(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 889 226**

(51) Int. CI.:

G06F 21/34 (2013.01)
H04L 9/08 (2006.01)
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
G06Q 20/38 (2012.01)
G06Q 20/40 (2012.01)
G06Q 20/34 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **26.07.2019 E 19188594 (6)**

(97) Fecha y número de publicación de la concesión europea: **14.07.2021 EP 3599564**

(54) Título: **Procedimiento de gestión de un dispositivo electrónico que suministra códigos de autenticación, dispositivos y servidores asociados**

(30) Prioridad:

26.07.2018 FR 1856956

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.01.2022

(73) Titular/es:

IDEMIA FRANCE (100.0%)
2 Place Samuel de Champlain
92400 Courbevoie, FR

(72) Inventor/es:

LESEIGNEUR, GILLES y
DEPRUN, JEAN-FRANÇOIS

(74) Agente/Representante:

DEL VALLE VALIENTE, Sonia

DESCRIPCIÓN

Procedimiento de gestión de un dispositivo electrónico que suministra códigos de autenticación, dispositivos y servidores asociados

Antecedentes de la invención

La presente invención se refiere a un dispositivo electrónico asociado a un usuario y, en particular, a un dispositivo electrónico que suministra códigos de autenticación a un usuario. La presente invención se define en las reivindicaciones independientes 1 , 9 , 1 0 y 1 1 .

La invención se refiere más particularmente a los códigos de autenticación algunas veces denominados códigos de autenticación dinámicos.

Tales códigos pueden usarse en dispositivos electrónicos tales como tarjetas bancarias o incluso fichas de autenticación.

Cuando se usa una tarjeta bancaria para efectuar transacciones financieras a distancia (por Internet o por teléfono), existen riesgos de fraudes que son más importantes que cuando el usuario se presenta en un punto de venta con su tarjeta bancaria. Por tanto, se ha propuesto pedir a los usuarios que introduzcan un código denominado código CVV ("Card Verification Value" en inglés) para autenticar las transacciones e indicar que el usuario está realmente en posesión de la tarjeta bancaria. En la técnica anterior, los códigos CVV eran estáticos y estaban impresos en la parte trasera de la tarjeta bancaria. Como puede concebirse, esta solución no es lo suficientemente segura.

Por tanto, se ha propuesto equipar las tarjetas bancarias de pantallas en las que pueden visualizarse códigos de autenticación denominados CVV dinámicos. Los códigos CVV dinámicos cambian regularmente, por ejemplo, cada hora. En el lado del servidor que va a autenticar la transacción, se actualiza también regularmente el código de autenticación que estará asociado a la tarjeta bancaria para que puedan realizarse las transacciones.

Por tanto, las tarjetas bancarias que suministran códigos CVV dinámicos son dispositivos electrónicos complejos, dado que estas tarjetas bancarias incluyen todas un microcircuito, una pantalla, una batería que puede alimentar la pantalla y, finalmente, un reloj que va a servir para actualizar el código CVV dinámico (de manera sincronizada con el servidor). Existe un riesgo de que uno o varios de estos elementos presenten un fallo.

Por ejemplo, en caso de un fallo del reloj de la tarjeta bancaria, la tarjeta suministrará códigos de autenticación que no están sincronizados con los del servidor usado para autenticar las transacciones. En caso de fallo de la batería, la pantalla no podrá visualizar nuevos códigos de autenticación. Por tanto, la tarjeta bancaria se vuelve inutilizable.

Generalmente, los fabricantes de tarjeta bancaria y las entidades emisoras de estas tarjetas (normalmente los bancos) no tienen ninguna información sobre estos fallos. Un usuario cuya tarjeta presenta un fallo va a solicitar un cambio de tarjeta, pero generalmente no se estudiará la causa del fallo de la tarjeta. Por tanto, los fabricantes de tarjeta bancaria y las sociedades emisoras de estas tarjetas han tomado la costumbre de sustituir regularmente estas tarjetas, por ejemplo, después de un periodo de dos años, correspondiendo este periodo a una vida útil normal de una batería. Se comprende que los servidores de autenticación no tienen acceso a información sobre el funcionamiento de la tarjeta. Por tanto, existe una necesidad de proporcionar información relativa al estado de las tarjetas bancarias para poder gestionar mejor una flota de tarjetas bancarias.

A partir del estado de la técnica anterior, también se conocen fichas de autenticación que se usan para autenticar usuarios en Internet.

Estas fichas de autenticación podrán usarse, por ejemplo, para acceder a servicios, por ejemplo, servicios de mensajería. Los problemas anteriormente mencionados que se plantean para las tarjetas bancarias también se plantean para las fichas de autenticación. A partir del estado de la técnica anterior también se conoce el documento US 2008/029607.

Objeto y resumen de la invención

Para resolver los problemas anteriormente mencionados, la presente invención se refiere a un procedimiento de gestión de un dispositivo electrónico asociado a un usuario y puesto en práctica por el dispositivo electrónico, comprendiendo el procedimiento:

a- una obtención de un código de autenticación actual,

b- una detección de un estado predefinido del dispositivo electrónico,

c- una aplicación al código de autenticación actual de una función predefinida asociada al estado predefinido, para obtener un código de autenticación modificado, y

d- un suministro del código de autenticación modificado al usuario.

En este procedimiento, el código de autenticación puede usarse para una autenticación posterior del usuario, por ejemplo, con un servidor. El servidor esperará, por ejemplo, el código de autenticación actual para autenticar al usuario, pero, si se ha modificado un código de autenticación, el servidor puede detectar y, por tanto, obtener una información sobre el estado del dispositivo electrónico.

Por tanto, el servidor puede determinar que es un código de autenticación modificado que se ha introducido, y, por tanto, podrá detectar que el dispositivo electrónico se encuentra en el estado predefinido que se ha detectado a lo largo de la etapa b.

Evidentemente, la invención no se limita en absoluto a la introducción de código de autenticación en interfaces de servidor. Encuentra aplicación en proporcionar códigos de autenticación que pueden introducirse en cualquier interfaz.

También, el suministro del código de autenticación modificado al usuario puede ponerse en práctica mediante una visualización del código de autenticación modificado en una pantalla del dispositivo electrónico. También podrá suministrarse el código de autenticación modificado al usuario mediante una señal de audio o incluso mediante visualización de un código unidimensional o bidimensional tal como un código de barras o un código QR.

Según un modo particular de puesta en práctica, se detecta un estado predefinido comprendido de entre una pluralidad de estados predefinidos de la tarjeta, estando cada estado predefinido de la pluralidad de estados predefinidos respectivamente asociado a una función predefinida.

Este modo particular de puesta en práctica permite detectar varios estados predefinidos basándose en un código de autenticación modificado.

Por tanto, este modo particular de realización está particularmente adaptado a los dispositivos electrónicos complejos en los que pueden aparecer diferentes tipos de fallos.

Según un modo particular de puesta en práctica, cada estado predefinido de la pluralidad de estados predefinidos está asociado a un código de estado y, para cada estado predefinido, la aplicación de la función predefinida asociada a este estado predefinido comprende la aplicación de una función intermedia común a todos los estados predefinidos y que tiene por variables el código de autenticación actual y el código de estado del estado predefinido.

Este modo particular de puesta en práctica es particularmente fácil de implementar. El código de estado puede ser una cadena de caracteres (letras, cifras, signos o símbolos o varios de los mismos) que se ha elegido previamente. Por tanto, la función intermedia que se usa podrá ser una función matemática o una función lógica.

Según un modo particular de puesta en práctica, la función intermedia que tiene por variables el código de autenticación actual y el código de estado del estado predefinido es la función o exclusiva.

La función o exclusiva es particularmente fácil de implementar. Las propiedades de esta función lógica permiten recuperar un estado predefinido a partir de un código de autenticación modificado.

Según un modo particular de puesta en práctica, se ponen en práctica una primera vez las etapas a a d en un primer instante, y en un segundo instante posterior al primer instante, se repiten las etapas a a d, determinándose los códigos de autenticación actuales a lo largo de las etapas a teniendo en cuenta el instante.

Este modo particular de puesta en práctica está adaptado para los dispositivos electrónicos que suministran códigos de autenticación actualizados regularmente, por ejemplo, cada hora. Cuando debe actualizarse un código de autenticación actual (teniendo en cuenta el instante) también vuelve a actualizarse el código de autenticación modificado. De este modo, los instantes se definen como una duración que transcurre desde una referencia temporal y tener en cuenta el instante significa entonces tener en cuenta esta duración.

También, un instante puede corresponder a la realización de un evento. Por tanto, en este caso hay dos realizaciones de eventos predefinidos separadas en el tiempo en el primer instante y en el segundo instante. Tener en cuenta el instante puede comprender entonces una etapa en la que se tiene en cuenta el evento predefinido asociado a este instante.

Por ejemplo, la realización de un evento puede ser la pulsación de un botón o, más particularmente, la n-ésima pulsación de un botón, y tener en cuenta el instante significa entonces tener en cuenta n. Puede usarse un

contador de pulsaciones desde la entrega al usuario del dispositivo electrónico. Se observará que es posible detectar un nuevo estado predefinido del dispositivo electrónico cada vez que se obtiene un nuevo código de autenticación modificado.

Según un modo particular de puesta en práctica, el código de autenticación actual incluye una pluralidad de caracteres y dicha función predefinida se elige para modificar varios caracteres de la pluralidad de caracteres del código de autenticación actual o todos los caracteres de la pluralidad de caracteres del código de autenticación actual.

