(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 723 224**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.11.2013 PCT/EP2013/074998**

(87) Fecha y número de publicación internacional: **19.06.2014 WO14090590**

(96) Fecha de presentación y número de la solicitud europea: **28.11.2013 E 13799010 (7)**

(97) Fecha y número de publicación de la concesión europea: **28.11.2018 EP 2929649**

(54) Título: **Método de protección de un depósito de claves asistido por servidor**

(30) Prioridad:

10.12.2012 EP 12306551

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.08.2019

(73) Titular/es:

THALES DIS FRANCE SA (100.0%)
6, rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es:

WEBSTER, MICHAEL;
POHJA, SEPPO y
PALO, TIMO

(74) Agente/Representante:

CASANOVAS CASSÁ, Buenaventura

DESCRIPCION

Método de protección de un depósito de claves asistido por servidor

CAMPO DE LA INVENCIÓN

La presente invención se refiere a un método para acceder a un almacén de datos almacenado de forma segura en un dispositivo mientras está asistido por un servidor con el que el dispositivo puede comunicarse según sea necesario. Típicamente, la invención se aplica en el campo del almacenamiento y recuperación de claves en un entorno no seguro.

ANTECEDENTES DE LA INVENCIÓN

Casi todo el software criptográfico se basa, entre otras cosas, en el almacenamiento de secretos. Dicho software a menudo asume que el almacenamiento es permanente y preserva la confidencialidad del secreto. Esto se logra comúnmente mediante el uso de hardware seguro, como una tarjeta inteligente como medio de almacenamiento. El acceso a los secretos depende de dos factores: tener acceso al hardware seguro, el denominado factor "lo que tienes", y conocer el código correcto, como un PIN que desbloquea el acceso (el factor "lo que sabes"). El código suele ser de unos pocos dígitos o caracteres de longitud.

El software criptográfico que se ejecuta en ordenadores personales, tabletas, teléfonos inteligentes o dispositivos no seguros similares, tiene que funcionar a menudo sin ningún hardware seguro: el almacenamiento permanente es accesible pero las medidas disponibles para preservar la integridad y la confidencialidad del secreto son limitadas.

La presente invención se centra en el software que se ejecuta en tales dispositivos no seguros. Un enfoque comúnmente utilizado para implementar la criptografía de dos factores en un dispositivo de este tipo es almacenar los secretos en un archivo llamado depósito de claves, que se cifra mediante una frase de contraseña larga. Sin embargo, las frases de contraseña largas son difíciles de utilizar; cuanto más complicadas, más limitadas las posibilidades del teclado del dispositivo, especialmente sin un teclado "qwerty".

El uso de un PIN u otra frase de contraseña corta hará que el software sea más fácil de usar, pero podría ser factible un ataque por la fuerza en el archivo cifrado. Normalmente, los ataques de diccionario pueden permitir que un atacante acceda al contenido del almacén de datos confidenciales.

Otra diferencia entre los dispositivos no seguros y los dispositivos seguros como las tarjetas inteligentes es que copiar una tarjeta inteligente junto con los secretos almacenados se considera extremadamente dificultoso, mientras que copiar un depósito de claves desde un dispositivo no seguro generalmente se considera bastante factible.

Así, en general, los dispositivos no seguros no pueden proporcionar criptografía de doble cifrado de manera confiable porque el núcleo del factor "lo que tienes", el depósito de claves, puede ser clonado en otros dispositivos. Después de la clonación, el depósito de claves ya no se considera como "lo que tienes" sino como "lo que cualquiera podría tener". Además, puede llevar mucho tiempo detectar que se ha producido la clonación o puede pasar totalmente desapercibida.

La confianza en un servidor para acceder a datos confidenciales se conoce a partir del documento US 7,149,311. En este documento se describen varias soluciones basadas en servidores, algunas de las cuales se basan en el uso de un servidor confiable para almacenar claves. En este caso, los datos confidenciales se envían a un dispositivo a petición del dispositivo.

Esto presenta el inconveniente de permitir la recepción de la propia clave privada una vez que se conoce la contraseña. Si se adivina o se ataca la contraseña, un atacante obtendrá la clave del servidor y podrá usarla por tiempo ilimitado.

Este documento también describe un protocolo basado en un servidor donde una parte de los cálculos criptográficos son realizados por el servidor. En la medida en que este servidor es seguro, aumenta la seguridad por lo que respecta a la manipulación de datos confidenciales. Sin embargo, esta solución no es directamente relevante en cuanto al ataque de diccionario sin conexión y presenta puntos débiles similares a los de la solución anterior.

