usuario U.

Un mismo usuario U (persona física) puede poseer varios Uid y PIN y así utilizar datos criptográficos Usk diferentes a partir del mismo o de diferentes terminales T en función del contexto de utilización.

El elemento de autentificación ZK(PIN) del usuario se establece a partir de una contraseña PIN conocida solamente por el usuario. Una tal contraseña PIN está generalmente formada por una secuencia de caracteres en un número limitado de preferencia superior o igual a cuatro de manera que permite una memorización fácil por el usuario U. El elemento de autentificación ZK(PIN) es de preferencia diferente de la contraseña PIN y comprende una prueba de conocimiento, de dicha contraseña PIN, susceptible de ser utilizada en el marco de un protocolo de autentificación de divulgación nula. Un tal protocolo, designado en inglés con la denominación «zero-knowledge protocol» permite como su nombre indica verificar el conocimiento mutuo de una información, generalmente un secreto, por dos sistemas diferentes sin comunicación de la información en sí misma.

El elemento de autentificación ZK(Tsk) del terminal se establece a partir de la clave secreta Tsk de la que solo el terminal está en posesión. El elemento de autentificación ZK(Tsk) es de preferencia distinto de la clave secreta Tsk y comprende una prueba de conocimiento de dicha clave secreta susceptible de ser utilizada en el marco de un protocolo de autentificación de divulgación nula.

Teniendo en cuenta su importancia y su carácter crítico, el elemento ZK(PIN) de autentificación del usuario U, el elemento ZK(Tsk) de autentificación del terminal T y los datos criptográficos Usk del usuario U están grabados de preferencia en la base de datos BD de forma cifrada de manera que protegen en confidencialidad el contenido de los ZK(x) y en su integridad la asociación entre los pares «Uid ZK(PIN)» y «Tid ZK(Tsk)» respectivamente.

Según la invención, los datos criptográficos Usk del usuario U serán utilizados por el módulo de seguridad SM que procederá entonces a la autentificación del usuario U y del terminal T. Así los elementos de autentificación del usuario ZK(PIN) y del terminal T ZK(Tsk) están destinados a ser utilizados por el módulo de seguridad SM de forma que su cifrado mediante una clave SMk propia al módulo de seguridad SM contribuye de manera eficaz a su protección en caso de acceso no autorizado, de divulgación o de alteración del contenido de la base de datos BD.

Los datos criptográficos del usuario Usk por su parte están destinados a ser utilizados en el seno del módulo de seguridad SM después de la autentificación del usuario U y del terminal T para su uso o que tiene asociado.

En este contexto, un cifrado mediante la clave SMk propia del módulo de seguridad permite garantizar que los datos criptográficos del usuario Usk solo se utilicen en el módulo de seguridad SM. Un cifrado mediante la clave secreta del terminal Tsk permite garantizar que los datos criptográficos del usuario Usk solo sean utilizables (descifrables) en presencia del terminal T mediante la clave secreta Tsk. Un cifrado mediante la contraseña del usuario PIN permite garantizar que los datos criptográficos del usuario Usk solo sean utilizables (descifrables) en presencia del usuario U. Este último aspecto permite garantizar el no repudio por el usuario de la utilización de los datos criptográficos que tiene asociados en la medida en que estos últimos solo pueden utilizarse en su presencia.

Así, puede realizarse un primer cifrado de los datos criptográficos del usuario Usk mediante una contraseña del usuario PIN, de manera que se obtienen unos primeros datos cifrados ENC(PIN, Usk). Estos primeros datos cifrados ENC(PIN,Usk) pueden ser objeto a continuación de un segundo cifrado mediante la clave secreta del terminal de manera que se obtienen unos segundos datos cifrados ENC(Tsk, ENC(PIN,Usk)). Estos segundos datos cifrados ENC(Tsk,ENC(PIN,Usk)) pueden ser objeto a continuación de un tercer cifrado mediante la clave secreta del módulo de seguridad SMk de manera que se obtienen unos terceros datos cifrados ENC(SMk,ENC(Tsk,ENC(PIN,Usk))) que se registrarán en la base de datos BD. Se observará que la secuencia de los cifrados se realiza en orden creciente de las entropías de la clave y la clave más débil se utiliza en primer lugar.

En la aplicación de la invención, el cifrado mediante la contraseña del usuario PIN y de la clave secreta del terminal Tsk se realiza utilizando una clave de cifrado KDF establecida a partir de la clave secreta del terminal Tsk y de la contraseña del usuario PIN. La clave de cifrado KDF es por ejemplo una clave KDF(Tsk,PIN) que está derivada de la clave secreta del terminal Tsk y de la contraseña del usuario PIN mediante una función de derivación de clave como por ejemplo la función KDF3 definida por la norma ISO-18033-2 o NIST SP800-56A.

Los datos criptográficos del usuario Usk son objeto entonces de un primer cifrado, mediante una primera clave de

cifrado correspondiente a la clave derivada KDF(Tsk,PIN), lo que permite obtener datos cifrados ENC(KDF(Tsk,PIN),Usk). Estos datos cifrados son objeto entonces de un segundo cifrado mediante una segunda clave de cifrado correspondiente a la clave propia del módulo de seguridad SMk, lo que permite obtener los datos cifrados ENC(SMk, ENC(KDF(Tsk,PIN),Usk)) registrados en la base de datos BD. La utilización de la clave derivada KDF(Tsk,PIN) vincula fuertemente la autentificación conjunta del terminal T y del usuario U en la medida en que esta clave derivada solo puede obtenerse en presencia simultánea del terminal T y del usuario U. Los datos cifrados ENC(SMk, ENC(KDF(Tsk,PIN),Usk)) corresponden a la forma cifrada de los datos criptográficos del usuario Usk presente en la base de datos BD.

