(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 416 483**

(51) Int. CI.:

G06F 21/34 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **29.04.2009 E 09749482 (7)**

(97) Fecha y número de publicación de la concesión europea: **03.04.2013 EP 2281259**

(54) Título: **PIN modificable para token de hardware**

(30) Prioridad:

20.05.2008 DE 102008024364

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.08.2013

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
Friedrich-Ebert-Allee 140
53113 Bonn, DE

(72) Inventor/es:

KRAMARZ-VON KOHOUT, GERHARD

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

PIN modificable para token de hardware

La invención se refiere a un sistema de gestión de contraseñas para su modificación y verificación de la contraseña y asignar la contraseña a un token de hardware, en particular, una tarjetas de banda magnética y/o una tarjeta inteligente, en donde la contraseña sirve para autenticar el token de hardware frente a un sistema técnico, en donde la contraseña es un número de identificación personal PIN y en donde el PIN se puede determinar por medio un algoritmo de los datos a leer que se almacena en el token de hardware.

Se conocen token de hardware tales como tarjetas de banda magnética puras, así como tarjetas combinadas que tienen tanto un chip como una banda magnética.

Tales tarjetas con banda magnética, inteligentes o combinadas funcionan como una tarjeta de cliente. Por ejemplo, las tarjetas bancarias permiten a sus usuarios a retirar dinero de los cajeros automáticos y el pago electrónico en las cajas de comercio al por menor dotadas para ello.

El cliente generalmente recibe un PIN, es decir, un número de identificación personal, para proteger la aplicación que utiliza los datos del token de hardware.

Los métodos de autenticación rara vez funcionan sin contraseña. Una tarjeta con banda magnética, tarjeta inteligente, combinada u otro token de hardware, por ejemplo, suelen ser liberadas mediante la introducción de un PIN numérico. El término "contraseña en el marco de esta invención de forma se usa equivalente al término "PIN (número de identificación personal)". Una contraseña es una información de autenticación que se conoce sólo por el usuario legítimo. Un PIN puede ser alfanumérico, pero en las tarjetas de cliente descritas a menudo consiste sólo de una secuencia de números.

Los datos de una tarjeta de banda magnética no están protegidos y están almacenados en la banda magnética sin copia de seguridad. Cualquier persona con un dispositivo de lectura y de escritura correspondiente puede leer los datos o sobrescribirlos.

El PIN por lo tanto, típicamente no es parte de los datos que puede leer cualquier persona, es decir que se almacenas, por ejemplo, en una banda magnética. En su lugar, el PIN se deriva por medio de un proceso criptográfico de los datos almacenados en la banda magnética. El cálculo del PIN no se realiza en la misma tarjeta de banda magnética, ya que esta, como tarjeta de datos pura, no puede hacer ningún tipo de cálculo. En cambio, el cálculo se realiza ya sea fuera de línea (por ejemplo, para tarjetas bancarias esto significa un cálculo dentro de los cajeros automáticos) o en línea (por ejemplo, para tarjetas bancarias esto significa un cálculo en un servidor central, que está conectado a los cajeros automáticos individuales), por ejemplo, generando un valor hash a partir de los datos almacenado en la banda magnética (con una tarjeta bancaria, esto podrían ser el número de cuenta, el código bancario y número de serie). Para que el cliente reciba un PIN formado por dígitos decimales, el valor hash, si es originalmente un valor hexadecimal, debe ser convertido en dígitos decimales de forma entera o dígito por dígito. Las últimas cifras del hash decimal entonces podrían representar el PIN. Por tarjeta bancaria de hoy, el PIN tiene cuatro dígitos.

El cliente recibe el PIN mediante la empresa que emite la tarjeta (por ejemplo, a través de su banco). El PIN no se puede cambiar por el cliente, debido a que los datos de los que se deriva el PIN, son constantes. La validez del PIN que así se predetermina para él de forma fija es ilimitada, o sólo es limitada por la validez general de la tarjeta (la validez de las tarjetas bancarias suele ser de varios años). Es, como se describe, por lo general puramente numérico.

Si el cliente pierde su tarjeta, puede bloquearla a través de la empresa emisora de la tarjeta. Si después de la pérdida recibe una nueva tarjeta, entonces también recibe un nuevo código PIN, que por lo general difiere del PIN anterior. Además, este PIN de nuevo no es un PIN elegido por el cliente, sino se fija por la empresa emisora de la tarjeta.

El usuario tiene que recordar la contraseña, ya sea en la memoria o tiene que depositarlo de forma lógica y/o físicamente segura para impedir que terceros accedan de forma fácil a la información. Sería concebible, por ejemplo, la transcripción de la contraseña en un pedazo de papel, que, a continuación, se deposita en una caja fuerte.