Más específicamente, la invención descrita en el documento US 7,149,311 propone dividir la clave en porciones y utilizar el servidor para la recuperación de una de las porciones. Para este fin, la petición del dispositivo al servidor comprende información criptográfica incluida en los datos almacenados en el depósito de claves y generados previamente a partir de la clave, es decir, una porción de la clave. Los datos protegidos en el depósito de claves de esta técnica anterior no son ningún tipo de datos sino porciones compartidas de claves. Este depósito de claves no pretende incluir ningún tipo de datos confidenciales completos que deban protegerse. El servidor presta una asistencia parcial para extraer el recurso compartido que luego se usa en el dispositivo para recuperar la clave completa. Esta solución implica cálculos dentro del servidor y dentro del dispositivo, de manera preliminar a la

implementación y durante a ejecución del método.

SUMARIO DE LA INVENCIÓN

La presente invención apunta a tales propósitos y se define, en su sentido más amplio, como un método para acceder a un depósito de datos previamente bloqueado utilizando una frase de contraseña de un dispositivo, dicho método incluye los pasos preliminares de:

- para el dispositivo, solicitar al usuario que introduzca un código personal en el dispositivo;
- para el dispositivo, calcular una primera función de al menos el código personal;
- para el dispositivo, enviar, para el almacenamiento, dicha primera función a un servidor que conoce la frase de contraseña;

dicho método comprende además los siguientes pasos, cuando el usuario solicita acceso al depósito de datos:

- para el dispositivo, solicitar al usuario que introduzca el código personal,
- para el dispositivo, generar un código de acceso aplicando dicha primera función a al menos el código personal introducido;
- para el dispositivo, enviar, al servidor, al menos un identificador del dispositivo y el código de acceso;
- para el servidor, comparar el código de acceso con la primera función preliminar recibida;
- para el servidor, si el código de acceso es correcto, devolver la frase de contraseña al dispositivo;
- para el dispositivo, desbloquear el almacén de datos usando la frase de contraseña recibida en combinación con el código personal introducido.

La invención se basa en el servidor con el que el dispositivo puede comunicarse según sea necesario. La comunicación puede producirse, por ejemplo, a través de Internet. La invención resuelve el problema de cómo las frases de contraseña cortas, el código personal, se pueden usar en dispositivos no seguros al tiempo que se mantiene la confidencialidad de los secretos en el depósito de claves. El usuario necesita tener el depósito de claves y conocer el código personal. El/ella lo necesita para solicitar la frase de contraseña y desbloquear el depósito de claves en combinación con la frase de contraseña recibida.

Según una característica ventajosa:

- antes del cálculo preliminar de la primera función, un paso de cálculo y almacenado de una suma de comprobación del código personal;
- cada vez que el usuario introduce el código personal, un paso de cálculo de la suma de comprobación del código personal introducido;
- un paso para de comparación de la suma de comprobación calculada con la suma de comprobación previamente almacenada,
- si existe una discrepancia, un paso de exhibición de un mensaje de error, y
- si la suma de comprobación es correcta, procesado de los siguientes pasos del método.

Esta función asegura que el PIN introducido nunca se almacena en el dispositivo no seguro, sino que solo se verifica mediante la suma de comprobación.

Según una realización ventajosa de la invención, habría pasos preliminares de generación de un número aleatorio fijo y almacenamiento en el dispositivo, siendo la primera función una función del código personal y del número aleatorio fijo.

El uso del número aleatorio fijo, no conocido por ningún otro dispositivo, proporciona protección contra el uso de "tablas arcoiris" para deducir el código personal del usuario del código de acceso enviado al servidor.

Ventajosamente, la primera función es una función de la suma del código personal y el número aleatorio fijo.

Dicha implementación es particularmente simple ya que un único valor, es decir la suma, se proporciona a la función.

En una realización, el almacén de datos se cifra y almacena previamente en el dispositivo.

En esta realización, el depósito de claves se almacena en el propio dispositivo no seguro. La invención es particularmente ventajosa ya que proporciona seguridad en un entorno no seguro.

En otra realización, el almacén de datos se almacena previamente en una tarjeta inteligente, o elemento seguro similar, que tiene acceso bloqueado y está vinculado al dispositivo.

Con tal realización, es necesario que el dispositivo pueda incorporar una tarjeta inteligente. La seguridad se gestiona

así físicamente.

De acuerdo con una característica ventajosa, el método comprende, cada vez que el usuario solicita acceso al almacén de datos, un paso para determinar un número aleatorio utilizado una sola vez que se envía al servidor con el código de acceso.

El uso de un número aleatorio utilizado una sola vez comprobado por el servidor proporciona algunas capacidades para la detección de la clonación del depósito de claves. También evita la repetición de solicitudes del dispositivo, ya que el contenido de la solicitud es necesariamente diferente de una solicitud a otra. Esta función permite asegurar que el dispositivo sea el adecuado para la frase de contraseña y que la recibirá. Es útil para detectar la clonación del depósito de claves.