Los datos presentes en la base de datos habrán estado almacenados allí en el marco de una etapa de inicialización que estará suministrada por el módulo de seguridad que es el único que posee la clave de cifrado SMk utilizada aquí en el marco de un cifrado simétrico. El hecho de que sea el módulo de seguridad SM el que procede al suministro de los datos sensibles evita cualquier corrupción de los datos contenidos en la base de datos BD. Esto garantiza que solo el módulo de seguridad pueda utilizar los datos sensibles presentes en la base de datos BD. Así las medidas de protección de la base de datos no necesitan ser tan pesadas como las utilizadas por el módulo de seguridad.

Durante la etapa de inicialización se eligen la clave secreta del terminal Tsk y la contraseña del usuario PIN y el módulo de seguridad SM procede al registro, en la base de datos de los datos de autentificación asociados en la forma cifrada descrita anteriormente. En el marco de la etapa de inicialización, la clave secreta del terminal Tsk y la contraseña del usuario PIN pueden por ejemplo ser generadas por un proceso automatizado y transmitido al usuario por correo segurizado. La etapa de inicialización también puede hacer intervenir una primera conexión en el módulo de seguridad SM mediante una contraseña de uso único y de fuerte entropía que habrá sido comunicada al usuario por correo segurizado. La clave secreta del terminal Tsk y la contraseña del usuario PIN se eligen entonces o se determinan en el marco de esta primera conexión y el módulo de seguridad las almacena en la base de datos BD como se ha explicado más arriba.

Posteriormente a la etapa de inicialización, cuando el usuario U desea, según el ejemplo ilustrado, proceder a la firma de un documento electrónico mediante una aplicación que funciona en el terminal T.

En primer lugar, se establece un canal de comunicación segurizada CS entre el terminal T y el módulo de seguridad SM. En una etapa 1, el terminal T envía entonces una solicitud de establecimiento del canal de comunicación segurizada enviando el identificador del terminal Tid y el elemento de autentificación ZK(Tsk) del terminal.

En una etapa 2, el módulo de seguridad SM obtiene en la base de datos BD a través, de preferencia, una comunicación segurizada con autentificación mutua el elemento de autentificación ZK(Tsk) tal como está registrado en una forma cifrada ENC(SMk, ZK(Tsk)) mediante la clave secreta SMk del módulo de seguridad SM en la base de datos BD. El identificador del terminal Tid se utiliza entonces como un índice para interrogar a la base de datos BD.

En una etapa 3, se establece un canal segurizado CS con la clave de sesión única mediante un protocolo de divulgación nula que utiliza el elemento de autentificación ZK(Tsk) que habrá sido descrifrado por el módulo de seguridad SM mediante su clave secreta SMk. Este canal segurizado solo se establece en caso de autentificación positiva del terminal T.

El protocolo de divulgación nula utilizado en la etapa 3 es un protocolo cuyo principio de funcionamiento está descrito en concreto por Louis Guillou y Jean-Jacques Quisquater en el artículo «How to Explain Zero-Knowledge Protocols to Your Children CRYPTO '89 -Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology publicado en 1990 por Springer-Verlag London.

El protocolo de divulgación nula utilizado en la etapa 3 permite, por un lado, al módulo de seguridad SM autentificar el terminal T verificando que el terminal T posee efectivamente la clave secreta Tsk sin que esta clave secreta Tsk transite por la red en el marco de esta fase de autentificación. El protocolo de divulgación nula utilizado en la etapa 3 permite, por un lado, al terminal T autentificar el módulo de seguridad SM verificando que el módulo de seguridad SM posee efectivamente prueba de conocimiento de la clave secreta ZK(Tsk) sin que esta prueba de conocimiento de la clave secreta ZK(Tsk) transite por la red en el marco de esta fase de autentificación.

La autentificación del módulo de seguridad SM mediante ZK(Tsk) permite obstaculizar los ataques denominados del «hombre del medio» y evita así una divulgación de los datos de autentificación a un tercero no autorizado. La autentificación del módulo de seguridad SM podría hacerse mediante certificados de tipo X509. Sin embargo, esta manera de proceder impone pesados procesos de actualización de los certificados que se evitan para la aplicación del protocolo de divulgación nula de la etapa 3.

Además, el hecho de proceder, según el ejemplo ilustrado, en primer lugar, a la autentificación del terminal T permite utilizar un dato de autentificación Tsk o ZK(Tsk) que posea una fuerte entropía muy superior a la del dato de autentificación del usuario, es decir, su contraseña PIN. La utilización del módulo de seguridad SM permite una protección contra los ataques por fuerza bruta limitando el número de intentos posible. Además, la utilización en primer lugar de un dato de autentificación distinto de la contraseña del usuario y que presenta una fuerte entropía permite una protección contra los ataques distribuida que consiste en probar las contraseñas más utilizadas por un gran número de usuarios y acaba por encontrar estadísticamente la contraseña correcta de un usuario antes de que

el mecanismo de limitación del número de intentos por usuario entre en acción.