Aunque sea posible modificar únicamente un único carácter de la pluralidad de caracteres del código de autenticación actual, es preferible modificar varios caracteres del código de autenticación actual. Esto permite concretamente evitar que un error en un carácter, durante la introducción del código de autenticación modificado, conduzca a la detección de un estado predefinido del dispositivo electrónico.

Según un modo particular de puesta en práctica, en la etapa b, se detectan varios estados predefinidos del dispositivo electrónico, comprendiendo entonces la etapa c una aplicación al código de autenticación actual de una función predefinida asociada a dichos varios estados predefinidos, para obtener un código de autenticación modificado.

Este modo particular de puesta en práctica permite modificar el código de autenticación actual para que pueda leerse en el código de autenticación modificado que el dispositivo electrónico se encuentra en varios estados predefinidos simultáneos. Por tanto, este modo particular de puesta en práctica está bien adaptado a los dispositivos electrónicos complejos que incluyen una pluralidad de componentes.

Según un modo particular de puesta en práctica, el suministro del código de autenticación modificado al usuario comprende una visualización del código de autenticación modificado en una pantalla del dispositivo electrónico.

Se observará que, para el usuario, la visualización de un código de autenticación modificado es totalmente análoga a la visualización de un código de autenticación actual, por ejemplo, un código de autenticación actual según la técnica anterior. De este modo, el usuario puede tener conocimiento del código de autenticación modificado, introducirlo en una interfaz de un servidor y transmitir sin conocerla una información que indica que el dispositivo electrónico se encuentra en un estado predefinido.

Según un modo particular de puesta en práctica, el dispositivo electrónico está configurado además para visualizar códigos de autenticación según varios modos de visualización, comprendiendo el procedimiento además una selección del modo de visualización que va a usarse para visualizar el código de autenticación, teniendo en cuenta dicho estado predefinido detectado.

En este modo particular de puesta en práctica, se visualiza el código de autenticación modificado y se cambia el modo de visualización usado para la visualización de este código de autenticación modificado. Este modo particular de puesta en práctica también se aplica a la detección de varios estados predefinidos detectados simultáneamente.

Si el código de autenticación se visualiza en forma de una cadena de caracteres, entonces en este caso un modo de visualización es una característica de formateo de texto. Un cambio de modo de visualización se refiere a un cambio de al menos una característica de formateo de texto (el texto del código modificado). Una característica de formateo de texto puede estar asociada, de manera no exhaustiva, al color del texto, a un subrayado, etc.

Alternativamente, si el código de autenticación se visualiza de una manera que difiere de una cadena de caracteres, por ejemplo, si se visualiza en forma de un código bidimensional, también podrán ponerse en práctica cambios de modo de visualización, por ejemplo, con una elección de colores particular.

Este cambio de modo de visualización puede percibirse por un usuario y esto implica que el usuario tiene conocimiento de una información complementaria, además del código modificado. Por consiguiente, es posible preguntar al usuario en la interfaz en la que va a introducir un código si el modo de visualización presenta una característica particular, por ejemplo, una característica de formateo. Si esta interfaz es una interfaz de un servidor, entonces el servidor recibe dos informaciones: el código introducido por el usuario y una información sobre el modo de visualización del texto. La información relativa al modo de visualización del texto puede usarse, por ejemplo, para confirmar, en el lado del servidor, el estado predefinido del dispositivo electrónico.

Según un modo particular de puesta en práctica, el dispositivo electrónico es una tarjeta de microcircuito de tipo CVV dinámico o una ficha de autenticación.

Si el dispositivo electrónico es una tarjeta de microcircuito de tipo CVV dinámico, entonces el código de autenticación actual es el código CVV dinámico que se obtendría en una tarjeta según la técnica anterior. En una tarjeta de este tipo, el código de autenticación modificado se visualiza en la parte trasera de la tarjeta junto a la

firma del usuario o en la cara delantera de la tarjeta.

Según un modo particular de puesta en práctica, el estado predefinido se elige de un grupo que comprende al menos un estado de entre los siguientes estados: un estado de funcionamiento normal, un estado en el que una batería del dispositivo electrónico presenta un fallo, un estado en el que una memoria del dispositivo electrónico presenta un fallo, un estado en el que un módulo de determinación del instante del dispositivo electrónico presenta un fallo y un estado en el que el dispositivo electrónico ha alcanzado un valor de temperatura predefinido.

Si el estado predefinido es un estado de funcionamiento normal, puede elegirse una función predefinida que no modificará el código de autenticación actual. De este modo, para un estado de funcionamiento normal, el código de autenticación modificado es idéntico al código de autenticación actual.

El experto en la técnica sabrá implementar la detección de los estados en los que la batería presenta un fallo, una memoria presenta un fallo o incluso un módulo de determinación del instante, por ejemplo, un reloj, presenta un fallo.

También, el seguimiento de la temperatura mediante sensores se conoce en sí mismo en las tarjetas de microcircuito y el experto en la técnica sabrá definir valores de temperatura que pueden considerarse como problemáticos.

Puede observarse que la invención encuentra aplicación en la detección de anomalías o fallos. También encuentra aplicación en la detección de otros estados predefinidos, por ejemplo, el final de la validez del dispositivo electrónico o el número de pulsaciones en un botón de dicho dispositivo electrónico.

La invención también se refiere a un procedimiento de gestión de un dispositivo electrónico asociado a un usuario y puesto en práctica por un servidor, que comprende:

p- una obtención de un código de autenticación actual,

q- una recepción de un código de autenticación introducido asociado al dispositivo electrónico,

r- una detección de un estado predefinido del dispositivo electrónico a partir del código de autenticación actual y del código de autenticación introducido, si el código de autenticación introducido puede obtenerse mediante una aplicación al código de autenticación actual de una función predefinida asociada al estado predefinido.

Este procedimiento de gestión de dispositivo electrónico se pone en práctica por un servidor y puede ponerse en práctica tras la puesta en práctica del procedimiento de gestión de un dispositivo electrónico puesta en práctica por un dispositivo electrónico tal como se describió anteriormente. De hecho, el procedimiento puesto en práctica por un servidor está adaptado para procesar los códigos de autenticación modificados que puede introducir un usuario. En este procedimiento, van a procesarse los códigos de autenticación introducidos como los códigos de autenticación que se han modificado según el procedimiento puesto en práctica por un dispositivo electrónico tal como se describió anteriormente.

La obtención del código de autenticación actual puede realizarse de una manera análoga a la obtención de un código de autenticación dinámico según la técnica anterior.

La recepción de un código de autenticación introducido asociado a los dispositivos electrónicos puede realizarse a través de medios de comunicación o a través de una red tal como Internet. En particular, el usuario puede introducir un código de autenticación en una interfaz del servidor (por ejemplo, que aparece en un terminal del usuario de tipo ordenador o teléfono).

Si el código de autenticación introducido puede obtenerse mediante una aplicación al código de autenticación actual de una función predefinida asociada al estado predefinido, entonces puede detectarse que el dispositivo electrónico se encuentra en este estado predefinido.

Según un modo particular de puesta en práctica, el procedimiento comprende además una comparación del código de autenticación actual con el código de autenticación introducido recibido.

Puede observarse que el procedimiento de gestión de un dispositivo electrónico puesto en práctica por un servidor también puede incluir una etapa de autenticación del usuario. Esta autenticación tiene en cuenta el código de autenticación introducido y la detección del estado predefinido.

En particular, si el código de autenticación introducido es idéntico al código de autenticación actual (lo cual es el caso si un estado predefinido para el estado "normal" usa una función identidad que no modifica el código de autenticación actual; o si no se aplica ninguna función al código de autenticación actual cuando se detecta el

estado "normal") o si el código de autenticación introducido corresponde a un código de autenticación obtenido después de la aplicación de una función predefinida al código de autenticación actual (en este caso, hay autenticación y el procedimiento puede incluir tener en cuenta el estado predefinido, por ejemplo, memorizar el estado predefinido detectado).

Según un modo particular de puesta en práctica, se pone en práctica la etapa r si el código de autenticación actual difiere del código de autenticación introducido recibido.

Este modo particular de puesta en práctica está adaptado a los dispositivos para los que el estado predefinido para el estado "normal" del dispositivo usa una función identidad, es decir, que no modifica el código de autenticación actual, o a los dispositivos que no aplican ninguna función al código de autenticación actual cuando se detecta el estado "normal". Puede observarse que estos dispositivos son ventajosos, ya que pueden funcionar con servidores tales como los descritos en el método definido a continuación, pero también con servidores según la técnica anterior. De este modo, el uso de la invención con tales dispositivos no implica una sustitución de todos los servidores susceptibles de usarse con el dispositivo electrónico con vistas a una autenticación.

También, en este modo de puesta en práctica, solo se pone en práctica la etapa r si existe una diferencia entre el código de autenticación introducido que se ha recibido y el código de autenticación actual. De hecho, si el código de autenticación introducido recibido y el código de autenticación actual son diferentes, o bien se trata de un intento fraudulento de autenticación, o bien se trata de una transmisión de un código de autenticación que se ha modificado para indicar que el dispositivo electrónico se encuentra en un estado predefinido.

De este modo, puede observarse que este modo particular de puesta en práctica es ventajoso, ya que puede funcionar con dispositivos tales como los descritos en el procedimiento definido anteriormente, pero también con dispositivos según la técnica anterior.