En una primera realización de esta característica, el número aleatorio utilizado una sola vez es generado por el servidor y recuperado del servidor por el dispositivo cada vez que el usuario solicita acceso al almacén de datos, verificando el servidor el número aleatorio y luego lo recibe del dispositivo.

En una segunda realización de esta característica, el número aleatorio utilizado una sola vez se calcula en el dispositivo y se vincula al número aleatorio utilizado una sola vez enviado previamente para que el servidor verifique la secuencia del número aleatorio utilizado una sola vez.

De acuerdo con una realización preferida, el método comprende un paso adicional de, después del cálculo del código de acceso, calcular una segunda función del código de acceso y del número aleatorio, un paso de enviarlo al servidor con el número aleatorio y un paso, para que el servidor verifique la información enviada realizando el mismo cálculo que el dispositivo, utilizando el código de acceso y el número aleatorio.

En una realización, la introducción del código personal se realiza mediante incorporación segura. Esto evita una fácil obtención del PIN por parte de una aplicación maliciosa que podría instalarse en el dispositivo.

En una realización particular, estando protegidas las comunicaciones entre el dispositivo y el servidor, el dispositivo cifra los mensajes utilizando una clave pública del servidor.

Esto también evita la recuperación de datos mientras se rastrean las comunicaciones.

En este caso, preferiblemente, el servidor comprende un entorno seguro donde se produce el descifrado de los mensajes. Esto asegura que los datos permanezcan en secreto de un lado a otro.

Según una característica específica, estando protegidas las comunicaciones entre el dispositivo y el servidor, el dispositivo envía una clave de cifrado utilizada una sola vez al servidor que la usa para cifrar el envío del mensaje.

Esta característica permite asegurar la comunicación a través de una sola tecla de uso.

En una realización ventajosa, la primera función es una función de hash. Dichas funciones están adaptadas a los propósitos de la invención.

La presente invención también se refiere a un dispositivo capaz de implementar el método de la invención, teniendo dicho dispositivo al menos un almacén de datos previamente bloqueado mediante el uso de una frase de contraseña, un módulo de adquisición de código personal, un módulo de cálculo capaz de generar un código de acceso aplicando una primera función a al menos el código personal introducido, un transmisor para enviar al menos un identificador del dispositivo y el código de acceso a un servidor que conoce la frase de contraseña para el almacenamiento, un receptor para recibir una frase de contraseña del servidor, un módulo de desbloqueo para desbloquear el almacén de datos utilizando la frase de contraseña recibida en combinación con el código personal ingresado por el usuario.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Otras ventajas y características novedosas se harán evidentes a partir de la siguiente descripción detallada cuando se consideren en conjunto con los dibujos y se pretende que las realizaciones descritas incluyan todos estos aspectos y sus equivalentes.

La figura 1 representa el entorno en el que se implementa ventajosamente la invención;
La figura 2 muestra un diagrama de flujo de una primera realización del método de la invención;
La figura 3 muestra un diagrama de flujo de una segunda realización del método de la invención.

DESCRIPCION DETALLADA DE REALIZACIONES DE LA INVENCIÓN

En la siguiente descripción detallada, se hace referencia a los dibujos adjuntos que muestran, a modo de ejemplo,

realizaciones específicas en las que se puede poner en práctica la invención. Estas realizaciones se describen con suficiente detalle para permitir a los expertos en la materia realizar la invención. Debe entenderse que, por tanto, la siguiente descripción detallada no debe tomarse en un sentido limitativo, y el alcance de la presente invención definido solo por las reivindicaciones adjuntas, interpretadas adecuadamente, junto con el rango completo de equivalentes para los cuales las reivindicaciones están habilitadas. En los dibujos, los números similares se refieren a la misma entidad o funcionalidad similar en las distintas vistas.

La FIG. 1 muestra esquemáticamente un dispositivo no seguro UD. Este dispositivo UD puede comunicarse con un servidor SV según sea necesario. La comunicación puede ocurrir, por ejemplo, a través de Internet. El dispositivo tiene un almacén DS para almacenar datos confidenciales en la memoria. Este almacén DS normalmente almacena claves. Un dispositivo de claves de este tipo, por lo general, se ha cifrado usando lo que vuelve del servidor (una frase de contraseña segura) y lo que el usuario introduce (el código personal). La invención se aplica a cualquier DS de almacén bloqueado, en el que los datos se pueden cifrar. Varios dispositivos pueden usar el mismo servidor SV. Ventajosamente, el servidor utiliza algún entorno seguro, por ejemplo, el módulo de seguridad de hardware (HSM), para almacenar datos confidenciales y llevar a cabo todas las operaciones confidenciales.

Las comunicaciones entre el dispositivo UD y el servidor SV se protegen ventajosamente a través de uno o más mecanismos de seguridad. Por lo tanto, es posible que el dispositivo cifre todos los mensajes que envía al servidor utilizando la clave pública del servidor, que luego los descifra en un entorno seguro local.