Después de la autentificación mutua del terminal T y del módulo de seguridad SM y el establecimiento del canal de comunicación segurizada, se procede a una autentificación del usuario U. En una etapa 4, el terminal T solicita al usuario que introduzca su contraseña PIN mediante por ejemplo el teclado C o, de preferencia, una interfaz gráfica de introducción que limite los riesgos de fuga de la contraseña. En una etapa 5, el usuario U introduce su contraseña PIN y en una etapa 6 el terminal establece un elemento de autentificación ZK(PIN) a partir de esta contraseña y en el caso presente una prueba de conocimiento del motor utilizable en el marco de un protocolo de divulgación nula.

En una etapa 7, el terminal T dirige al módulo de seguridad SM, a través del canal de comunicación segurizada establecido en la etapa 3, el identificador del usuario Uid y el elemento de autentificación ZK(PIN) de este último. A continuación, en una etapa 8 el módulo de seguridad SM obtiene en la base de datos BD, siempre en el marco de una comunicación segurizada con autentificación alta, el elemento de autentificación del usuario ZK(PIN) en una forma cifrada ENC(SMk, ZK(Tsk)) mediante la clave secreta del módulo de seguridad SM.

En una etapa 9, el módulo de seguridad SM utiliza el elemento de autentificación ZK(PIN) que habrá descifrado para proceder a la autentificación del usuario U igualmente en el marco de un protocolo de divulgación nula.

Debe señalarse que de manera preferida la autentificación del terminal T ocurre antes de la autentificación del usuario U. Sin embargo, en la medida en que el terminal T está asociado al usuario U, en caso de robo o de descubrimiento de Tsk, el atacante solo puede probar la contraseña PIN específica del usuario U. Sin embargo, el módulo de seguridad SM obstaculiza un ataque por fuerza bruta mientras que el hecho de que solo haya un usuario U o un número muy bajo de usuarios asociados a un mismo terminal T impide un ataque según el método distribuido.

En este punto, se ha establecido un canal de comunicación segurizada CS entre el terminal T el módulo de seguridad SM mientras que el usuario U y el terminal T han sido autentificados por el módulo de seguridad SM y que el módulo de seguridad SM ha sido autentificado por el terminal T. Por supuesto, el canal de seguridad solo se establece en caso de autentificaciones mutuas positivas.

En una etapa 10, el terminal T deriva, de su clave secreta Tsk y de la contraseña PIN la clave de cifrado KDF(Tsk,PIN) para a continuación en una etapa 11 enviarla, a través del canal de comunicación segurizada CS, al módulo de seguridad SM. Después de este envío, el terminal T borra de sus memorias la contraseña PIN y la clave de cifrado derivada KDF(Tsk,PIN). Hay que señalar que el borrado de la contraseña PIN puede ocurrir justo después del establecimiento de la clave de cifrado KDF(Tsk,PIN).

En una etapa 12, el módulo de seguridad SM obtiene, en la base de datos BD, los datos criptográficos del usuario Usk en su forma cifrada ENC(SMk, ENC(KDF (Tsk,PIN), Usk)).

En una etapa 13, el módulo de seguridad SM descifra en primer lugar mediante su clave secreta SMk y después mediante la clave derivada KDF(Tsk,PIN) los datos criptográficos del usuario Usk. En este punto, el módulo de seguridad SM ya no necesita la clave derivada KDF(Tsk,PIN) y puede borrarla mientras que los datos criptográficos del usuario Usk están listos para ser utilizados y se encuentran por tanto en un estado activado.

En una etapa 14, el módulo de seguridad SM dirige al terminal T una información según la cual la utilización de los datos criptográficos del usuario es posible.

En el marco de una firma electrónica, el terminal T dirige, en una etapa, al módulo de seguridad SM, a través del canal de comunicación segurizada CS, una o varias huellas digitales SH(DOC) del documento electrónico que hay que firmar. En una etapa 16 el módulo de seguridad SM calcula un valor de firma correspondiente al cifrado ENC(Usk,SH(DOC)) de la huella digital SH(DOC) mediante datos criptográficos Usk del usuario U y devuelve este valor al terminal T, a través del canal de comunicación segurizada CS. El terminal T puede terminar entonces el proceso de firma a partir del valor recibido del módulo de seguridad SM.

Cuando finaliza la etapa 16, el módulo de seguridad SM puede borrar los datos criptográficos del usuario Usk y se cierra el canal de comunicación segurizada.

Se revela que el procedimiento según la invención permite utilizar los datos criptográficos de un usuario a partir de un terminal para uso de este último sin que estos datos criptográficos se presenten nunca en el terminal y se sometan a riesgos de divulgación o de corrupción. Además, la autentificación del usuario asociada a las del terminal permite obtener una autentificación más fuerte que la que se obtendría mediante la autentificación del usuario solamente. Además, la utilización de un módulo de seguridad SM remoto, así como una base de datos BD remota permite implantar mecanismos de vigilancia de los accesos e intentos de acceso a los sistemas que integran el módulo de seguridad y la base de datos. Estos mecanismos de vigilancia permiten en concreto obstaculizar los ataques por fuerza bruta y utilizar mecanismos de detección del fraude por análisis ambiental (origen de las solicitudes, fecha y hora...) o comportamental (estadística de uso).