Según un modo particular de puesta en práctica, la etapa r incluye:

- una aplicación de la función inversa a dicha función predefinida al código de autenticación introducido para obtener un código de autenticación intermedio, y una comparación del código de autenticación intermedio con el código de autenticación actual, para deducir que el dispositivo electrónico está en el estado predefinido, o - una aplicación de la función predefinida al código de autenticación actual para obtener un código de autenticación modificado, y una comparación del código de autenticación modificado con el código de autenticación introducido recibido, para deducir que el dispositivo está en el estado predefinido, o

- una aplicación de una función intermedia al código de autenticación actual y al código de autenticación introducido para obtener un código de estado intermedio, y una comparación del código de estado intermedio con un código de estado asociado al estado predefinido, para deducir que el dispositivo electrónico está en el estado predefinido,

siendo la función intermedia la función que, aplicada al código de autenticación actual y al código de estado del estado predefinido, suministra un código de autenticación que es el código de autenticación introducido si el dispositivo está en el estado predefinido.

La detección del estado predefinido del dispositivo electrónico puede ponerse en práctica de tres maneras. La primera manera implica que existe una función inversa a dicha función predefinida. Dicho de otro modo, en un estado predefinido, para cada código de autenticación modificado, existe un único código de autenticación actual. Si el código de autenticación intermedio corresponde al código de autenticación actual, entonces a la vez puede deducirse que el dispositivo electrónico está en el estado predefinido y también puede autenticarse al usuario y/o al dispositivo electrónico.

De manera alternativa, puede aplicarse la misma función en el servidor que la que se ha aplicado en el dispositivo electrónico y comparar el código de autenticación modificado (por el servidor) obtenido con el código de autenticación introducido que se ha recibido.

Finalmente, según la tercera manera, puede usarse una función intermedia de tipo función matemática o una función lógica con un código de estado que puede ser una cadena de caracteres (letras, cifras, signos o símbolos o varios de los mismos) que se ha elegido previamente.

Esta tercera variante es muy ventajosa con una función intermedia de tipo o exclusiva, ya que la aplicación de la o exclusiva a un código de estado y a un código de autenticación facilita un código de autenticación modificado, y la aplicación de la o exclusiva a este código de autenticación modificado y al código de autenticación no modificado (por ejemplo, el código de autenticación actual) suministra el código de estado. Esto permite recuperar fácilmente el estado predefinido en el que se encuentra el dispositivo electrónico.

Según un modo particular de puesta en práctica, se detecta un estado predefinido de entre una pluralidad de

estados predefinidos, estando cada estado predefinido de la pluralidad de estados predefinidos respectivamente asociado a una función predefinida.

Este modo de puesta en práctica permite detectar varios estados predefinidos. Está particularmente adaptada a la detección de estados predefinidos en dispositivos electrónicos complejos que incluyen una pluralidad de componentes.

Por ejemplo, cada estado predefinido puede estar asociado a un código de estado diferente. Usando la función intermedia para poner en práctica la etapa r, puede aplicarse esta función intermedia al código de autenticación actual y al código de autenticación introducido y el resultado de esta operación puede ser uno de los códigos de estado (puede ponerse en práctica una comparación con cada código de estado previamente grabado).

Este modo de puesta en práctica está bien adaptada a una función intermedia del tipo o exclusiva.

Según un modo particular de puesta en práctica, se ponen en práctica una primera vez las etapas p a r en un primer instante, y en un segundo instante posterior al primer instante, se repiten las etapas p a r, determinándose los códigos de autenticación actuales a lo largo de las etapas p teniendo en cuenta el instante.

Este modo de puesta en práctica está adaptado para los códigos de autenticación actuales que se obtienen en función del tiempo (y, por tanto, teniendo en cuenta el instante) y para los que existe una sincronización entre los dispositivos electrónicos y los servidores.

De este modo, puede seguirse el estado en el que se encuentra el dispositivo electrónico cada vez que un usuario introduce un código de autenticación que recibe el servidor.

De manera alternativa, este modo de puesta en práctica puede dirigirse a códigos de autenticación actuales que se determinan en un instante que corresponde a la realización de un evento.

Por tanto, en este caso hay dos realizaciones de eventos predefinidos separadas en el tiempo en el primer instante y en el segundo instante. Tener en cuenta el instante puede comprender entonces una etapa en la que se tiene en cuenta el evento predefinido asociado a este instante.

Por ejemplo, la realización de un acontecimiento puede ser la pulsación de un botón del dispositivo o, más particularmente, la n-ésima pulsación de un botón, y tener en cuenta el instante significa entonces tener en cuenta n. Puede usarse un contador de pulsaciones desde la entrega al usuario del dispositivo electrónico en el servidor (y, de manera correspondiente, puede usarse otro contador en el dispositivo electrónico).

Según un modo particular de puesta en práctica, el procedimiento comprende además una puesta en práctica de un procesamiento de seguridad.

Este procesamiento de seguridad puede ponerse en práctica teniendo en cuenta el código de autenticación introducido o incluso teniendo en cuenta el estado predefinido que se ha detectado.

Según un modo particular de puesta en práctica, si en una pluralidad de instantes consecutivos se detectan estados predefinidos del dispositivo que son consecutivamente diferentes, entonces se pone en práctica dicho procesamiento de seguridad.

De este modo, si se observa que un dispositivo electrónico pasa de un estado predefinido a otro estado predefinido entre dos puestas en práctica del procedimiento, entonces puede efectuarse una acción apropiada tal como un procesamiento de seguridad.

El experto en la técnica sabrá elegir el procesamiento de seguridad que va a aplicarse, en función concretamente de la diferencia entre los estados predefinidos observados y de la aplicación.

Según un modo particular de puesta en práctica, el procesamiento de seguridad se pone en práctica si al menos dos de dichos estados predefinidos detectados sucesivamente forman un par predefinido de estados incompatibles sucesivamente.

En este modo de puesta en práctica, puede detectarse, por ejemplo, que un dispositivo electrónico se encuentra en un estado posterior que no es compatible con el estado anterior. Por ejemplo, si un dispositivo electrónico está en un estado en el que presenta un fallo de batería, este dispositivo electrónico ya no puede encontrarse normalmente en un estado en el que presenta un funcionamiento normal. La detección de dos estados sucesivos incompatibles puede indicar concretamente un intento de autenticación fraudulenta. El experto en la técnica sabrá establecer pares de estados incompatibles sucesivamente.

Según un modo particular de puesta en práctica, el procesamiento de seguridad incluye una petición, por parte del

servidor, de un nuevo código de autenticación.

Este modo de puesta en práctica está particularmente adaptado para los dispositivos electrónicos equipados con un botón para obtener un nuevo código de autenticación (por ejemplo, una ficha de autenticación). El servidor podrá verificar de este modo que el nuevo código de autenticación introducido por el usuario permite detectar que el dispositivo electrónico sigue estando en el mismo estado predefinido.

Puede observarse que, después de la petición del nuevo código de autenticación, el procedimiento de gestión de un dispositivo electrónico puesto en práctica por un servidor también puede incluir una etapa de autenticación posterior del usuario. Esta autenticación posterior tiene en cuenta el nuevo código de autenticación introducido y la detección del estado predefinido.

Se observará que esta autenticación posterior del usuario puede obtenerse únicamente si se detecta el mismo estado predefinido después de la introducción del nuevo código de autenticación.

También, en la presente solicitud, si la autenticación se realiza en el contexto de una transacción bancaria, entonces la autenticación posterior satisfactoria del usuario conduce a la validación de la transacción bancaria.

Según un modo particular de puesta en práctica, el procesamiento de seguridad incluye un envío por el servidor de un código de autenticación complementario a un terminal del usuario distinto del dispositivo electrónico y una recepción de un código de autenticación complementario introducido por el usuario.

De la misma manera, el código de autenticación complementario puede permitir una autenticación posterior del usuario. La autenticación posterior del usuario solo puede obtenerse si el código de autenticación complementario introducido por el usuario es el mismo que el código de autenticación complementario enviado por el servidor al terminal del usuario.

También, si la autenticación se realiza en el contexto de una transacción bancaria, entonces la autenticación posterior satisfactoria del usuario conduce a la validación de la transacción bancaria.

Este modo de puesta en práctica permite proteger adicionalmente el procedimiento. El envío por parte del servidor puede ponerse en práctica, por ejemplo, mediante envío de un mensaje de tipo SMS hacia un terminal del usuario.

Según un modo particular de puesta en práctica, el procesamiento de seguridad incluye además el envío de una comunicación a una entidad emisora del dispositivo electrónico.

Este procesamiento de seguridad puede ponerse en práctica, por ejemplo, si se ha detectado un mismo estado predefinido durante detecciones sucesivas un número predefinido de veces.

La entidad emisora del dispositivo electrónico puede ser, por ejemplo, un banco, en el caso en el que el dispositivo electrónico es una tarjeta bancaria.

Según un modo particular de puesta en práctica, el servidor autentica el dispositivo electrónico si el estado predefinido del dispositivo electrónico está comprendido en una lista de estados predefinidos autorizados.

De este modo, podrá denegarse la autenticación de un dispositivo electrónico que está en un estado en el que es poco probable que se encuentre el dispositivo electrónico.

Según un modo particular de puesta en práctica, dicha lista de estados predefinidos autorizados varía en función del tiempo.

Este modo de puesta en práctica permite tener en cuenta fallos que son más probables cuando envejece un dispositivo electrónico. Por ejemplo, los fallos asociados a las baterías son particularmente poco comunes durante la puesta en servicio de un dispositivo electrónico, pero son frecuentes cuando un dispositivo electrónico tiene una antigüedad del orden de dos años.

Se observará que este modo de puesta en práctica se aplica a la vez a los dispositivos que elaboran códigos de autenticación a partir de una duración (por ejemplo, desde la entrega del dispositivo al usuario) o incluso a los dispositivos que elaboran códigos de autenticación con la realización de un evento. En efecto, las n-ésimas pulsaciones de un botón usado para generar un código se efectúan necesariamente más tarde en la vida útil del dispositivo que las primeras pulsaciones. Por consiguiente, para estos dispositivos, el tiempo se estima en función del número de pulsaciones.