Por razones de seguridad una contraseña debe ser cambiada tan a menudo como sea posible, ya que con el tiempo, aumenta la posibilidad, respectivamente, aumenta el riesgo de que un tercero - intencionalmente o accidentalmente - tenga conocimiento de la contraseña sin autorización. Se recomienda, por ejemplo, en los sistemas informáticos por lo general un cambio aproximadamente cada 30 días. Aquí, uno debe abstenerse de la reutilización de contraseñas antiguas, así como el uso múltiple de la misma contraseña en diferentes cuentas y/o equipos. Algunos sistemas operativos modernos recuerdan al usuario de la expiración de la validez de su contraseña y le solicitan con tiempo y si es necesario varias veces en intervalos regulares (por ejemplo, con 8 días de antelación, con 7 días de antelación, ...) cambiar su contraseña.

En el documento EP 1685471 B1 se describe un método tal como a una tarjeta inteligente se le puede asignar un PIN que no es siempre válido, pero puede tener una validez individual en función de la calidad del PIN.

La publicación "Omer Berkman et al:" The Unbearable Lightness of PIN Cracking" en Financial Cryptography and Data Security [notas de conferencia en Computer Science] editorial Springer Verlag, Berlín, Heidelberg, tomo 4886, 12 de febrero de 2007, páginas 224 - 238 (ISBN: 978-3-540-77365-8), describe dos métodos, llamados métodos de IBM 3624 y el método del valor de verificación del PIN VISA (PVV), en los que en cada caso se utiliza un valor de verificación que comprende de cuatro cifras decimales, que en el método IBM 3624 se denomina "valor de compensación" y en el método VISA PVV " valor de verificación del PIN (PW)", véase D1: p.231 y siguientes. El valor de verificación se puede almacenar en una base de datos o en la tarjeta del cliente y permite al cliente cambiar su PIN. El valor de compensación V se determina a partir de V = P - G (A), en donde P es el PIN encriptado dentro de un bloque de PIN EPB (bloque de PIN encriptado), A es un número de cuenta y g es una función que calcula un número que comprende cuatro dígitos decimales. El valor de compensación corresponde a un valor de diferencia entre un nuevo PIN P solicitado y el PIN inicial, que se determina a partir de g(A). Esta publicación, por lo tanto, describe un método para la re-asignación de un PIN, en el que se almacena un valor de diferencia entre el PIN solicitado y el PIN inicial en el token de hardware para determinar el nuevo PIN. Otra revelación similar se encuentra en el documento US 2007/282756 A1, que describe también el uso de un valor de compensación para la determinación de PINs (nuevos).

Una desventaja en las conocidas tarjetas de banda magnética, tarjetas combinadas y similares es que el PIN una vez asignado no se puede cambiar y por lo tanto a medida que avanza el tiempo de uso se acompaña de un aumento de riesgo de espiar el PIN y un uso no autorizado de la tarjeta.

El objeto de la invención es superar estas desventajas, desarrollar el proceso de la clase mencionada de tal manera, que se supera la restricción en tarjetas inteligentes, y permitir, en particular, poder cambiar en una tarjeta de banda magnética el PIN asignado y asignar al PIN de una tarjeta de banda magnética un tiempo de validez individual dependiendo de la calidad de la PIN, es decir en particular, cambiar el PIN de cualquier token de hardware.

Este objeto se consigue por el sistema o el procedimiento indicado en las reivindicaciones independientes.

Las realizaciones ventajosas y perfeccionamientos de la invención son evidentes a partir de las reivindicaciones dependientes.

Es una ventaja particular del sistema de gestión de contraseña según la invención para el cambio y la comprobación de una contraseña y la asignación de esta contraseña a un token de hardware, en particular, una tarjeta de banda magnética y/o la tarjeta inteligente, donde se utiliza la contraseña para la autenticación del token de hardware frente a un sistema técnico, en donde la contraseña a un número de identificación personal PIN y en donde el PIN se puede determinar por medio de un algoritmo de datos almacenados de forma legible en el token de hardware, que para cambiar el PIN original a un nuevo PIN se almacena un valor de cambio legible en el token de hardware y/o en el sistema de gestión de contraseñas, que se utiliza para determinar el nuevo PIN por medio del mismo algoritmo o uno diferente. En el caso de la tarjeta combinada el valor de cambio, en principio, también podría ser almacenado en el chip.

Por tanto, es posible poder cambiar el número de identificación personal, es decir el PIN, asociado a una tarjeta, que, por medio del cual varias aplicaciones se autentican y autorizan utilizando la tarjeta.