Según el ejemplo descrito anteriormente en relación con las figuras 1 y 2, los datos que hay que tratar se envían al

módulo de seguridad SM por el terminal T para uso del usuario T. Sin embargo, según la invención, los datos que hay que tratar pueden dirigirse al módulo de seguridad SM mediante otro dispositivo informático. Así, las figuras 3 y 4 ilustran otra forma de aplicación de la invención según la cual los datos que hay que tratar se envían al módulo de seguridad SM mediante un puesto de trabajo P diferente del terminal T.

Según el ejemplo ilustrado el puesto de trabajo P está formado, por ejemplo, por un ordenador personal que comprende una interfaz hombre máquina. Según el ejemplo ilustrado, la interfaz hombre máquina se compone de una pantalla E, táctil o no, asociada a un teclado C, así como a un dispositivo señalador S como por ejemplo un ratón. El puesto de trabajo P está además conectado a la red de comunicación R.

El terminal T está formado por su parte por un dispositivo móvil como un teléfono móvil conectado asimismo a la red de comunicaciones R.

El usuario U desea, por ejemplo, firmar numéricamente un documento establecido en el puesto de trabajo P. El procedimiento según la invención utiliza entonces las etapas como las que se ilustran en la figura 4.

En primer lugar, se procede a la activación de los datos criptográficos del usuario Usk dentro del módulo de seguridad SM mediante la realización de las etapas 1 a 13 tal como se han descrito anteriormente.

Una vez los datos criptográficos Usk listos para ser utilizados en el módulo de seguridad SM, este último envía, en una etapa 20, una contraseña de uso único OTP al terminal T para su visualización. En una etapa 21, el usuario introduce la contraseña de uso único OTP en el puesto de trabajo P. En una etapa 22, el puesto de trabajo P utiliza esa contraseña de uso único OTP para establecer un canal de comunicación segurizada CS' con el módulo de seguridad SM en el marco de un protocolo con autentificación fuerte del usuario. En una variante se puede considerar un protocolo de autentificación mutua de divulgación nula, cunado los datos que hay que transmitir hacia el SM son sensibles. En un tal caso, el puesto P autentifica el SM antes de transmitir los datos y el SM autentifica el puesto P antes de utilizar la clave Usk.

El canal de comunicación segurizada CS' se utiliza entonces, por un lado, por el puesto de trabajo P para enviar los datos que hay que tratar al módulo de seguridad SM como se describe para la etapa 15 y, por otro lado, por el módulo de seguridad SM para enviar el resultado del tratamiento al puesto de trabajo P como se describe para la etapa 16.

Hay que observar que el establecimiento del canal de comunicación segurizada CS' entre el puesto de trabajo P y el módulo de seguridad SM podría intervenir asimismo antes de la activación de los datos criptográficos del usuario en el módulo de seguridad SM.

En los ejemplos descritos anteriormente la autentificación del terminal T y del usuario U se realizan sucesivamente. Sin embargo, según la invención es posible realizar estas dos autentificaciones de forma conjunta. Para ello puede utilizarse una prueba de conocimiento ZK(KDF(Tsk,PIN)) de la clave KDF(Tsk,PIN) en el marco de un protocolo de divulgación nula en el momento del establecimiento de la comunicación entre el terminal T y el módulo de seguridad. En este caso la contraseña PIN se introduce en el terminal T y a continuación la clave derivada KDF(Tsk,PIN) se genera antes de la autentificación y establecimiento de la comunicación entre el terminal T y el módulo de seguridad SM. En este caso la prueba de conocimiento ZK(KDF(Tsk,PIN)) se registra en la base de datos BD.

Según el ejemplo de aplicación de la invención descrito anteriormente la forma cifrada de los datos criptográficos del usuario Usk presente en la base de datos BD corresponde a ENC(SMk, ENC(KDF(Tsk,PIN),Usk)). Sin embargo, según la invención, los datos criptográficos del usuario Usk también pueden ser objeto de un primer cifrado mediante una primera clave de cifrado correspondiente a la clave propia del módulo de seguridad SMk, lo que permite obtener datos cifrados ENC(SMk, Usk). Estos datos cifrados son objeto a continuación de un segundo cifrado mediante una segunda clave de cifrado correspondiente a la clave derivada KDF(Tsk,PIN) lo que permite obtener los datos cifrados ENC(KDF(Tsk,PIN), ENC(SMk,Usk)) que se registran entonces en la base de datos BD. Esta manera de proceder permite asociar un nuevo terminal T' al usuario U sin que sea necesario conocer o descifrar la clave secreta del usuario Usk. Efectivamente, en una etapa de inscripción de un nuevo terminal T' asociado a una clave secreta T'sk, el usuario U puede autentificarse mediante su terminal T ya registrado, así como el terminal T ante el módulo de seguridad SM como se ha descrito anteriormente en las etapas 1 a 12. Mediante KDF(Tsk,PIN) el módulo de seguridad SM procede al descifrado de ENC(KDF(Tsk,PIN), ENC(SMk,Usk)) para obtener ENC(SMk,Usk) que puede volver a cifrar entonces mediante KDF(T'sk,PIN) que habrá obtenido mediante un canal segurizado establecido después de una autentificación mutua del nuevo terminal T' y del módulo de seguridad SM efectuada mediante por ejemplo una contraseña de uso único mostrada en el primer terminal T o por un código de activación enviado al usuario por un medio alternativo (de manera no exhaustiva, por correo, teléfono, SMS, email). Una vez esta inscripción realizada, el nuevo terminal T' puede utilizarse de la misma manera que el terminal T.