Como parte de cada mensaje, el dispositivo envía ventajosamente una clave de cifrado que el servidor utiliza para responder al dispositivo. Ventajosamente, una nueva clave se genera cada vez. La clave puede ser simétrica o asimétrica y, en cualquier caso, el dispositivo utiliza la clave de descifrado correspondiente para descifrar la respuesta.

La FIG. 2 muestra un diagrama de flujo de una primera realización del método de la invención.

En un primer paso preliminar P0, se solicita al usuario que introduzca un de código personal PIN. Luego, se aplica una primera función F1 a dicho PIN personal introducido en un segundo paso preliminar P1, cuyo resultado se envía en un paso P2 a un servidor SV para el almacenamiento P3 del valor recibido F1 (PIN).

Cada vez que el usuario del dispositivo UD solicita acceso al depósito de claves DS, en un primer paso E0, se le solicita que introduzca su código personal, generalmente un Número de Identificación Personal (PIN, en lo sucesivo) o un código similar de un solo uso en el dispositivo.

El PIN no es conocido por el dispositivo. Sin embargo, el dispositivo puede tener una suma de comprobación CS del PIN para realizar una primera comprobación. En este caso, si la suma de comprobación del PIN no es correcta (CSN), un paso E7 implica que el almacén de claves DS permanezca bloqueado.

En cualquiera de los dos casos, el PIN se transfiere a un paso E2 en el que se calcula un código de acceso AC a partir de a al menos el PIN del código personal. Para este propósito, se aplica al código personal una primera función F1, ventajosamente un hashing.

De acuerdo con una realización ventajosa mostrada en una línea de puntos, se realiza un paso E1. El paso E1 consiste en recuperar un número aleatorio fijo RN para alimentar el paso E2 de crear el código de acceso AC aplicando la primera función F1 al código personal PIN y al número aleatorio RN. Por supuesto, en esta realización ventajosa, durante los pasos preliminares, la primera función también se aplica al código personal PIN y al mismo número aleatorio RN previamente generado y almacenado.

Ventajosamente, la suma del código personal y el número aleatorio fijo RN se procesa para obtener el código de acceso AC. El número aleatorio fijo es ventajosamente un código sal. El sal es un número aleatorio fijo que evita que un atacante use una tabla arcoiris para calcular el PIN de F1 (PIN) (definición en Criptografía aplicada, Bruce Shneier).

En una etapa E3, el dispositivo UD prepara un mensaje que incluye al menos un identificador del dispositivo (por supuesto, este identificador puede incluirse en la propia llamada) y el código de acceso AC.

En un paso E4, el servidor SV verifica que el código de acceso recibido AC se generó usando el PIN correcto.

En el caso, el código de acceso recibido corresponde al recibido previamente y almacenado en el paso preliminar P3 del método.

En una primera realización de una característica ventajosa de la invención que también se muestra en línea de puntos, la etapa E1 1 consiste en enviar un identificador ID_{UD} al servidor SV. En un paso E12, el servidor SV genera un número aleatorio utilizado una sola vez OTN. El dispositivo UD recibe dicho número aleatorio OTN y lo incluye en un mensaje con el identificador de dispositivo ID_{UD} y en una función F2 del código de acceso previamente calculado

y el número aleatorio OTN M (ID_{UD}, F2 (AC, OTN), OTN). Dicha función F2 es conocida desde el servidor SV.

Luego, el servidor SV verifica en el paso E4 si el mensaje del dispositivo contiene el número aleatorio OTN correcto. Si se incluye cualquier otro número aleatorio, el servidor SV asume que se trata de un ataque de repetición y lanza una contramedida. Por ejemplo, dicha contramedida puede consistir en enviar una frase de contraseña incorrecta.

De lo contrario, el servidor SV calcula la función F2 (AC, OTN) a partir del código de acceso previamente almacenado AC y de la OTN recibida. Si los datos recibidos F2 (AC, OTN) coinciden, significa que el código de acceso AC utilizado por el dispositivo para el cálculo de F2 es correcto, y se envía una frase de contraseña PP al dispositivo UD. En un paso E6, el dispositivo UD desbloquea el depósito de claves DS mediante una función de la frase de contraseña PP y el PIN. El usuario puede acceder a las claves almacenadas en el almacén DS.

La FIG. 3 muestra un diagrama de flujo de una segunda realización de la característica ventajosa previamente expuesta de la invención que consiste en usar una contraseña de un solo uso en el método de la invención. Los pasos preliminares son idénticos a los de la figura 2 y esta figura solo muestra el método después del paso E0, donde el usuario solicita acceso al depósito de claves DS.