En el caso del valor de cambio, que se almacena en el token de hardware y/o en una base de datos del sistema de gestión de contraseñas, se trata de un valor de entrada de una función hash con la que se determina al menos se determina el nuevo PIN.

Al almacenar el valor de cambio en el token de hardware, por ejemplo, en la banda magnética de una tarjeta de banda magnética o en el chip de una tarjeta inteligente o tarjeta combinada, este valor de cambio se lee directamente de una manera ventajosa. Como alternativa o acumulativamente, este valor de cambio también puede ser almacenado en el lado del sistema en una base de datos correspondiente del sistema de gestión de contraseñas. Si el valor de cambio se almacena únicamente en el lado del sistema y no se almacena de forma adicional en el token de hardware, se aumenta aún más la seguridad, ya que el token de hardware no contiene la información correspondiente. Si, alternativamente, el valor de cambio se almacena legible tanto en el token de hardware como también en el lado del sistema en una base de datos, la seguridad se incrementará en un posible examen adicional mediante una comparación adecuada.

Seguidamente se detalla como las características correspondientes (validez no permanente del PIN, validez individual del PIN dependiendo de la calidad de la PIN) pueden ser implementadas para las tarjetas con banda magnética, siendo la ilustración sólo a modo de ejemplo y no limitado a tarjetas de banda magnética, pero es aplicable a cualquier token de hardware, que comprende un área de datos escribible y legible, en donde en PIN se deriva de datos allí almacenados.

Para el cambio del PIN se pueden utilizar dos procedimientos. El método I que se describe a continuación es el estado de la técnica:

Método I: valor diferencial en texto plano

Además se ha de almacenar un "valor diferencial" en la banda magnética, que inicialmente puede tener el valor 0, pero también cualquier valor individual para la tarjeta.

Por lo tanto, valor diferencial = 0 se corresponde con el PIN original, el cual, como se ha descrito, se deriva de un valor hash de los datos almacenados en la banda magnética.

Un nuevo PIN y el PIN original tienen una cierta diferencia matemática, que de acuerdo con la invención se almacena como valor de diferencia en la banda magnética. Ahora, cuando el cliente introduce su PIN, este PIN se puede verificar fuera de línea o en línea cuando el sistema dispone además del propio método criptográfico, tanto los datos de la banda magnética, de los cuales se puede determinar el PIN original, como también el valor diferencial de la banda magnética. El PIN introducido es correcto si la diferencia entre el valor de entrada y el PIN original (el sistema calcula como hasta el momento) se corresponde con el valor diferencial.

Para configurar un nuevo PIN hay que poner a la disposición del cliente una aplicación para cambiar su PIN (por ejemplo, como un punto de selección adicional en el uso de cajeros automáticos) en cuyo curso se compara el PIN original y el PIN nuevo y se almacena el valor diferencial en la banda magnética.

El almacenamiento adicional del valor diferencial en texto sin formato en la banda magnética en cuanto a la técnica de seguridad básicamente no es problemático, siempre y cuando el método para calcular el PIN original es seguro. El valor diferencial en sí no proporciona información adicional para un atacante para determinar el PIN original o el PIN actual. Como antes, el usuario está obligado a mantener en secreto su PIN cambiado.

Un atacante solo podría inferir el PIN actual a partir del conocimiento del valor diferencial, si conoce el PIN original (valor diferencial = 0) o, en general, un PIN anterior con el valor diferencial. A este respecto, el usuario debe tratar esta información de forma confidencial.

Para relevar en este punto un poco al usuario, el primer PIN que el cliente recibe de su compañía emisora de tarjeta, no debería ser el "PIN original" con valor diferencial = 0, sino un PIN diferente, con un valor diferencial individual desigual a 0.

Método II: valor de entrada adicional para la función de hash

Sin embargo, el almacenamiento del valor diferencial en texto plano en la banda magnética permite que cualquier persona lea esto. En este sentido es posible que alguien que conoce el PIN actual y el valor diferencial actual, determinar sin problemas el nuevo PIN, si también conoce el nuevo valor diferencial.

Con el fin de evitar este riesgo y prevenir la deducción del nuevo PIN para cualquiera que conoce el PIN antiguo, los datos anteriores sobre la banda magnética, se sugiere el siguiente procedimiento.

El valor hash a partir del cual, como se ha descrito, se obtiene el PIN, recibe un valor de entrada adicional para ser almacenado en la banda magnética. Para el PIN original este valor de entrada de PIN debe tener el valor 0 o otro valor inicial diferente. El valor de entrada puede ser individual para cada cliente.