Según un modo particular de puesta en práctica, la etapa p comprende la obtención de una primera pluralidad de códigos de autenticación actuales asociados, cada uno, a una ventana, poniéndose la etapa r en práctica para al menos un (o cada) código de autenticación actual de la primera pluralidad de códigos de autenticación actuales, y

si el estado predefinido detectado en el primer instante y en el segundo instante es un estado en el que un módulo de determinación del instante (el módulo que va a determinar que el primer instante o que el segundo instante se alcanza) del dispositivo electrónico presenta un fallo, entonces para los instantes posteriores la etapa p comprende la obtención de una segunda pluralidad de códigos de autenticación actuales asociados, cada uno, a una ventana, teniendo la segunda pluralidad un cardinal más elevado que la primera pluralidad.

El módulo de determinación del instante puede ser un reloj del dispositivo, un botón (el instante es una pulsación de este botón) o incluso un sensor que detecta la realización de un evento.

Por ejemplo, obteniendo una información sobre un fallo del reloj del dispositivo electrónico, puede garantizarse que se efectuará la autenticación del dispositivo electrónico, ya que se observa un número más elevado de ventanas.

La invención también se refiere a un dispositivo electrónico asociado a un usuario que comprende:

- un módulo de obtención de un código de autenticación actual,

- un módulo de detección de un estado predefinido del dispositivo electrónico,

- un módulo de aplicación al código de autenticación actual de una función predefinida asociada al estado predefinido, para obtener un código de autenticación modificado, y

- un módulo de suministro del código de autenticación modificado al usuario

Este dispositivo puede estar configurado para la puesta en práctica de todos los modos de puesta en práctica del procedimiento de gestión de un dispositivo electrónico puesto en práctica por el dispositivo electrónico tal como se describió anteriormente.

La invención también se refiere a un servidor de gestión de un dispositivo electrónico asociado a un usuario, que comprende:

- un módulo de obtención de un código de autenticación actual,

- un módulo de recepción de un código de autenticación introducido asociado al dispositivo electrónico,

- un módulo de detección de un estado predefinido del dispositivo electrónico a partir del código de autenticación actual y del código de autenticación introducido, si el código de autenticación introducido puede obtenerse mediante una aplicación al código de autenticación actual de una función predefinida asociada al estado predefinido.

Este servidor puede estar configurado para la puesta en práctica de todos los modos de puesta en práctica del procedimiento de gestión de un dispositivo electrónico puesto en práctica por un servidor tal como se definió anteriormente.

La invención también propone un programa de ordenador que incluye instrucciones para la ejecución de las etapas de un procedimiento (puesto en práctica por un dispositivo electrónico) tal como se definió anteriormente cuando dicho programa se ejecuta por un ordenador.

La invención también propone un programa de ordenador que incluye instrucciones para la ejecución de las etapas de un procedimiento (puesto en práctica por un servidor) tal como se definió anteriormente cuando dicho programa se ejecuta por un ordenador.

Debe observarse que los programas de ordenador mencionados en el presente documento pueden usar cualquier lenguaje de programación y estar en forma de código fuente, código objeto o de código intermedio entre código fuente y código objeto, tal como en una forma parcialmente compilada, o en cualquier otra forma deseable.

La invención también propone un soporte de grabación legible por un ordenador en el que está grabado un programa de ordenador que comprende instrucciones para la ejecución de las etapas de un procedimiento (puesto en práctica por un dispositivo electrónico) tal como se definió anteriormente.

La invención también propone un soporte de grabación legible por un ordenador en el que está grabado un programa de ordenador que comprende instrucciones para la ejecución de las etapas de un procedimiento (puesto en práctica por un servidor) tal como se definió anteriormente.

Los soportes de grabación (o de información) mencionados en el presente documento pueden ser cualquier entidad o dispositivo que puede almacenar el programa. Por ejemplo, el soporte puede incluir un medio de

almacenamiento, tal como una ROM, por ejemplo, un CD ROM o una ROM de circuito microelectrónico, o incluso un medio de grabación magnético, por ejemplo, un disquete (floppy disc) o un disco duro.

Por otra parte, los soportes de grabación pueden corresponder a un soporte transmisible tal como una señal eléctrica u óptica, que puede dirigirse a través de un cable eléctrico u óptico, por radio o mediante otros medios. En particular, el programa según la invención puede descargarse en una red de tipo Internet.

Alternativamente, los soportes de grabación pueden corresponder a un circuito integrado en el que está incorporado el programa, estando el circuito adaptado para ejecutar o para usarse en la ejecución del procedimiento en cuestión.

Breve descripción de los dibujos

Otras características y ventajas de la presente invención se desprenderán de la descripción realizada a continuación, con referencia a los dibujos adjuntos que ilustran un ejemplo de realización de la misma carente de cualquier carácter limitativo. En las figuras:

- la figura 1 representa de manera esquemática un ejemplo de las etapas de procedimientos puestos en práctica por un dispositivo electrónico y por un servidor,

- la figura 2 representa de manera esquemática un ejemplo de dispositivo electrónico,

- la figura 3 representa en dos ejes los códigos de autenticación actuales del dispositivo electrónico y del servidor,

- las figuras 4A y 4B representan de manera esquemática ejemplos de servidores,

- las figuras 5A y 5B son ejemplos de modos de realizaciones de dispositivos electrónicos,

- las figuras 6A, 6B, 6C y 6D representan modos de visualizaciones de códigos de autenticación,

- la figura 7 representa la detección de un estado que conduce a un procesamiento de seguridad,

- la figura 8 también representa la detección de un estado que conduce a un procesamiento de seguridad.

Descripción detallada de varios modos de realización

La presente invención se refiere al campo de los dispositivos electrónicos que pueden obtener códigos de autenticación y suministrarlos a usuarios. Estos códigos de autenticación pueden introducirse, por ejemplo, en interfaces de sitios de Internet de servidores de autenticación con vistas a la autenticación del usuario o de su dispositivo electrónico, estando el dispositivo electrónico asociado a un usuario.

La presente invención encuentra aplicación concretamente en las transacciones financieras efectuadas mediante tarjetas bancarias a distancia (por ejemplo, en Internet o por teléfono).

En la figura 1 se han representado esquemáticamente las etapas de dos procedimientos: un primer procedimiento P1 puesto en práctica por un dispositivo electrónico, por ejemplo, una tarjeta bancaria, y un segundo procedimiento P2 puesto en práctica por un servidor, por ejemplo, un servidor de autenticación que va a recibir códigos de autenticación introducidos por un usuario para autenticar al usuario.

En una primera etapa A1 el dispositivo electrónico obtiene un código de autenticación actual. Esta etapa puede incluir la aplicación de una función criptográfica, que recibe en la entrada parámetros del dispositivo electrónico y también una información temporal procedente de un reloj del dispositivo electrónico.

También puede usarse una alternativa a la información temporal, y esta alternativa consiste en un número de apariciones de un evento predeterminado, por ejemplo, el número de veces que se ha pulsado el botón del dispositivo desde la entrega de dicho dispositivo al usuario.

El código de autenticación actual puede incluir una pluralidad de caracteres, eventualmente cifras únicamente, por ejemplo, tres cifras (como, por ejemplo, un código CVV dinámico).

En una etapa A2 el dispositivo electrónico detecta un estado predefinido del dispositivo electrónico. Por ejemplo, puede elegirse un estado predefinido del grupo que comprende un estado de funcionamiento normal, un estado en el que una batería del dispositivo electrónico presenta un fallo, un estado en el que una memoria del dispositivo electrónico presenta un fallo, un estado en el que un módulo de determinación del instante del dispositivo electrónico presenta un fallo y un estado en el que el dispositivo electrónico ha alcanzado un valor de temperatura predefinido. Evidentemente, el experto en la técnica podrá retirar etapas de esta lista y/o añadir a la misma otros

estados predefinidos, en función de la aplicación.

No obstante, se observará que esta lista de estados predefinidos está particularmente bien adaptada a los dispositivos electrónicos de tipo tarjetas bancarias.

También, varios estados predefinidos pueden ser detectables simultáneamente. Por ejemplo, una batería que presenta un fallo y una memoria que presenta un fallo son dos estados que no son incompatibles.

A continuación, el dispositivo electrónico pone en práctica la etapa A3 en la que aplica al código de autenticación actual obtenido en la etapa A1 una función predefinida asociada al estado predefinido que se ha detectado en la etapa A2. De este modo, se obtiene un código de autenticación modificado.

Si, por ejemplo, se han detectado simultáneamente dos estados (o más), entonces puede aplicarse una función predefinida asociada a estos dos estados. De este modo, si se ha detectado que el dispositivo presenta una batería que presenta un fallo y una memoria que presenta un fallo, puede usarse una función predefinida asociada a la combinación de estos dos estados.

A continuación, se pone en práctica la etapa A4 en la que se suministra el código de autenticación modificado obtenido en la etapa A3 al usuario. Si el dispositivo electrónico está dotado de una pantalla de visualización, el suministro puede incluir la visualización en esta pantalla de visualización del código de autenticación modificado. De manera alternativa, el código de autenticación modificado puede suministrarse al usuario por medio de una señal de audio o incluso mediante la visualización de un código unidimensional o bidimensional tal como un código de barras o QR en el que está codificado el código de autenticación modificado.