Después del primer paso, E0, donde se le solicita al usuario que introduzca su código personal, si la suma de comprobación CS del PIN no es correcta, el depósito de claves permanece bloqueado en un paso E7. El depósito de claves también puede ser destruido después de un número predeterminado de intentos incorrectos. Si la suma de comprobación CS del PIN es correcta, se realizan dos pasos E1 y E10. El paso E1 consiste en generar y almacenar un número aleatorio fijo RN, o en recuperarlo si se generó previamente, para alimentar el paso E2 de crear un código de acceso AC.

La etapa E10 consiste, para el dispositivo UD, en generar un número aleatorio OTN que es un valor de secuencia SEQ. Normalmente, el valor de secuencia SEQn consiste en un número cada vez mayor, una marca de tiempo o algún otro dato similar.

Luego, en un paso E3, el dispositivo U D crea un mensaje M (ID_{UD}, F2 (AC, SEQn), SEQn) cifrado de manera ventajosa. Luego lo envía al servidor SV. El servidor SV mantiene el registro del último valor de secuencia SEQn-1 que ha visto. El intento de repetición del ataque se revelaría porque el valor de la secuencia permanecería sin cambios o saltaría hacia atrás.

El código de acceso AC es ventajosamente una función, por ejemplo un hash, de F1 (PIN, RN) del código personal PIN y el número aleatorio fijo RN.

En una etapa E4, el servidor SV verifica la corrección de la función F2 del código de acceso AC y el valor de secuencia SEQn y la exactitud del valor de secuencia SEQn en comparación con el SEQn-1 recibido previamente.

La presencia del número aleatorio en las dos realizaciones de la característica ventajosa protege contra la reproducción al hacer único el mensaje enviado por el dispositivo. Esta característica permite detectar la clonación. Para clonar el dispositivo, el atacante tendría que copiar al menos el depósito de claves y otras características que permiten que el servidor no pueda distinguir el dispositivo original y los dispositivos clonados entre sí. Sin embargo, el servidor detectará el uso activo de más de un dispositivo con el mismo identificador de dispositivo mediante el uso de un número aleatorio utilizado una sola vez y puede iniciar contramedidas apropiadas que incluyen, entre otras, el bloqueo del uso posterior de los dispositivos.

En una realización preferida, el dispositivo envía con cada mensaje un valor de secuencia que revela no solo el orden de los mensajes, lo que permite la revelación de ataques de repetición, sino también el número de valores de secuencia generados, es decir, si dos valores de secuencia son adyacentes, separados por un valor intermedio, dos valores, tres valores, etc.

Dependiendo de la sofisticación del ataque, dos o más dispositivos que usen los mismos identificadores de dispositivo se revelarán creando lo que parecería un ataque de repetición o haciendo que el valor de la secuencia salte en incrementos mayores de lo que podría explicarse suponiendo que el servidor y el dispositivo pierdan la sincronización debido a un fallo ocasional de comunicación.

El valor de secuencia SEQn utilizado para detectar la clonación podría, por supuesto, usarse también para detectar ataques de repetición si así se desea. En cualquier caso provocará contramedidas.

Por ejemplo, dicha contramedida puede consistir en enviar una frase de contraseña incorrecta.

De lo contrario, si el código de acceso AC y el número aleatorio son correctos, se envía una frase de contraseña PP al dispositivo UD. En un paso E6, el dispositivo UD desbloquea el DS del depósito de claves utilizando la frase de contraseña PP y el PIN. El usuario puede acceder a las claves almacenadas en el almacén DS.

Se pueden habilitar algunos requisitos de seguridad para contrarrestar varios ataques. Se aplicarán principios de diseño de seguridad. Por ejemplo, cualquier secreto que se encuentre en la memoria de trabajo del dispositivo debe sobrescribirse tan pronto como ya no sea necesario. El PIN nunca se almacena en el dispositivo y nunca se comunica al servidor. En su lugar, se utiliza el código de acceso y, en caso de necesidad, una suma de comprobación del PIN dentro del dispositivo. Esto protege la confidencialidad del PIN.

El mensaje cifrado enviado por el dispositivo únicamente puede ser cifrado/descifrado en un entorno seguro dentro del servidor. Si el servidor o la línea de comunicación se ven comprometidos, el atacante no tendrá acceso a la información cifrada. El entorno seguro, por ejemplo, HSM, está configurado para revelar la frase de contraseña asociada con una identidad de dispositivo determinada solo si se utiliza el código de acceso correcto y todas las comprobaciones de seguridad se pasan con éxito.

Ventajosamente, se registran las incidencias de códigos de acceso incorrectos y cuando se exceden algunos límites predeterminados, por ejemplo 4 intentos fallidos consecutivos o el 10% de fallos de los últimos 100 intentos, se pueden activar contramedidas adicionales. Por ejemplo, el dispositivo puede ser bloqueado completamente del sistema o el servidor puede aumentar exponencialmente su tiempo de respuesta al dispositivo. Este enfoque protege contra ataques por la fuerza cuando el atacante intenta adivinar el PIN incluso si ya conoce la sal.