Debido a la clasificación de una función hash, un valor de entrada modificado, por lo general, conduce a un cambio de PIN. En el caso de una función hash adecuado los valores son distribuidos homogéneamente, cada PIN es, pues, igual de probable. Si el PIN es ahora relativamente corto (sólo alrededor de 4 dígitos) y existe la capacidad computacional para determinar para muchos valores de entrada el PIN asociado, la probabilidad es muy alta, en caso de valores hash uniformemente distribuidos respecto a un PIN deseado, de encontrar también un valor de entrada coincidente. En el caso de un PIN de 4 dígitos, es decir, en caso de 10.000 valores diferentes para el PIN y, a 100.000 intentos con diferentes valores de entrada para una función hash con los valores de hash distribuidas de manera uniforme, la probabilidad es de >99,99%, de uno de los intentos conduce al PIN deseado.

Para configurar un nuevo PIN, por lo tanto, hay que poner a disposición del cliente una aplicación para cambiar su PIN (por ejemplo, como un punto adicional de selección en el uso de un cajero automático). Durante su transcurso el cliente entra en su PIN deseado. La aplicación varias veces pasará a través de la función hash con los valores de entrada cambiados hasta que se ha encontrado un valor de entrada adecuado para el PIN. Este valor de entrada se almacena en la banda magnética. El cliente recibe correspondiente un mensaje del sistema positivo. Si la solicitud no encontrara ningún valor de entrada adecuado en un período de tiempo aceptable para el cliente, entonces el cliente recibirá un mensaje de error correspondiente. Como alternativa, la aplicación puede sugerir a los clientes varios PINs nuevos, para los que ha encontrado valores de entrada durante el cálculo anterior. El cliente puede elegir uno de los PIN propuestos como su nuevo PIN. El valor de entrada correspondiente se almacena en la banda magnética.

Ambos métodos permiten una variabilidad del PIN de una tarjeta con una banda magnética.

Cuando el valor diferencial del Método I o el valor de entrada del Método II no se almacenan en la banda magnética, sino se almacena en el sistema, también es dada la variabilidad del PIN. Como ventaja resulta en un mayor nivel de seguridad, ya que a un tercero que solo conoce los datos de la banda magnética, permanecerán ocultos el valor diferencial o bien el valor de entrada. Como desventaja se presenta la necesidad de llevar una base de datos en el lado del sistema en la que se almacenan por cada cliente el valor diferencial correspondiente o bien el valor de entrada, en donde esta base de datos se consulta en cada verificación de PIN.

En lugar de mantener una base de datos en el lado del sistema y proceder como se describe anteriormente, también es posible almacenar el valor diferencial en el chip de una tarjeta combinada que tiene tanto un chip como una banda magnética. Entonces, es posible leer los datos correspondientes y evaluarlos en el lado del sistema, o por medio de chip llevar a cabo del análisis de los datos, es decir, la determinación del PIN.

Tarjetas de banda magnética nunca tienen un temporizador interno. Por lo tanto, un control de la validez del PIN de tal no es posible. Sin embargo, si una base de datos del lado del sistema está disponible, en el sentido del documento EP 1685471 B1 como contador para tarjetas inteligentes, por ejemplo, se puede almacenar el número de entradas de PIN en el sistema. Si el contador ha alcanzado o superado un cierto valor umbral, el PIN ya no es válido, la aplicación solicita al usuario cambiar el PIN. Al igual como se describe en términos de tarjetas inteligentes en el documento EP 1685471 B1, aquí un PIN mejor (por ejemplo, un PIN de seis en lugar de cuatro dígitos) puede conducir a un valor límite superior, para dar a los usuarios un incentivo para elegir una PIN mejor.

Si en el sistema se puede almacenar el momento del último cambio de PIN, entonces de forma alternativa con respecto al contador descrito en el sistema se puede controlar la validez del PIN mediante la evaluación de tiempo. El período de validez máximo del PIN a su vez, como se describió anteriormente, se puede definir en una función del grado de calidad del PIN.

Ni el contador descrito anteriormente (número de entradas de PIN o similar) ni el momento descrito (último cambio de PIN, o similar) deberán registrarse directamente sólo en la banda magnética de la tarjeta. El análisis de estos datos entonces daría lugar a errores o problemas de seguridad, ya que los datos podrían ser cambiados por cualquiera. A este respecto, una grabación protegida y evaluación del contador o bien del momento en el tiempo es imprescindible en el lado del sistema o también en el chip de una tarjeta combinada para asegurar un método fiable.

Aunque después de un cambio en de tarjeta, por ejemplo, debido a la pérdida de la tarjeta anterior, el usuario recibe un nuevo PIN, que puede ser diferente del PIN de la tarjeta anterior, el usuario ahora puede cambiar este según sus deseos, por ejemplo, al PIN de su tarjeta anterior .