El usuario interviene a continuación tomando conocimiento del código que se le ha suministrado a lo largo de la etapa B4. Normalmente, el usuario va a tomar conocimiento del código que se ha suministrado cuando desea autenticarse en un servidor. Para ello, el usuario pone en práctica la etapa B5 en la que introduce el código de autenticación en una interfaz de un sitio de Internet del servidor.

En el lado del servidor, previamente se ha puesto en práctica una etapa C0 en la que se obtiene un código de autenticación actual. Puede observarse que, si el dispositivo electrónico y el servidor están sincronizados en el tiempo, entonces, preferiblemente, la etapa A1 de obtención del código de autenticación actual puesta en práctica por el dispositivo electrónico se pone en práctica de manera sustancialmente simultánea con la etapa C0 de obtención del código de autenticación actual por el servidor. A lo largo de la etapa C5 el servidor recibe el código de autenticación que se ha introducido por el usuario a lo largo de la etapa B5. Como se concibe, este ejemplo solo se refiere a los dispositivos electrónicos que usan una información temporal de tipo de duración para elaborar códigos de autenticación.

A continuación, se pone en práctica la etapa C6 en la que se compara el código de autenticación introducido por el usuario recibido en la etapa C5 con el código de autenticación actual de la etapa C0. Si el código de autenticación actual difiere del código de autenticación que se ha recibido, entonces puede ponerse en práctica la etapa C7 en la que se detecta un estado predefinido del dispositivo electrónico. Si, por el contrario, la etapa C6 muestra que el código de autenticación introducido por el usuario y el código de autenticación actual son idénticos, entonces puede ponerse directamente en práctica la etapa C8 de autenticación del dispositivo electrónico (o del usuario, lo cual es equivalente en este caso). Se comprende que, si el código de autenticación actual es idéntico al código de autenticación introducido, esto puede implicar que se detecta un estado predefinido denominado "normal" y que el usuario podrá autenticarse finalmente.

Puede observarse que la etapa C6 está particularmente bien adaptada a los dispositivos para los que el estado predefinido para el estado "normal" del dispositivo usa una función identidad, es decir, que no modifica el código de autenticación actual, o a los dispositivos que no aplican ninguna función al código de autenticación actual cuando se detecta el estado "normal".

Como se concibe, si el estado "normal" está asociado a una función predefinida que va a modificar el código de autenticación actual, entonces no se pone en práctica la etapa C6 y se pone directamente en práctica la etapa C7 después de la etapa C5.

En la etapa C7, se ha usado a la vez el código de autenticación actual y el código de autenticación introducido, para detectar que una función predefinida asociada a un estado predefinido del dispositivo electrónico se ha aplicado al código de autenticación actual en el dispositivo electrónico.

En el ejemplo descrito anteriormente, se tiene en cuenta una información temporal (un instante) para elaborar los códigos de autenticación. Por tanto, la puesta en práctica de todas las etapas A1 a A4, B4 y B5, y C0 a C8 puede repetirse con informaciones temporales diferentes y por tanto en instantes diferentes. Por ejemplo, esta puesta en práctica puede efectuarse cada hora para el dispositivo y cada hora o al recibir el código de autenticación introducido por el usuario para el servidor.

En el caso de la alternativa en la que se usa un número de apariciones de un evento, entonces se pueden repetir estas etapas en cada aparición del evento. Por ejemplo, esta puesta en práctica puede efectuarse en cada pulsación de un botón del dispositivo para el dispositivo y al recibir el código de autenticación introducido por el usuario para el servidor. Se observará que, para esta alternativa, la etapa C0 puede ponerse en práctica con la etapa C5, es decir, al recibirse por el servidor el código introducido por el usuario.

La figura 2 es una representación esquemática de un dispositivo electrónico 200 según un ejemplo de realización. El dispositivo electrónico 200 incluye un primer módulo de obtención de un código 201 de autenticación actual, que puede poner en práctica la etapa A1 tal como se describió haciendo referencia a la figura 1.

El dispositivo electrónico 200 también incluye un módulo 202 de detección de un estado predefinido del dispositivo electrónico y que, por tanto, es adecuado para poner en práctica la etapa A2 tal como se describió haciendo referencia a la figura 1. El módulo 202 puede detectar un estado predefinido comprendido en una pluralidad de estados predefinidos de la tarjeta y, en este ejemplo, cada estado predefinido está asociado a un código de estado. Para ello, el dispositivo electrónico 200 está equipado con un módulo 203 de atribución de un código de estado a un estado predefinido que se ha detectado por el módulo 202. Por ejemplo, el módulo 203 puede atribuir una cifra o varias cifras a cada estado predefinido.

Para obtener códigos de autenticación modificados (y, por tanto, poner en práctica la etapa A3 descrita haciendo referencia a la figura 1) el dispositivo electrónico 200 incluye un módulo 204 de aplicación al código de autenticación actual de una función predefinida asociada al estado predefinido que se ha detectado, para obtener un código de autenticación modificado. En este caso, se usa una misma función para todos los estados predefinidos, pero el código de estado proporcionado por el módulo 203 permitirá codificar diferentes estados predefinidos en el código de autenticación modificado. A título indicativo, la función que se implementa por el módulo 204 puede ser la función o exclusiva.

El código de autenticación modificado obtenido por medio del módulo 204 se proporciona a un módulo de suministro del código de autenticación modificado al usuario. El módulo 205 visualiza en este caso tres caracteres ABC. De hecho, el módulo 205 es una pantalla del dispositivo electrónico 200.

La figura 3 ilustra en dos ejes de tiempo los códigos de autenticación actuales que se obtendrán por un lado por el dispositivo (en un primer eje de tiempo) y por otro lado a nivel del servidor (en un segundo eje de tiempo). En un primer instante, el dispositivo obtiene el código de autenticación ABC, este es el código que se visualizará por el dispositivo electrónico, salvo si debe modificarse teniendo en cuenta un estado predefinido detectado del dispositivo electrónico. El código ABC se visualizará, por ejemplo, en una pantalla del dispositivo electrónico durante una primera ventana temporal F11. A continuación, en la ventana temporal F12, el código de autenticación actual obtenido es DEF, en la ventana temporal F13 el código de autenticación actual obtenido es GHI, en la ventana temporal F14 el código de autenticación actual obtenido es JKL, y, finalmente, en la ventana temporal F15 el código de autenticación actual obtenido es MNO. Las ventanas temporales F11, F12, F13, F14 y F15 tienen una duración indicada 302.

El dispositivo electrónico y el servidor no están perfectamente sincronizados en el ejemplo ilustrado en esta figura. En este caso, está presente un desfase temporal 300 entre una referencia temporal del dispositivo electrónico (por ejemplo, un reloj del dispositivo) y una referencia temporal del servidor (por ejemplo, un reloj del servidor). Debido a esto, se observa un desfase temporal 300 entre el primer instante de las ventanas temporales F11, F12, F13, F14 y F15 del dispositivo electrónico y el primer instante de las ventanas temporales correspondientes F01, F02, F03, F04 y F05 en el lado del servidor.

El valor del desfase 300 puede no conocerse ni medirse por el servidor. Debido a esto, usando un código de autenticación actual por ventana F01 a F05, la autenticación del usuario puede fracasar.

Para tener en cuenta el desfase 300, puede introducirse otro desfase temporal 301 entre la referencia temporal del servidor y el primer instante de las ventanas temporales complementarias usadas por el servidor F21, F22, F23, F24, F25. Las ventanas temporales complementarias usadas por el servidor F21, F22, F23, F24, F25 también pueden tener una longitud temporal superior a la de las ventanas usadas en el lado del dispositivo F11, F12, F13, F14 y F15. En el ejemplo ilustrado, las ventanas usadas en el lado del servidor son más largas que las usadas en el lado del dispositivo electrónico, por una duración indicada 303.

De esta manera, el servidor obtiene un código de autenticación actual y puede aceptar el código de autenticación actual de la ventana anterior, ya que estas ventanas se solapan.

El desfase 301 y la duración 303 se eligen de manera que se cubren los desfases 300 posibles de los dispositivos electrónicos que están en estado de funcionamiento normal.

De este modo, en la primera ventana temporal complementaria F21, el servidor obtiene el código de autenticación

actual ABC. A continuación, en la ventana temporal complementaria F22, el servidor obtiene el código de autenticación actual DEF, en la ventana temporal complementaria F23 el servidor obtiene el código de autenticación actual GHI, en la ventana temporal complementaria F24 el servidor obtiene el código de autenticación actual JKL y, finalmente, en la ventana temporal complementaria F25 el servidor obtiene el código de autenticación actual MNO.

En el ejemplo ilustrado, en el instante t1, el servidor obtiene el código de autenticación actual GHI y acepta el código de autenticación actual DEF de la ventana anterior, mientras que, en el instante t2, el servidor obtiene el código de autenticación actual GHI y ya no acepta el código de autenticación actual DEF de la ventana anterior. De hecho, en el instante t1, el servidor ha obtenido dos códigos de autenticación actuales y puede poner en práctica las etapas C5 a C8 con DEF y GHI.

Puede observarse que, si un estado predefinido del dispositivo electrónico es un estado en el que un reloj del dispositivo electrónico presenta un fallo, entonces, para los instantes posteriores, el servidor puede obtener (y aceptar) más de dos códigos de autenticación actuales, por ejemplo, 3 códigos de autenticación actuales. Esto puede obtenerse aumentando la duración 303 de manera que puedan solaparse tres ventanas complementarias.

Por otro lado, el ejemplo de la figura 3 puede implementarse con un dispositivo que usa el número de pulsaciones de un botón para generar códigos de autenticación.