En las formas de aplicación descritas anteriormente, se utiliza como elemento de autentificación del usuario su contraseña PIN. Sin embargo, también podría utilizarse como elemento de autentificación del usuario un dato biométrico como una huella digital leída mediante un lector de huella digital que equipa el terminal T. En el marco de esta forma de aplicación, la base de datos BD comprende, por un lado, un primer elemento de autentificación del usuario que comprende los datos biométricos relativos a la huella del usuario y, por otro lado, un segundo elemento

de autentificación del usuario que comprende la contraseña PIN del usuario.

Esta forma de aplicación del procedimiento según la invención hace intervenir en primer lugar las etapas 1 a 3 de autentificación del terminal T y del módulo de seguridad SM, así como de establecimiento del canal de comunicación segurizada CS. A continuación, interviene una autentificación del usuario U. Para ello, el usuario U hace que el lector de huella digital del terminal T lea su huella digital. El resultado de la lectura se envía al módulo de seguridad SM mediante el canal segurizado CS. El módulo de seguridad SM realiza una comparación entre el resultado de la lectura y el primer elemento de autentificación del usuario que habrá obtenido de la base de datos BD. En caso de comparación positiva el proceso continúa mediante una solicitud de introducción de la contraseña del usuario U en el terminal T hasta la utilización de los datos criptográficos del usuario como se ha descrito anteriormente para las etapas 4 a 16.

De manera preferida, el terminal utiliza un módulo de cliente que se encarga de la gestión de las diferentes etapas del procedimiento según la invención y, en concreto, de los diferentes cálculos, solicitudes de introducción, comunicaciones con el módulo de seguridad de las fases de inicialización y de aplicación de la invención.

Por supuesto, se pueden aportar diversas modificaciones a la invención en el marco de las reivindicaciones anexas.

REIVINDICACIONES

1. Procedimiento de utilización, mediante un módulo de seguridad (SM), de los datos criptográficos (Usk) de un usuario (U), almacenados en una base de datos (BD), mediante un terminal (T) para uso del usuario y que comunica con el módulo de seguridad (SM) a través de una red de comunicación (R), procedimiento que comprende las etapas siguientes:

- una secuencia de autentificación que comprende las siguientes etapas sucesivas:

  - autentificación mutua entre el módulo de seguridad (SM) y el terminal (T), que se basa en un protocolo de criptografía asimétrica, que establece un canal de seguridad entre el módulo de seguridad (SM) y el terminal (T);

  - en caso de autentificación mutua positiva del módulo de seguridad y del terminal, autentificación mutua del módulo de seguridad y del usuario;

- en caso de autentificación mutua positiva entre, por un lado, el módulo de seguridad y el terminal y, por otro lado, el módulo de seguridad y el usuario:

  - obtención de los datos criptográficos del usuario (Usk) mediante el módulo de seguridad (SM) en la base de datos (BD), los datos criptográficos están almacenados en la base de datos (BD) en una forma cifrada mediante al menos una primera clave de cifrado (KDF(Tsk,PIN)) establecida a partir de al menos una clave secreta del terminal (Tsk) y del elemento de autentificación del usuario (PIN) y de una segunda clave de cifrado (SMk) propia del módulo de seguridad (SM), el cifrado mediante la segunda clave de cifrado que interviene después del cifrado mediante la primera clave de cifrado;

  - cálculo por el terminal de la primera clave de cifrado (KDF(Tsk,PIN));

  - envío a través del canal segurizado mediante el terminal al módulo de seguridad, de la primera clave de cifrado;

  - utilización de los datos criptográficos del usuario (Usk) mediante el módulo de seguridad (SM) después del descifrado, mediante el módulo de seguridad (SM) de los datos criptográficos del usuario (Usk) al menos mediante, en primer lugar, la segunda clave de cifrado (SMk) y después de la primera clave de cifrado (KDF(Tsk,PIN)).

2. Procedimiento según la reivindicación 1, caracterizado por que las etapas de control de autenticidad se realizan mediante:

- al menos un elemento de autentificación del terminal (ZK(Tsk));

- y al menos un elemento de autentificación del usuario (ZK(PIN));

obtenidos mediante el módulo de seguridad (SM) en la base de datos (BD), los elementos de autentificación están almacenados en la base de datos (BD) en una forma cifrada mediante una clave de cifrado (SMk) propia del módulo de seguridad (SM).

3. Procedimiento según la reivindicación 2, caracterizado por que se utiliza un elemento ZK(Tsk) de autentificación del terminal establecido en parte al menos a partir de una clave secreta del terminal (Tsk) almacenada en el terminal (T).

4. Procedimiento según la reivindicación 3, caracterizado por que el elemento de autentificación del terminal comprende una prueba ZK(Tsk) de posesión de la clave secreta (Tsk) del terminal (T) destinada a ser utilizada en el marco de un protocolo de autentificación de divulgación nula.

5. Procedimiento según cualquiera de las reivindicaciones 2 a 4, caracterizado por que se utiliza un elemento ZK(PIN) de autentificación del usuario (U) establecido en parte al menos a partir de una contraseña PIN introducida por el usuario (U).