El usuario de un sistema de procesamiento de datos o una aplicación define una contraseña (PIN) de su preferencia durante el uso inicial. El sistema calcula sobre la base de una función de evaluación interna (función de evaluación) de forma automática el nivel de seguridad de la contraseña.

Preferiblemente, el nivel de seguridad de la contraseña numérica para una tarjeta con banda magnética se determina individualmente con particular referencia a uno o más de los siguientes criterios: la longitud de la contraseña, el tipo y el número de repeticiones de las cifras utilizadas. Esquemas especiales de la contraseña (por ejemplo, 4711, 0815) o la coincidencia de la contraseña con los datos maestros de usuario (por ejemplo, la contraseña 0405 un cliente que nació el 04 de mayo) pueden ser otros criterios.

El sistema puede determinar automáticamente la validez de la contraseña en dependencia del nivel determinado de seguridad de la contraseña. Es decir, las contraseñas de alta seguridad pueden ser utilizadas, por ejemplo, algunos meses, contraseñas menos seguras, por ejemplo, no en absoluto, o sólo unos pocos días o semanas.

La validez de la contraseña no determina contante para todos los usuarios y todas las contraseñas posibles, por ejemplo, cuatro semanas, sino se determina en función de la calidad de la contraseña de forma individual.

Opcionalmente se prevé que el usuario se le puede requerir de forma automática a tiempo, por lo general poco antes de la expiración de la validez de la contraseña, por el sistema para cambiar su contraseña y crear una nueva contraseña. Del mismo modo, el usuario puede cambiar su contraseña en cualquier momento, a petición propia.

El proceso de la invención se consigue que el usuario de la tarjeta no sólo pueda cambiar su PIN, pero lo tiene que cambiar, y al hacerlo tiene un incentivo para elegir un PIN (más) seguro:

Dos formas de realización de la invención se ilustran esquemáticamente en las figuras y se explican a continuación. En los dibujos muestran:

Figura 1 una primera tarjeta de banda magnética;

Figura 2 una segunda tarjeta de banda magnética.

La tarjeta de banda magnética 1 mostrada en las Figuras tiene una banda magnética 2 en la que se pueden almacenar y leer datos. A partir de los datos leídos desde la banda magnética 2 por medio de una función hash h, que se aplica a los datos, se determina el número de identificación personal PIN.

En el ejemplo de realización de la Figura 1, en la banda magnética 2 de la tarjeta de banda magnética 1, además de un primer campo de datos que contiene los datos (data), se almacena un valor de cambio x una vez realizado el cambio del PIN en un segundo campo de datos de la banda magnética 2, en donde el valor de cambio x forma un valor diferencial entre el PIN anterior y el PIN modificado. El PIN modificado se calcula mediante la función hash h a partir de datos almacenados en la tarjeta 1 (data) y posteriormente teniendo en cuenta el valor diferencial x de acuerdo con la siguiente fórmula:

PIN = h (data) + x

en la que

PIN = número de identificación personal

h = función de hash utilizada para calcular el PIN

data = datos como valores de entrada para h

x = valor de cambio como el valor diferencial

En el segunda ejemplo de realización según la Figura 2 en la banda magnética 2 de la tarjeta de banda magnética 1, además de un primer campo de datos que contiene los datos (data), se almacena un valor de cambio y después de realizar el cambio de PIN en un segundo campo de datos de la banda magnética 2, en donde el valor de cambio y forma un valor de entrada. El nuevo PIN se calcula mediante la función hash h a partir de los datos (data) almacenado en la tarjeta 1, completado por el valor de cambio y, utilizando la siguiente fórmula:

PIN = h (data, y)

en la que

PIN = número de identificación personal

h = función de hash utilizada para calcular el PIN

data = datos como valores de entrada para h

y = valor de cambio como un valor de entrada adicional para h

REIVINDICACIONES

1. Sistema de gestión de contraseñas para la modificación y comprobación de una contraseña y asignación de esta contraseña de token de hardware, en particular, de una tarjeta de banda magnética y/o de una tarjeta inteligente, en donde la contraseña sirve para autenticar el token de hardware a un sistema técnico y la contraseña es un número de identificación personal PIN que se puede determinar mediante una función hash h a partir de los datos data que se están almacenados de forma legible en el token de hardware, y que se almacena y en donde para la modificación del PIN original a un nuevo PIN de un valor de cambio y se almacena en el sistema de gestión de contraseñas, y/o se almacena de forma legible en el token de hardware que sirve para determinar el nuevo PIN utilizando la misma función hash h, caracterizado porque el valor de cambio y es un valor de entrada adicional para la función hash, mediante la cual el nuevo PIN se determina mediante PIN = h (data, y), en donde el sistema de gestión de contraseña comprende una aplicación que está adaptada para, una vez especificado el nuevo PIN, calcular la función hash con valores de entrada cada vez cambiados hasta que encuentre un valor de entrada apropiado para el nuevo PIN, y para almacenar este valor de entrada.