El desfase temporal 300 correspondería entonces a una desviación entre el número de eventos en el lado del servidor y en el lado del dispositivo (por ejemplo, habiendo pulsado el usuario varias veces el botón de su dispositivo sin haber introducido los códigos de autenticación actuales de este modo obtenidos).

El desfase 301 y las duraciones 303 corresponderían entonces a un número de códigos de autenticación introducidos recibidos por el servidor para este dispositivo.

La figura 4A ilustra de manera esquemática un servidor 400, por ejemplo, un servidor adecuado para poner en práctica las etapas C0 a C8 descritas haciendo referencia a la figura 1. Por tanto, el servidor 400 puede ser un servidor de autenticación de un dispositivo electrónico, por ejemplo, un servidor de autenticación que se usa para poner en práctica transacciones financieras.

El servidor 400 incluye un primer módulo 401 de obtención de un código de autenticación actual, este módulo es adecuado para poner en práctica la etapa C0 de la figura 1. El servidor 400 incluye además un módulo 402 de recepción de un código de autenticación introducido y, para recibir los códigos de autenticación introducidos, el servidor 400 incluye medios 403 de comunicación, por ejemplo, un acceso a una red de tipo Internet.

El servidor 400 comprende un módulo 404 de detección de un estado predefinido del dispositivo electrónico a partir de un código de autenticación actual y de un código de autenticación introducido, si el código de autenticación introducido puede obtenerse mediante una aplicación al código de autenticación actual de una función predefinida asociada al estado predefinido del dispositivo electrónico. Por ejemplo, si el código de autenticación introducido que se ha recibido se indica AB'C, entonces puede detectarse un estado predefinido aplicando la función inversa indicada F^{-1} en un submódulo 405 del módulo 404 de detección, esta función inversa permite obtener un código de autenticación intermedio indicado ABC.

El código ABC se compara mediante un submódulo 406 con el código de autenticación actual obtenido por el módulo 401 (proporcionar el código de autenticación actual se representa por medio de una flecha). Si el código de autenticación intermedio ABC es idéntico al código de autenticación actual obtenido por el módulo 401, entonces se ha detectado el estado predefinido del dispositivo electrónico que está asociado a la función puesto en práctica por el módulo 405.

El modo de realización de la figura 4A puede implementarse dado que, en un estado predefinido, la función usada para modificar los códigos en el dispositivo electrónico es una función biyectiva para la que existe una función inversa.

Puede observarse que el módulo 404 de detección está configurado para la puesta en práctica de la etapa C7 descrita haciendo referencia a la figura 1.

También, la función inversa F^{-1} está asociada a un único estado predefinido (o, eventualmente, a varios estados predefinidos que pueden detectarse simultáneamente para los que existe una función predefinida asociada).

Para detectar otros estados predefinidos, se usa un bucle LP que va a reutilizar el submódulo 405 con una función inversa asociada a otro estado predefinido y reutilizar el submódulo 406 para poner en práctica una nueva comparación. El bucle LP puede usarse hasta que se detecte un estado predefinido o, alternativamente, puede usarse para todos los estados predefinidos.

De hecho, el bucle LP se usa por medio de una lista de funciones inversas todas asociadas a un estado predefinido. Por tanto, esta lista de funciones inversas todas asociadas a estados predefinidos está grabada en el servidor. Cuando se recibe un código de autenticación introducido, preferiblemente puede someterse a prueba en primer lugar en el submódulo 405 la función inversa asociada al estado predefinido que se ha detectado a partir del código de autenticación introducido anterior recibido por el servidor, y después recorrer la lista.

Por tanto, la etapa C7 descrita haciendo referencia a la figura 1 puede incluir una repetición de una detección para cada estado predefinido.

La figura 4B presenta un modo de realización alternativo de un servidor 400'. El servidor 400' incluye un primer módulo 401' de obtención de un código de autenticación actual, un módulo 402' de recepción de un código de autenticación introducido, medios 403' de comunicación y, finalmente, un módulo 404' de detección de un estado predefinido del dispositivo electrónico. Los módulos 401' 402' y 403' son análogos a los módulos 401 402 y 403 descritos haciendo referencia a la figura 4A.

En este caso, en el módulo 404', a partir del código de autenticación actual ABC obtenido por el módulo 401', va a aplicarse la misma función indicada F que la que ha podido aplicarse en un dispositivo electrónico. Esta aplicación se pone en práctica mediante un submódulo 405'. De este modo, se obtiene un código de autenticación modificado AB'C que puede compararse en un submódulo 406' con el código de autenticación introducido que se ha recibido por el módulo 402'. Si el código de autenticación modificado AB'C es idéntico al código de autenticación que se ha recibido por el módulo 402', entonces se ha detectado el estado predefinido del dispositivo electrónico que está asociado a la función puesto en práctica por el módulo 405'.

Puede observarse que el módulo 404' de detección también está configurado para la puesta en práctica de la etapa C7 descrita haciendo referencia a la figura 1.

También, la función predefinida F está asociada a un único estado predefinido (o, eventualmente, a varios estados predefinidos que pueden detectarse simultáneamente para los que existe una función predefinida asociada).

Para detectar otros estados predefinidos, se usa un bucle LP' que va a reutilizar el submódulo 405' con una función asociada a otro estado predefinido y reutilizar el submódulo 406' para poner en práctica una nueva comparación. El bucle LP' puede usarse hasta que se detecte un estado predefinido o, alternativamente, puede usarse para todos los estados predefinidos.

De hecho, el bucle LP' se usa por medio de una lista de funciones todas asociadas a un estado predefinido. Por tanto, esta lista de funciones todas asociadas a estados predefinidos está grabada en el servidor. Cuando se recibe un código de autenticación introducido, preferiblemente puede someterse a prueba en primer lugar en el submódulo 405' la función asociada al estado predefinido que se ha detectado a partir del código de autenticación introducido anterior recibido por el servidor, y después recorrer la lista.

Por tanto, la etapa C7 descrita haciendo referencia a la figura 1 puede incluir una repetición de una detección para cada estado predefinido.

La figura 5A representa une tarjeta bancaria 500 cuya parte trasera se ha representado. La tarjeta bancaria 500 comprende una zona 501 en la que un usuario puede poner su firma y una pantalla 502 en la que se ha visualizado un código de autenticación modificado AB'C.

La figura 5B representa una ficha 500' de autenticación, lo cual corresponde a un modo de realización alternativo de la invención. Una ficha 500' de este tipo puede usarse para acceder a servicios en Internet, por ejemplo, para acceder a un servicio de mensajería.

La ficha 500' de autenticación incluye un botón 501' que puede pulsarse para obtener un nuevo código de autenticación visualizado en una pantalla 502'. De hecho, la ficha puede incluir un contador de pulsaciones del botón y el valor asociado al contador puede usarse para la generación de códigos de autenticación actuales.

En el ejemplo ilustrado en la figura 5B, la pantalla 502' visualiza un código de seis caracteres AB'CDEF.

Puede observarse que en este ejemplo se ha modificado un único carácter. Siendo esto, puede concebirse (para este modo de puesta en práctica o todos los demás de la presente descripción) una función predefinida que modifica el código para obtener un código A'B'C'D'E'F', donde "'" indica que el carácter se ha modificado por la función.

Para aumentar la seguridad de los procedimientos tales como se describieron anteriormente, pueden modificarse varios caracteres de la cadena de caracteres del código de autenticación actual, incluso todos los caracteres. De este modo, se evita que un error en un carácter durante la introducción del código se considere en el lado del servidor como otro estado predefinido.

Para aumentar también la seguridad de los procedimientos tales como se describieron anteriormente, cuando se han detectado estados predefinidos particulares por dispositivos electrónicos y cuando estos dispositivos electrónicos incluyen pantallas, puede modificarse la visualización del código de autenticación modificado. Por ejemplo, la figura 6A muestra la visualización denominada normal de un código ABC en una pantalla 601, la figura 6B muestra la visualización del mismo código ABC en una pantalla 602, pero en este caso la visualización se realiza de manera que se obtiene un negativo de la visualización obtenida en el modo de realización de la figura 6A.

En la figura 6C se ha representado una visualización 603 en la que se ha invertido el código ABC. En la figura 6D se ha invertido el código ABC de la misma manera que en la figura 6C, pero se visualiza un negativo en la pantalla 604 de lo que se había obtenido en la pantalla 603 de la figura 6C.

Estos cuatro modos de visualización pueden usarse en función del estado predefinido en el que está el dispositivo electrónico. Si se usa un servidor para recibir códigos de autenticación introducidos, este servidor puede preguntar al usuario (por medio de una interfaz) cuál es el modo de visualización del código en su dispositivo electrónico. Esto puede permitir confirmar, en el lado del servidor, el estado del dispositivo electrónico. De hecho, esto permite verificar que un error de introducción no indica un estado particular del dispositivo electrónico.

En la figura 7, se ha representado un ejemplo de detección de un estado predefinido que conduce a la puesta en práctica de un procesamiento de seguridad. Estas etapas se ponen en práctica por un servidor, concretamente tal como se describió anteriormente.

En una primera etapa DETECCIÓN_N (se trata de la N-ésima detección), se detecta un estado predefinido del dispositivo electrónico, mediante aplicación de uno de los procedimientos tal como se describió anteriormente, con cualquiera de los dispositivos electrónicos descritos anteriormente. El estado detectado es el estado ESTADO_A.

Posteriormente, durante la puesta en práctica de la N+1-ésima detección (indicada DETECCIÓN_N+1), se detecta un estado ESTADO_B que difiere de ESTADO_A.