6. Procedimiento según la reivindicación 6, caracterizado por que el elemento de autentificación del usuario (U) comprende una prueba ZK(PIN) de conocimiento de la contraseña PIN destinada a ser utilizada en el marco de un protocolo de autentificación de divulgación nula.

7. Procedimiento según cualquiera de las reivindicaciones precedentes caracterizado por que el módulo de seguridad (SM) utiliza los datos criptográficos del usuario (Usk) para efectuar tratamientos criptográficos en datos que hay que tratar recibidos a través de la red de comunicación (R) y segurizados por el canal segurizado establecido durante la autentificación mutua entre el módulo de seguridad y el terminal.

8. Procedimiento según la reivindicación 7, caracterizado por que los datos que hay que tratar comprenden datos utilizados en el marco de un proceso de firma digital de un documento electrónico.

9. Procedimiento según cualquiera de las reivindicaciones precedentes, caracterizado por que el terminal

utiliza un módulo del cliente que gestiona al menos las comunicaciones con el módulo de seguridad, la introducción del elemento de autentificación del usuario, la secuencia de autentificación y el cálculo de la primera clave de cifrado.

10. Procedimiento según la reivindicación 9, caracterizado por que el módulo del cliente está adaptado para:

- conservar el valor del elemento de autentificación del cliente desde el momento de su introducción por el usuario y hasta el cálculo de la primera clave de cifrado;

- borrar el valor del elemento de autentificación después del cálculo de la primera clave de cifrado;

- borrar el valor de la primera clave de cifrado después de su envío al módulo de seguridad.

11. Procedimiento según la reivindicación 9 o 10, caracterizado por que el módulo del cliente está adaptado para impedir el acceso al valor del elemento de autentificación del cliente y al valor de la primera clave de cifrado por otro recurso u otro programa, del terminal o externos al terminal, diferente al módulo de seguridad.

12. Procedimiento según la reivindicación 7 u 8 y una de las reivindicaciones 9 a 11, caracterizado por que el módulo del cliente garantiza la transmisión de los datos que hay que tratar al módulo de seguridad.