Además, el servidor cifra el mensaje que contiene la frase de contraseña para el depósito de claves dentro del entorno seguro y el dispositivo nunca almacena ni la frase de contraseña ni la clave de descifrado en la memoria persistente, lo que protege la confidencialidad de la frase de contraseña.

Si se encuentra un código de acceso incorrecto, el servidor puede o no informarle al dispositivo explícitamente dependiendo de la configuración deseada. Si no se indica el dispositivo explícitamente, el servidor devolverá una frase de contraseña incorrecta al dispositivo. Entonces, dependería del dispositivo detectar que la frase de contraseña es incorrecta, si lo detecta.

La seguridad aumenta al utilizar la frase de contraseña del servidor en combinación con el PIN del usuario final para desbloquear el depósito de claves, en lugar de usar la frase de contraseña directamente. Esto significa que el lado del servidor no posee toda la información necesaria para acceder a las claves, lo que proporcionando integridad incorporada al sistema. El PIN y la frase de contraseña se pueden combinar de varias formas, incluidas la concatenación, XOR y otras operaciones matemáticas. Otras operaciones, como las funciones unidireccionales, también pueden aplicarse al PIN o la frase de contraseña o cualquier otro resultado intermedio durante el proceso.

El código de acceso (AC) enviado al servidor también puede ejecutarse enviando otros datos personales al servidor, que pueden ser la respuesta a una pregunta como "¿cuál es el apellido de soltera de su madre", etc.

La invención permite utilizar frases de contraseña cortas en dispositivos no seguros de criptografía de dos factores mientras se mantiene la confidencialidad de los secretos en el depósito de claves. El código personal es lo que el usuario sabe y el código criptográfico corresponde al dispositivo que es el que tiene el usuario. La invención también proporciona una solución para la detección de la clonación del depósito de claves.

En cualquier caso, la invención no implica la circulación de ningún dato confidencial encriptado o no. Las claves se encuentran solo en el almacén de claves y, salvo en el caso de clonación del depósito de claves, no es posible el acceso de un atacante.

El alcance de la presente invención se define únicamente por las reivindicaciones adjuntas, interpretadas de manera apropiada, junto con la gama completa de equivalentes para las que las reivindicaciones están habilitadas.

En particular, los pasos relativos a la creación del número aleatorio pueden realizarse en cualquier momento antes del paso E3 sin apartarse del alcance de la invención. También el descifrado es una forma de desbloqueo ya que, si el depósito de claves es un archivo almacenado en un dispositivo, el cifrado parece ser el único mecanismo de bloqueo. Si el depósito de claves se almacena en una tarjeta SIM o tarjeta inteligente, el desbloqueo sería simplemente presentar la frase de contraseña correcta.

REIVINDICACIONES

1. Método para acceder a un almacén de datos (DS) previamente bloqueado usando una frase de contraseña (PP) desde un dispositivo (UD), incluyendo dicho método los pasos preliminares de:

- para el dispositivo (UD), solicitar (P0) al usuario que introduzca un código personal (PIN) en el dispositivo (UD);
- para el dispositivo (UD), calcular (P1) una primera función (F1) de al menos el código personal (PIN);
- para el dispositivo (UD), enviar (P2), para el almacenamiento (P3), dicha primera función (F1) a un servidor (SV) que conoce la frase de contraseña (PP);

dicho método comprende además los siguientes pasos, cuando el usuario solicita acceso al almacén de datos (DS):

- para el dispositivo, solicitar (E0) al usuario que introduzca el código personal (PIN),
- para el dispositivo, generar (E2) un código de acceso (AC) aplicando dicha primera función (F1) a al menos el código personal (PIN) introducido;
- para el dispositivo, enviar (E3), al servidor (SV), al menos un identificador (ID_{UD}) del dispositivo (UD) y el código de acceso (AC);
- para el servidor (SV), comparar (E4) el código de acceso (AC) con la primera función preliminar recibida;
- para el servidor (SV), si el código de acceso (AC) es correcto, devolver la frase de contraseña (PP) al dispositivo (UD);
- para el dispositivo (DV), desbloquear el almacén de datos (DS) usando la frase de contraseña (PP) recibida en combinación con el código personal (PIN) introducido.

2. Método según la reivindicación 1, que comprende: -

- antes del cálculo preliminar de la primera función (F1), un paso de cálculo y almacenado de una suma de comprobación (CS) del código personal (PIN);
- cada vez que el usuario introduce el código personal (PIN), un paso de cálculo de la suma de comprobación (CS) del código personal (PIN) introducido;
- un paso para de comparación de la suma de comprobación (CS) calculada con la suma de comprobación previamente almacenada,
- si existe una discrepancia (CS_N), un paso de exhibición de un mensaje de error, y
- si la suma de comprobación es correcta (CS_Y), procesado de los siguientes pasos del método.