La detección consecutiva de dos estados predefinidos diferentes conduce a la puesta en práctica de un procesamiento de seguridad P_SEG. En un modo de puesta en práctica, P_SEG se pone en práctica únicamente si ESTADO_A y ESTADO_B son estados que son incompatibles (el experto en la técnica sabrá determinar qué estados son incompatibles entre sí para un mismo dispositivo electrónico).

El procesamiento de seguridad puede ponerse en práctica de varias maneras:

- 701: Solicitud por el servidor de un nuevo código de autenticación (por ejemplo, más tarde o después de una nueva pulsación de un botón);

- 702: Envío por el servidor de un código de autenticación complementario a un terminal del usuario (por ejemplo, un teléfono) para que el usuario introduzca este código de autenticación complementario;

- 703: Envío de una comunicación a una entidad emisora del dispositivo electrónico, por ejemplo, un banco si el dispositivo electrónico es una tarjeta bancaria.

Evidentemente, la lista 701 a 703 no es exhaustiva y pueden concebirse otros procesamientos de seguridad.

En la figura 8, se ha representado otro ejemplo puesto en práctica por un servidor y en el que puede iniciarse un procesamiento de seguridad.

En el instante 800, se entrega el dispositivo electrónico al usuario. Se memorizan dos listas por el servidor:

- una primera lista de estados aceptables que comprende: ESTADO_A

- una segunda lista de estados inaceptables en el instante 800 que comprende: ESTADO_B, ESTADO_C.

Por ejemplo, ESTADO_A puede corresponder a un funcionamiento normal y, si se detecta otro estado al entregarse el dispositivo al usuario, entonces se pone en práctica un procesamiento de seguridad.

Posteriormente, en el instante 800 (por ejemplo, dos años después de entregarle el dispositivo al usuario), la lista de estados inaceptables está vacía, mientras que la lista de estados aceptables comprende todos los estados: ESTADO_A, ESTADO_B y ESTADO_C.

Antes de alcanzar el instante 801, algunos estados (por ejemplo, los relativos a un fallo de batería) son poco probables. Si se detectan, esto puede ser porque un usuario malintencionado intenta adivinar el código de

autenticación.

Por tanto, el uso de estas dos listas que evolucionan a lo largo del tiempo permite proteger el procedimiento.

REIVINDICACIONES

1. Procedimiento de gestión de un dispositivo electrónico asociado a un usuario y puesto en práctica por un servidor, que comprende:

p- una obtención (C0) de un código de autenticación actual,
q- una recepción (C5) de un código de autenticación introducido asociado al dispositivo electrónico,
r- una detección (C7) de un estado predefinido del dispositivo electrónico a partir del código de autenticación actual y del código de autenticación introducido, si el código de autenticación introducido puede obtenerse mediante una aplicación al código de autenticación actual de una función predefinida asociada al estado predefinido,

en el que se ponen en práctica una primera vez las etapas p a r en un primer instante, y en un segundo instante posterior al primer instante, se repiten las etapas p a r, determinándose los códigos de autenticación actuales a lo largo de las etapas p teniendo en cuenta el instante,
la etapa p comprende la obtención de una primera pluralidad de códigos de autenticación actuales asociados, cada uno, a una ventana, poniéndose la etapa r en práctica para al menos un código de autenticación actual de la primera pluralidad de códigos de autenticación actuales, y **caracterizado por que**
si el estado predefinido detectado en el primer instante o en el segundo instante es un estado en el que un módulo de determinación del instante del dispositivo electrónico presenta un fallo, entonces para instantes posteriores la etapa p comprende la obtención de una segunda pluralidad de códigos de autenticación actuales asociados, cada uno, a una ventana, teniendo la segunda pluralidad un cardinal más elevado que la primera pluralidad.

2. Procedimiento según la reivindicación 1, que comprende además una comparación del código de autenticación actual con el código de autenticación introducido recibido.

3. Procedimiento según la reivindicación 2, en el que se pone en práctica la etapa r si el código de autenticación actual difiere del código de autenticación introducido recibido.

4. Procedimiento según una cualquiera de las reivindicaciones 1 a 3, en el que la etapa r incluye:

- una aplicación de la función inversa a dicha función predefinida al código de autenticación introducido para obtener un código de autenticación intermedio, y una comparación del código de autenticación intermedio con el código de autenticación actual, para deducir que el dispositivo electrónico está en el estado predefinido, o
- una aplicación de la función predefinida al código de autenticación actual para obtener un código de autenticación modificado, y una comparación del código de autenticación modificado con el código de autenticación introducido recibido, para deducir que el dispositivo está en el estado predefinido, o
- una aplicación de una función intermedia al código de autenticación actual y al código de autenticación introducido para obtener un código de estado intermedio, y una comparación del código de estado intermedio con un código de estado asociado al estado predefinido, para deducir que el dispositivo electrónico está en el estado predefinido,

siendo la función intermedia la función que, aplicada al código de autenticación actual y al código de estado del estado predefinido, suministra un código de autenticación que es el código de autenticación introducido si el dispositivo está en el estado predefinido.

5. Procedimiento según una de las reivindicaciones 1 a 4, en el que se detecta un estado predefinido de entre una pluralidad de estados predefinidos, estando cada estado predefinido de la pluralidad de estados predefinidos respectivamente asociado a una función predefinida.

6. Procedimiento según una cualquiera de las reivindicaciones 1 a 5, que comprende además una puesta en práctica de un procesamiento de seguridad.

7. Procedimiento según una cualquiera de las reivindicaciones 1 a 6, en el que el servidor autentica el dispositivo electrónico si el estado predefinido del dispositivo electrónico está comprendido en una lista de estados predefinidos autorizados.

8. Procedimiento según la reivindicación 7, en el que dicha lista de estados predefinidos autorizados varía en función del tiempo.

9. Servidor de gestión de un dispositivo electrónico asociado a un usuario, que comprende:

- un módulo (401, 401') de obtención de un código de autenticación actual,
- un módulo (402, 402') de recepción de un código de autenticación introducido asociado al dispositivo electrónico,
- un módulo (404, 404') de detección de un estado predefinido del dispositivo electrónico a partir del código de autenticación actual y del código de autenticación introducido, si el código de autenticación introducido puede obtenerse mediante una aplicación al código de autenticación actual de una función predefinida asociada al estado predefinido

en el que el servidor está configurado para poner en práctica una primera vez la obtención, la recepción y la detección en un primer instante, y en un segundo instante posterior al primer instante, y repetir la obtención, la recepción y la detección, determinándose los códigos de autenticación actuales a lo largo de las obtenciones teniendo en cuenta el instante,
la obtención comprende la obtención de una primera pluralidad de códigos de autenticación actuales asociados, cada uno, a una ventana, poniéndose la detección en práctica para al menos un código de autenticación actual de la primera pluralidad de códigos de autenticación actuales, y **caracterizado por que**
si el estado predefinido detectado en el primer instante o en el segundo instante es un estado en el que un módulo de determinación del instante del dispositivo electrónico presenta un fallo, entonces para instantes posteriores la obtención comprende la obtención de una segunda pluralidad de códigos de autenticación actuales asociados, cada uno, a una ventana, teniendo la segunda pluralidad un cardinal más elevado que la primera pluralidad.

10. Programa de ordenador que incluye instrucciones para la ejecución de las etapas de un procedimiento de gestión según una cualquiera de las reivindicaciones 1 a 8, cuando dicho programa se ejecuta por un ordenador.

11. Soporte de grabación legible por un ordenador en el que está grabado un programa de ordenador que comprende instrucciones para la ejecución de las etapas de un procedimiento según una cualquiera de las reivindicaciones 1 a 8.