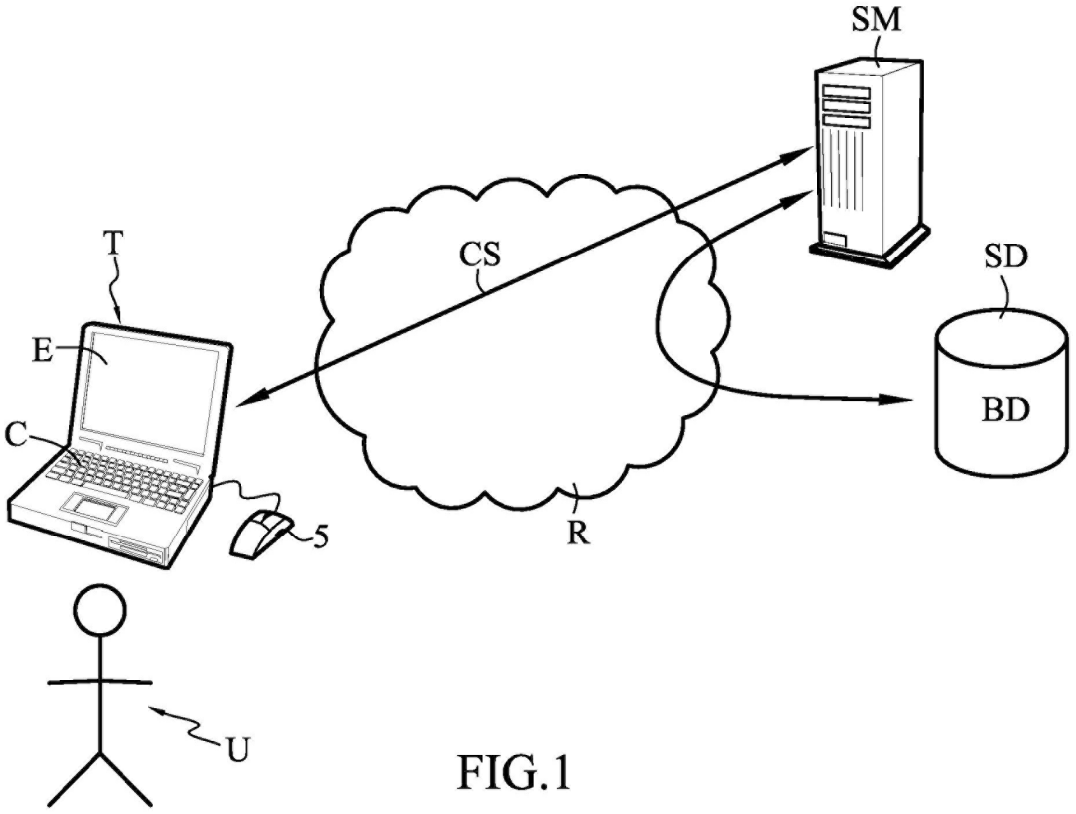

FIG.1

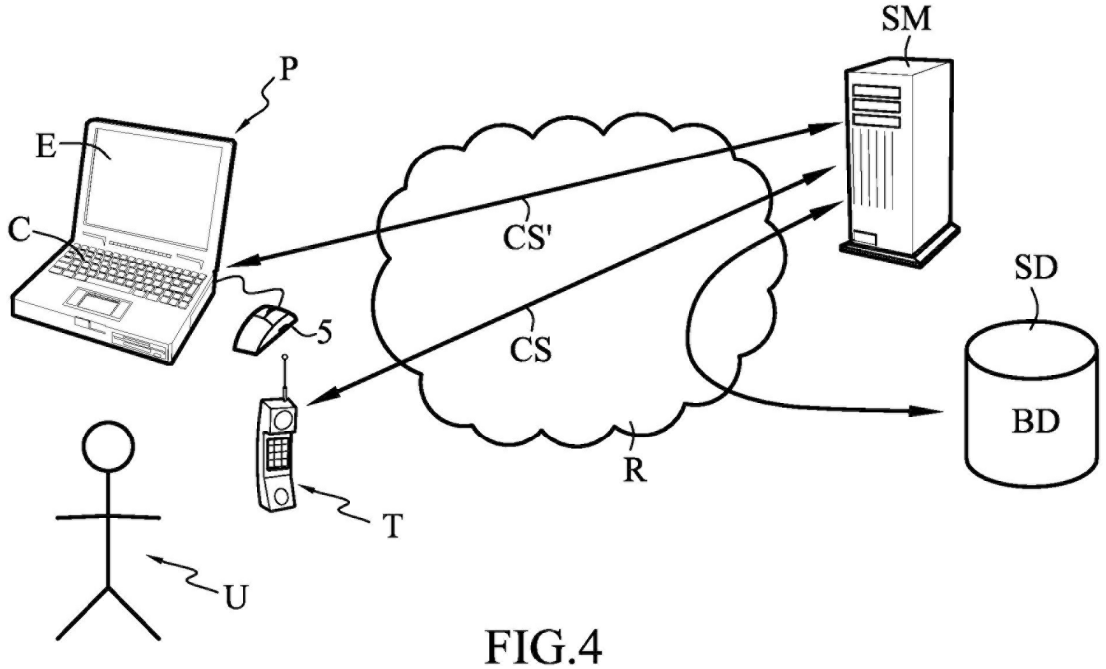

FIG.4

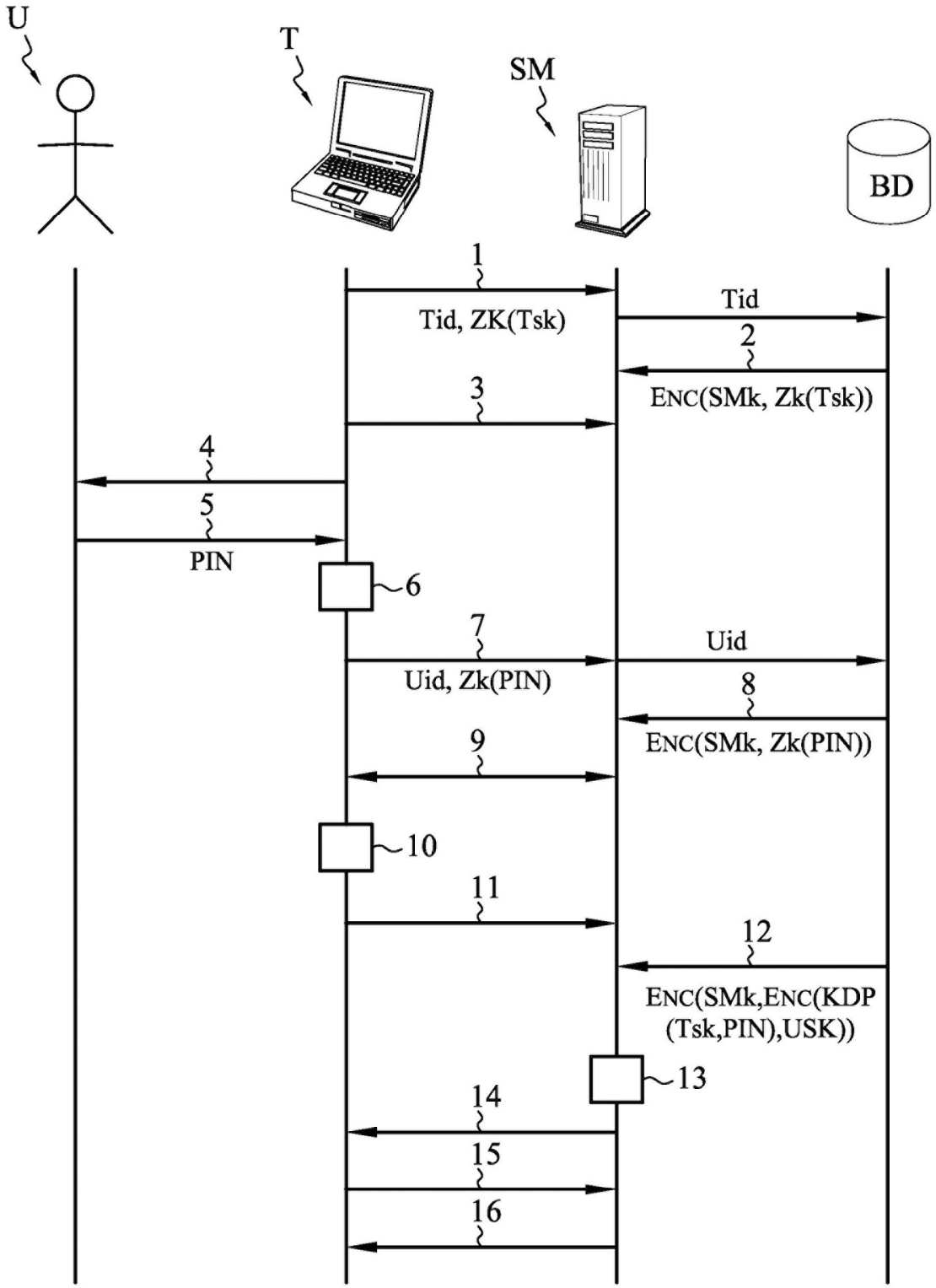
U
T
SM
BD
1
Tid, ZK(Tsk)
Tid
2
ENC(SMk, Zk(Tsk))
3
4
5
PIN
6
7
Uid, Zk(PIN)
Uid
8
ENC(SMk, Zk(PIN))
9
10
11
12
ENC(SMk,ENC(KDP
(Tsk,PIN),USK))
13
14
15
16