2. Sistema según la reivindicación 1, caracterizado porque el PIN no se almacena en el token de hardware.

3. Sistema según la reivindicación 1 o 2, caracterizado porque el token de hardware es una tarjeta de banda magnética o tarjeta inteligente, o una tarjeta combinada con una banda magnética y un chip, en donde el token de hardware tiene al menos un área de datos escribible y legible para los datos que determinan el PIN y el valor de cambio.

4. Sistema según la reivindicación 2, caracterizado porque las áreas de datos para los datos que determinan en PIN y el valor de cambio no tienen ningún mecanismo de protección y, por lo tanto, terceros los pueden escribir o leer.

5. El sistema según la reivindicación 2, caracterizado porque el área de datos para los datos que determinan el PIN no tiene ningún mecanismo de protección, y por lo tanto, terceros lo pueden escribir o leer y porque el área de datos para el valor de cambio está protegido, y no es escribible ni legible sin más por un terceros.

6. El sistema según una cualquiera de las reivindicaciones anteriores, caracterizado porque el sistema de gestión de contraseña implementa para cada contraseña un tiempo de validez individual en función de ciertos criterios y asigna al usuario la contraseña con la validez determinado individualmente.

7. Sistema según una cualquiera de las reivindicaciones anteriores, caracterizado porque la función de evaluación para una contraseña introducido por el usuario determina un nivel de seguridad basado en criterios predefinidos asigna a la contraseña un grado asociado al nivel de seguridad asociado y determina la validez individual de la contraseña como una función del nivel de seguridad o bien del grado de calidad asignado a la contraseña, en particular, porque la validez asignada a la contraseña resulte mayor, cuanto mayor sea el grado de calidad de la contraseña.

8. Sistema según una cualquiera de las reivindicaciones anteriores, caracterizado porque el momento de la última modificación del PIN se almacena en el sistema y/o en un área de datos protegida del token de hardware, en particular, por parte de terceros no se puede escribir o leer fácilmente.

9. Sistema según una cualquiera de las reivindicaciones anteriores, caracterizado porque la validez del PIN de la tarjeta de banda magnética está limitada por un contador en el sistema y/o un contador en un área de datos protegida del token de hardware, en particular, un contador para el número de entradas previas de un PIN correcto alcanza o excede un umbral numérico.

10. El sistema una cualquiera de las reivindicaciones anteriores, caracterizado porque los criterios para determinar el grado de calidad de una contraseña comprende una o más de los siguientes parámetros: número de caracteres utilizados, el número de caracteres utilizados de forma repetida, los tipos de caracteres utilizados, datos maestros del usuario en su conjunto o de partes de la contraseña.

11. Sistema según una cualquiera de las reivindicaciones anteriores, caracterizado porque determina la validez del PIN de la tarjeta de banda magnética como un intervalo de tiempo o por medio de una fijación individual del valor límite numérico en función del grado la calidad del PIN puramente numérico seleccionado.

12. Sistema según una cualquiera de las reivindicaciones anteriores, caracterizado porque rechaza automáticamente las contraseñas que no alcanzan un grado de calidad mínimo predeterminado.

13. Sistema según una cualquier de las reivindicaciones anteriores, caracterizado porque indica al usuario, antes de asignar le la contraseña, el grado de calidad determinado y/o su validez, y el usuario puede decidir individualmente sobre la base del grado de calidad y/o de la validez si quiere utilizar la contraseña o no.

14. Sistema según una cualquiera de las reivindicaciones anteriores, caracterizado porque, en general, o sólo en caso de un nuevo PIN imposible por el sistema pero deseada por el usuario, se propone una o más nuevo PIN alternativos y son seleccionables.

15. Sistema según una cualquiera de las reivindicaciones anteriores, caracterizado porque comprueba de forma automática el paso en cuanto a contraseñas del usuario, mediante la comparación de la contraseña actual con los últimos x contraseñas del usuario y/o contraseñas del usuario desde el período pasado y o una combinación de esto.

16. Sistema según una cualquiera de las reivindicaciones anteriores, caracterizado porque le pide al usuario automáticamente a el tiempo, preferiblemente justo antes de la expiración de la validez de la contraseña, para definir una nueva contraseña de su elección.

17. Sistema según una cualquiera de las reivindicaciones anteriores, caracterizado porque el usuario recibe instrucciones generales para la generación de una contraseña segura por el sistema de gestión de contraseña antes de o durante la entrada.