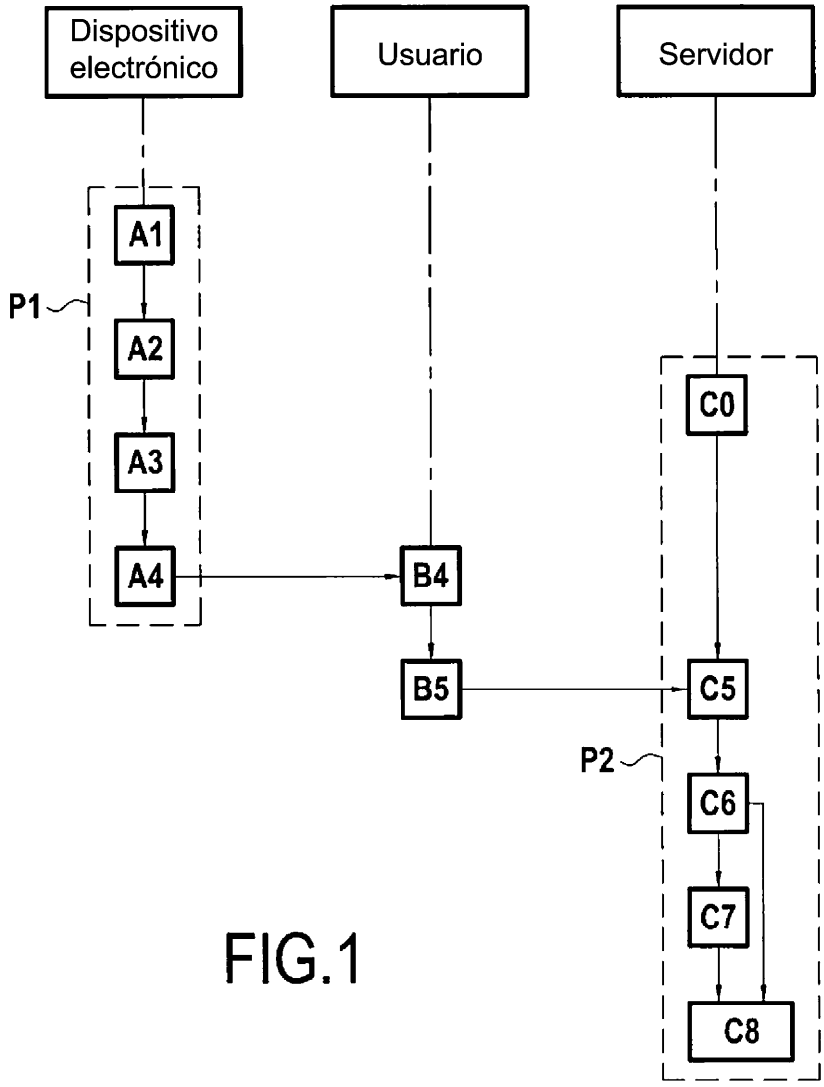

Dispositivo electrónico
Usuario
Servidor
A1
P1
A2
A3
A4
B4
B5
C0
C5
P2
C6
C7
C8

FIG.1

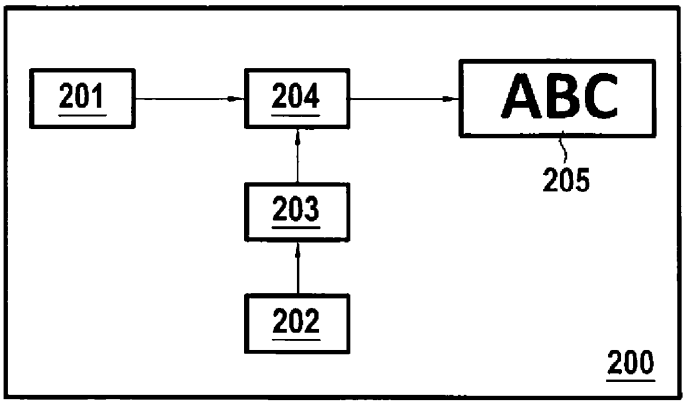

201
204
ABC
205
203
202
200

FIG.2

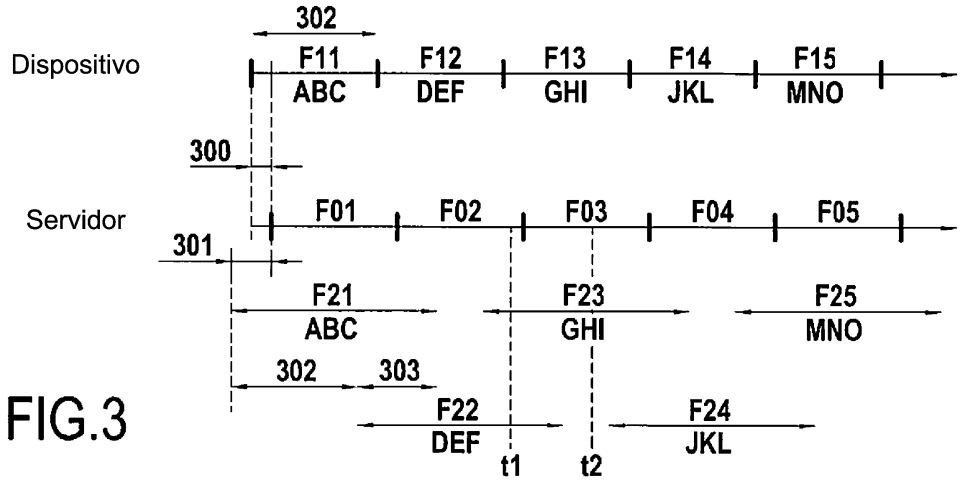


FIG.3

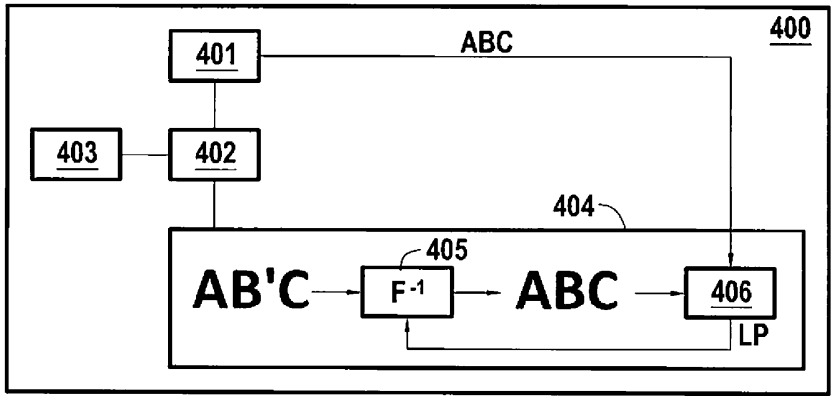


FIG.4A

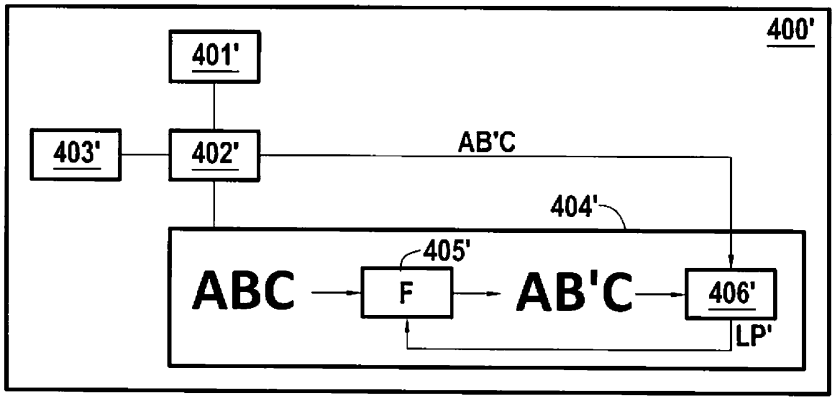


FIG.4B

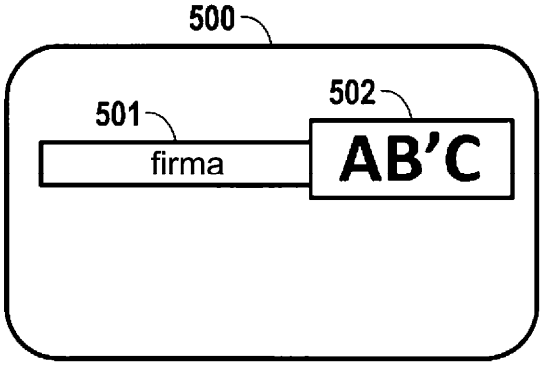


FIG.5A

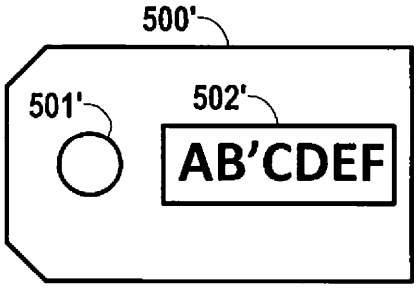


FIG.5B

FIG.6A 

FIG.6B 

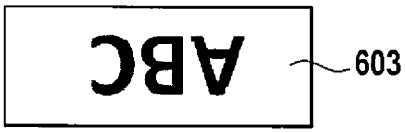
FIG.6C 

FIG.6D 

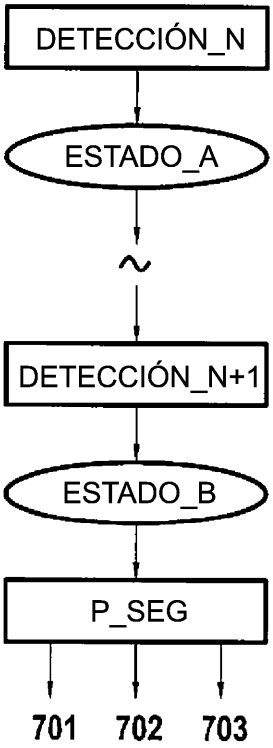

DETECCIÓN_N
ESTADO_A
DETECCIÓN_N+1
ESTADO_B
P_SEG
701
702
703

FIG.7

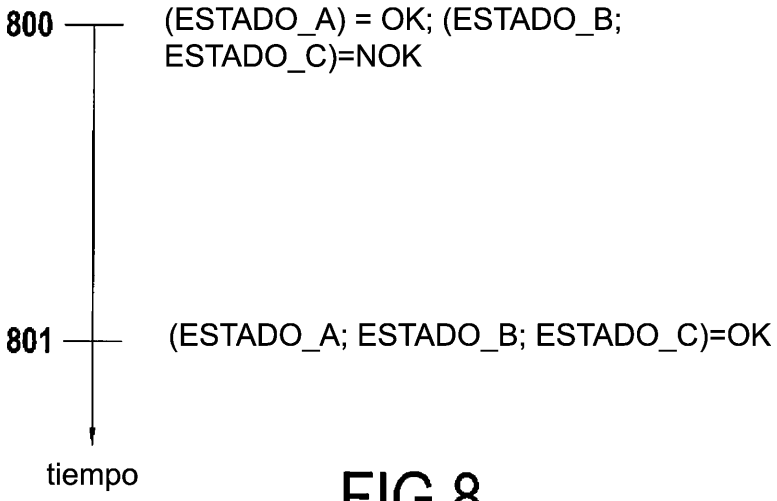

800
(ESTADO_A) = OK; (ESTADO_B; ESTADO_C)=NOK
801
(ESTADO_A; ESTADO_B; ESTADO_C)=OK
tiempo

FIG.8