FIG.2

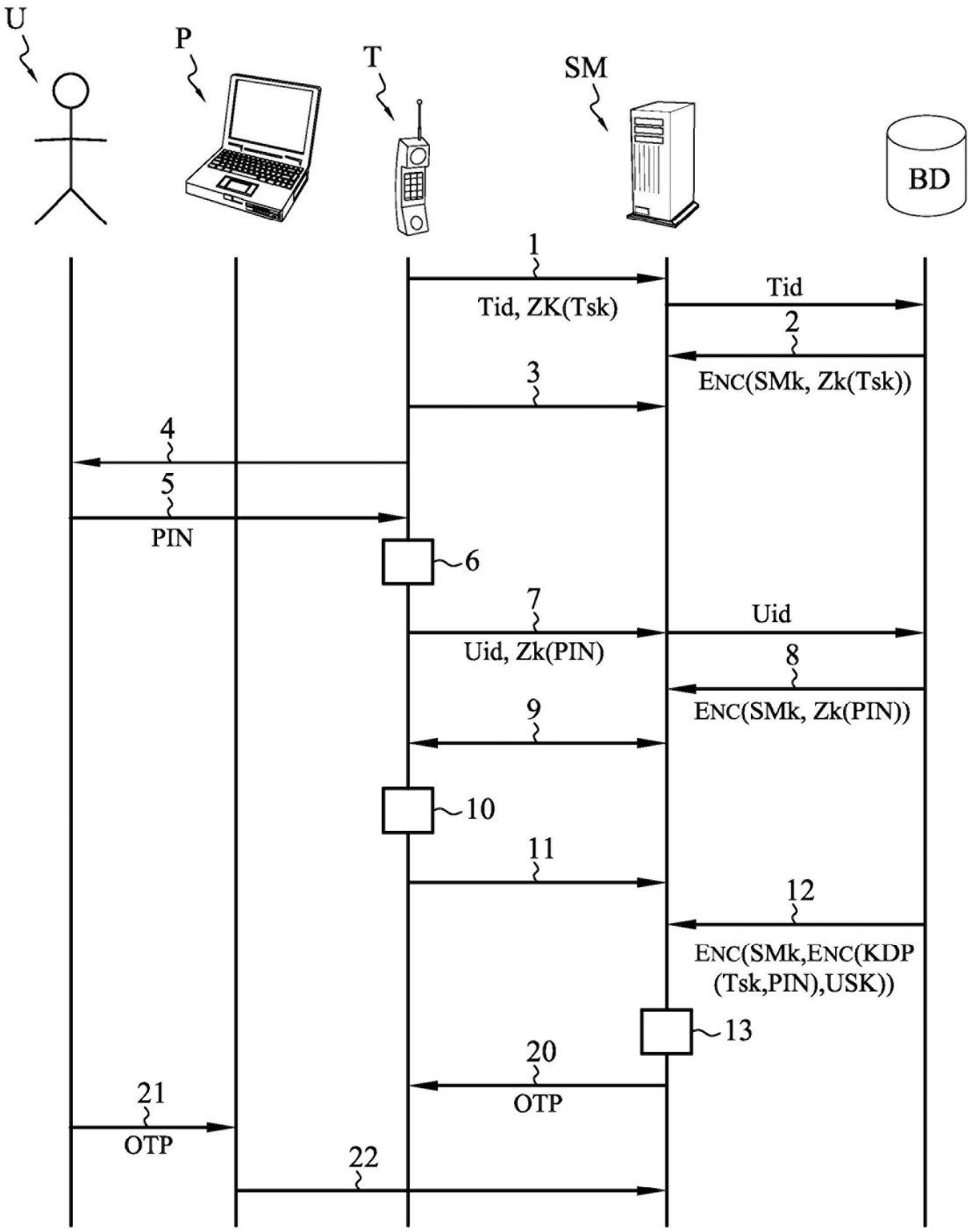
U
P
T
SM
BD
1
Tid, ZK(Tsk)
Tid
2
ENC(SMk, Zk(Tsk))
3
4
5
PIN
6
7
Uid, Zk(PIN)
Uid
8
ENC(SMk, Zk(PIN))
9
10
11
12
ENC(SMk,ENC(KDP
(Tsk,PIN),USK))
13
20
OTP
21
OTP
22

FIG.3