18. Sistema según una cualquiera de las reivindicaciones anteriores, caracterizado porque le comunica al usuario que las contraseñas con alto grado de calidad tienen un periodo de validez más largo que las contraseñas con un grado de calidad bajo.

19. Sistema según una cualquiera de las reivindicaciones anteriores, caracterizado porque es parte de un sistema de procesamiento de datos o de una aplicación y se basa en el hardware y/o software.

20. Sistema según una cualquiera de las reivindicaciones anteriores, caracterizado porque en caso del token de hardware por parte de la aplicación asociada que evalúa un contador y/o otros parámetros, en particular el tiempo, se le pide al usuario cambiar el PIN.

21. Sistema según una cualquiera de las reivindicaciones anteriores, caracterizado porque la aplicación está adaptada para proponer una pluralidad de nuevos PIN para los que ha encontrado valores de entrada durante los cálculos anteriores, en donde uno de estos PIN propuestos se puede seleccionar como nuevo PIN.

22. Método de sistema de gestión de contraseñas para la modificación y verificación de una contraseña y asignación de esta contraseña a un token de hardware, en particular, una tarjeta de banda magnética y/o una tarjeta inteligente, en donde la contraseña sirve para autenticar el token de hardware a un sistema técnico, y la contraseña es un número de identificación personal PIN se determina y se verifica mediante una función hash h de los datos data, que son almacenado de forma legible en el token de hardware, y en donde para la modificación del PIN original a un nuevo PIN se almacena un valor de cambio y de forma legible en el token de hardware y/o en el lado del sistema en una base de datos, que sirve para determinar y verificar el nuevo PIN utilizando la misma función hash h, caracterizado porque el valor de cambio y es un valor de entrada adicional para la función hash es, con la que se determina al menos el nuevo PIN como PIN = h (datos, y), en donde el sistema de gestión de contraseñas comprende una aplicación que, una vez especificado el nuevo PIN, calcula la función hash con cada vez modificados los valores de entrada hasta que se encuentra un valor de entrada adecuado para el nuevo PIN y almacena este valor de entrada.

23. Método según con la reivindicación 22, caracterizado porque para cada contraseña se implementa una validez individual en función de determinados criterios y se asigna la contraseña con la validez fijada individualmente al token de hardware.

24. Método según la reivindicación 22 ó 23, caracterizado porque por medio de una función de evaluación para una contraseña introducida por el usuario se determina el nivel de seguridad en base a criterios predeterminados y a la contraseña se le asigna un grado de calidad asociado el nivel de seguridad y se determina el grado de calidad individual de la contraseña en función del nivel de seguridad asignado a la contraseña o bien el grado de calidad asignado a la contraseña.

25. Método según una cualquiera de las reivindicaciones 22 a 24, caracterizado porque se limita la validez del PIN del token de hardware alcanzando o excediendo un contador, en particular, un contador para el número de entradas previas de un PIN correcto, un límite numérico.

26. Método según una cualquiera de las reivindicaciones 22 a 25, caracterizado porque la aplicación propone varios nuevos PIN, para los que ha encontrado valores de entrada en los anteriores cálculos, en donde uno de estos PIN propuestos se puede seleccionar como nuevo PIN.