3. Método según una de las reivindicaciones 1 y 2, que comprende los pasos preliminares de generar (E1) un número aleatorio fijo (RN) y de almacenarlo en el dispositivo (UD), siendo la primera función (F1) una función del código personal (PIN) y del número aleatorio fijo (RN).

4. Método según la reivindicación 3, en el que la primera función (F1) es una función de la suma del código personal (PIN) y el número aleatorio fijo (RN).

5. Método según una de las reivindicaciones precedentes, en el que el almacén de datos (DS) es previamente encriptado y almacenado en el dispositivo (UD).

6. Método según una de las reivindicaciones 1 a 4, en el que el almacén de datos (DS) es almacenado previamente en una tarjeta inteligente que tiene acceso bloqueado y está vinculada al dispositivo (DV).

7. Método según una de las reivindicaciones precedentes, que comprende, cada vez que el usuario solicita acceso al almacén de datos (DS), un paso para determinar el número aleatorio utilizado una sola vez (OTN) enviado al servidor (SV) con el código de acceso (AC).

8. Método según la reivindicación 7, en el que el servidor (SV) genera (E12) el número aleatorio utilizado una sola vez (OTN) y el dispositivo (DV) lo recupera del servidor (SV) cada vez que el usuario solicita acceso al almacén de datos (DS), el servidor (SV) comprueba el número aleatorio (OTN) y luego lo recibe de nuevo del dispositivo (UD).

9. Método según la reivindicación 7, en el que el número aleatorio utilizado una sola vez (SEQn) se calcula (E10) en el dispositivo (UD) y se vincula al número aleatorio utilizado una sola vez enviado previamente (SEQn-1) para el servidor (SV) para comprobar la secuencia de los números aleatorios utilizados una sola vez.

10. Método según la reivindicación 9, que comprende un paso adicional de, después del cálculo (E2) del código de acceso (AC), calcular una segunda función (F2) del código de acceso (AC) y del número aleatorio (OTN, SEQn), un paso para enviarlo al servidor (SV) con el número aleatorio (OTN, SEQn) y un paso (E4), para que el servidor (SV) verifique la información enviada realizando la misma operación que el dispositivo (UD), utilizando el código de acceso (AC) previamente almacenado y el número aleatorio recibido (OTN, SEQn).

11. Método según una de las reivindicaciones precedentes, en el que la introducción del código personal (PIN) se

realiza mediante incorporación segura.

12. Método según una de las reivindicaciones precedentes, en el que siendo seguras las comunicaciones entre el dispositivo (UD) y el servidor (SV), el dispositivo (UD) cifra los mensajes utilizando una clave pública del servidor (SV).

13. Método según la reivindicación 12, en el que el servidor (SV) comprende un entorno seguro en donde se realiza el descifrado de los mensajes.

14. Método según una de las reivindicaciones precedentes, en el que siendo seguras las comunicaciones entre el dispositivo (UD) y el servidor (SV), el dispositivo (UD) envía una clave de cifrado utilizada una sola vez al servidor (SV) que la utiliza para cifrar el envío de la frase de contraseña (PP).

15. Método según una de las reivindicaciones precedentes, en el que la primera función (F1) es una función de hashing.

16. Dispositivo (UD) habilitado para implementar el método según se reivindica en una de las reivindicaciones 1 a 15, teniendo dicho dispositivo (UD) al menos un almacén de datos (DS) previamente bloqueado utilizando una frase de contraseña (PP), un módulo de adquisición de código personal (PIN) , un módulo de cálculo capaz de generar un código de acceso (AC) aplicando una primera función (F1) a al menos al código personal (PIN) introducido, un transmisor para enviar al menos un identificador (ID_{UD}) del dispositivo (UD) y el código de acceso (AC) a un servidor (SV) que conoce la frase de contraseña (PP) para el almacenamiento, un receptor para recibir una frase de contraseña (PP) del servidor (SV), un módulo de desbloqueo para desbloquear el almacén de datos (DS) usando la frase de contraseña recibida (PP) en combinación con el código personal (PIN) introducido por el usuario.