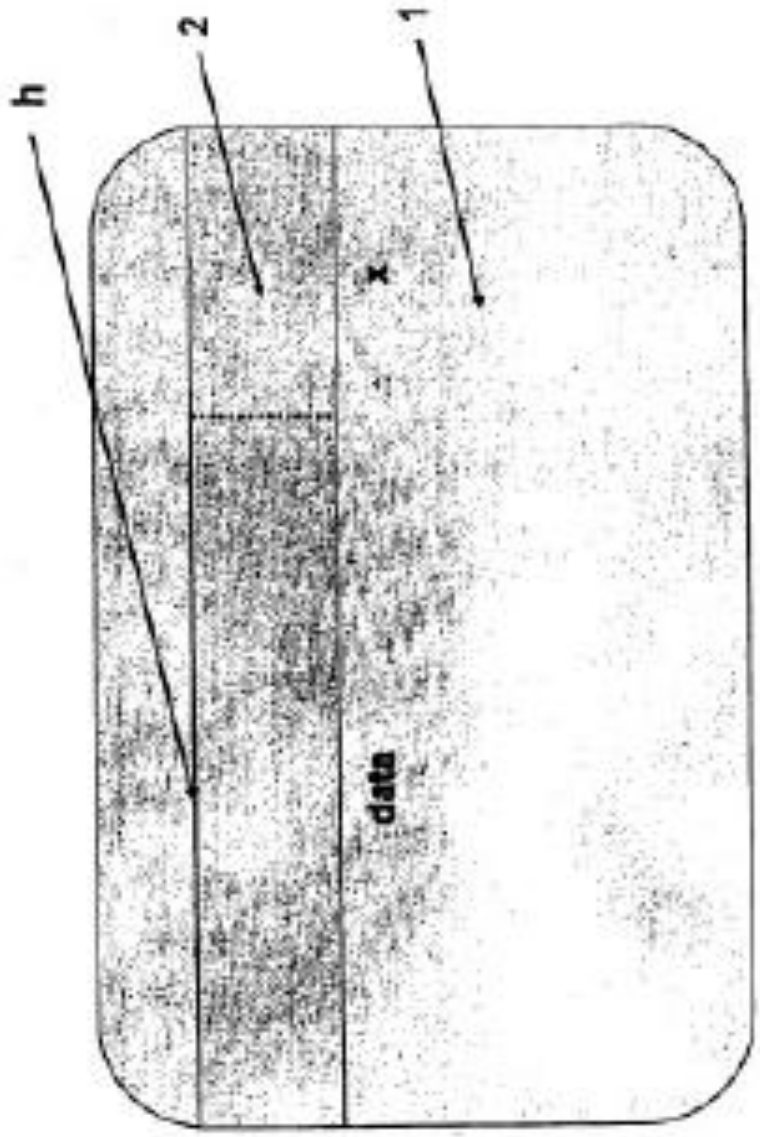
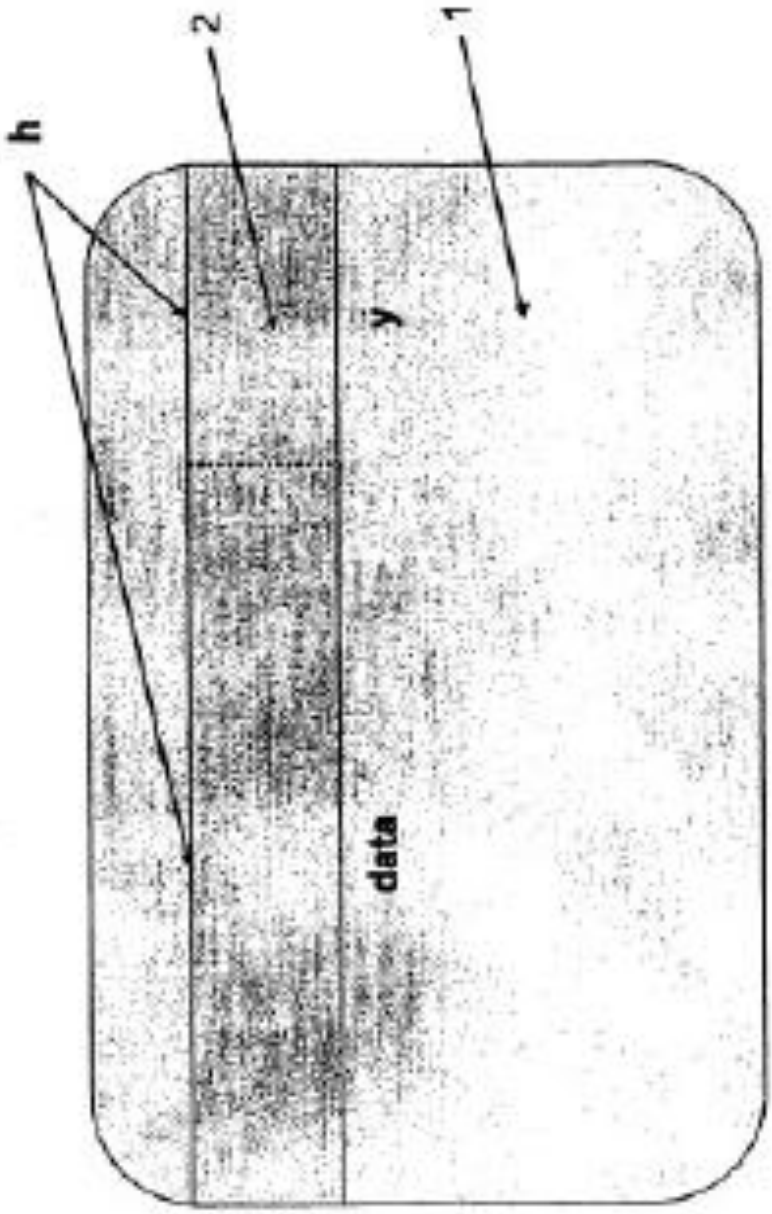

h
2
1
x
data
x: valor de cambio como valor diferencial
h: función hash
PIN = h (data) + x

Figura 1



x: valor de cambio como valor de entrada
h: función hash
PIN = h (data y)

Figura 2