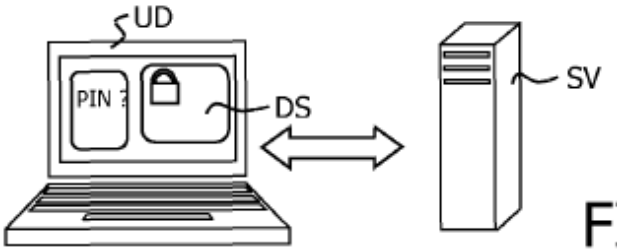

FIG.1

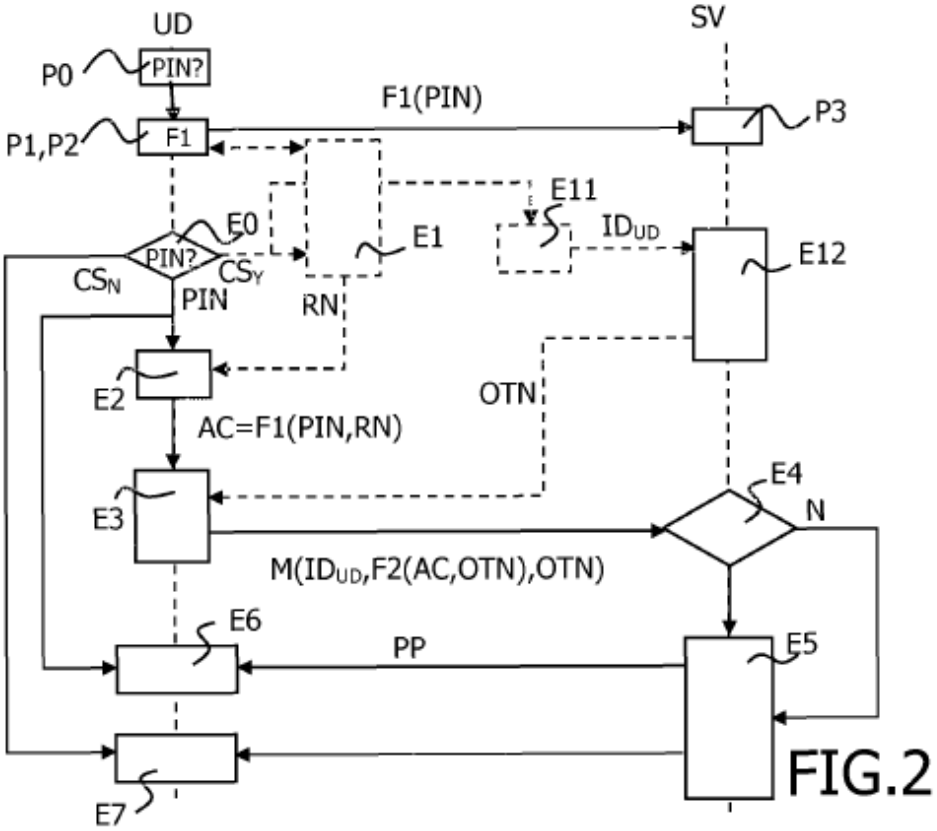

FIG.2

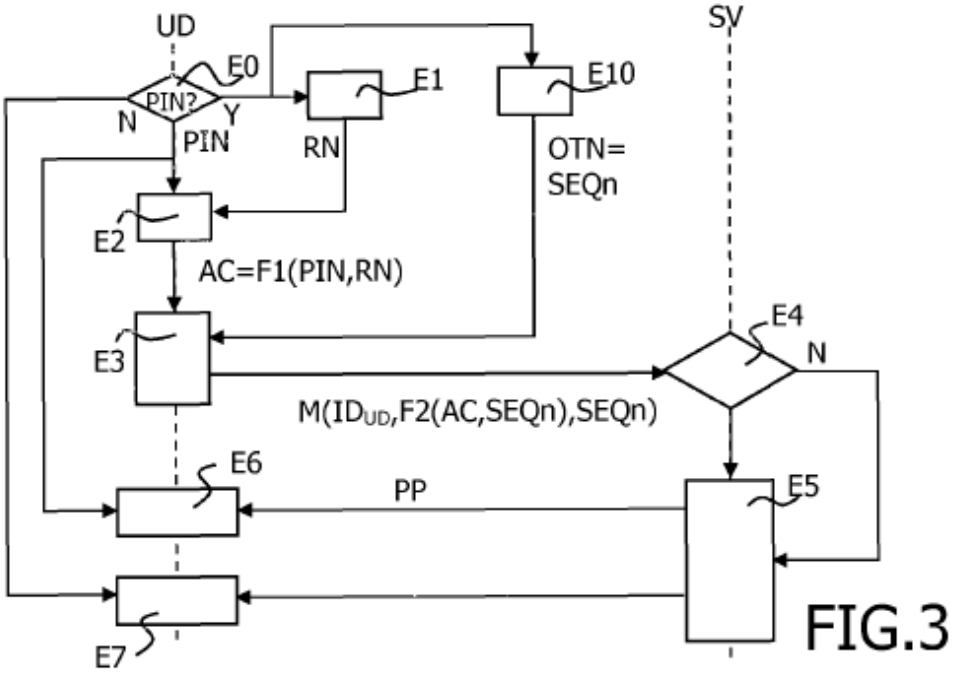

FIG.3